Informe Jurídico

"REGULACIÓN JURÍDICA DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES AL INTERIOR DE LA ADMINISTRACIÓN DEL ESTADO, Y SU ARMONIZACIÓN CON LA LEY 20.285 SOBRE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN DE LOS SERVICIOS PÚBLICOS".

RENATO JIJENA LEIVA

Profesor de Derecho Informático PUCV
www.jijena.com

SUMARIO

INTRODUCCIÓN

1. El artículo 33 letra m) de la ley 20.285 del año 2008 -sobre acceso y transparencia de la información administrativa- estableció, dentro de las competencias del nuevo "Consejo de Transparencia", la obligación de velar por la aplicación y el cumplimiento de la ley 19.628 del año 1999 sobre el tratamiento o procesamiento electrónico -o manual- y la protección de *datos personales o nominativos*[1] en la gestión de los órganos de la Administración del Estado.

Esta segunda normativa, titulada en concreto *"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 -*los que a efectos de este Informe son considerados términos sinónimos pero que en doctrina poseen alcances diversos*[2]- 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[3], 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[4].

Al decir del artículo 1°, a la ley 19.628 se sujeta el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares[5]. En este Informe 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.

---

[1] El articulo 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.

[2] El artículo 2° letra g) de la ley 19.628, cuando define lo que son los datos sensibles, alude a los hechos o circunstancias de *"la vida privada o intimidad"* de las personas.

[3] La primera Moción senatorial era un proyecto más amplio, sobre protección civil de la privacidad en el caso de intromisiones ilegítimas, y luego de su paso por la Cámara se limitó al tema del procesamiento computacional o del tratamiento informático de los datos personales, sin que su título inicial fuera modificado.

[4] 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* -en adelante ley de acceso y transparencia-, 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*.

[5] 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 N°12 de la Constitución Política.

Ergo, al ser subsumida la aplicación de la ley 19.628 dentro de la competencia de Derecho Público del Consejo de Transparencia, lo que no está exento de generar las distorsiones que se analizan en la Parte Segunda de este Informe, 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 *"tratados"*[6] 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 *"generar criterios y mecanismos que puedan ser utilizados por los diversos órganos de la Administración del Estado para proteger la privacidad de terceros"*[7].

2. 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 asignarse 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[8].

Son adecuadas las constataciones que se han hecho[9] en cuanto a que el Estado es el principal tenedor de información personal (posee lo que la ley 19.628

---

[6] Como veremos, 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.

[7] (SOTO VELASCO)2009

[8] Se ha mencionado la existencia, en este sentido, de *"...una tensión entre las necesidades de la gestión pública, sobre todo una gestión moderna estructurada en torno a las necesidades de los servicios públicos que requiere conocer a sus usuarios, con la necesaria protección de la privacidad de las personas ante el poder público".* Pero efectivamente, si *"…tener información detallada de las personas es tremendamente valioso"* ello *"…no implica que sea necesario poder individualizar a las personas, sino simplemente contar con datos innominados para evaluar el impacto de políticas públicas y para la investigación académica"*, de manera que sea posible *"…medir la pertinencia de los subsidios, del sistema de protección social u otros instrumentos del Estado que implican importantes gastos y que requieren evaluaciones rigurosas sobre los efectos que han tenido en la población objetivo específica".*

[9] Véase la URL http://protecciondedatospersonales.cl/2009/11/16/proteccion-de-datos-en-el-xiii-congreso-de-derecho-informatico/ la exposición de la abogado Romina GARRIDO.

denomina *"registros, recopilaciones o bancos de datos*"[10]), 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.

3. A la normativa del *"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 de Tratamiento de Datos Personales o STDP en el Sector Público"*, porque conceptualmente -en sede 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.

Pero el marco normativo de los STDP no se circunscribe sólo a la ley 19.628, sino que se extiende -por ejemplo- a la regulación de convenios de intercambio de datos, se proyecta a las realidades de la red Internet, y exige la adopción de mecanismos idóneos de seguridad de sistemas por parte de los servicios públicos que, en su calidad legal de *"responsables de bases de datos"*[11]*,* siempre deben ser diligentes.

4. ***En la Parte Primera de este Informe***, la mas extensa, se analiza -creemos sin omisiones importantes- todo el marco normativo relacionado con el tratamiento de datos personales por los servicios públicos de la Administración, en base incluso a casos concretos, recogiéndose estudios cualitativos y cuantitativos ya realizados y analizándose fallos de los tribunales.

---

[10] 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".*

[11] El artículo 2° letra n) dispone que n) *el responsable del registro o banco de datos es la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.*

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 especial N°19.628 de 1999 (acápite "B"), 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 realiza el cruce con todas las otras normas relacionadas.

Así y con este objetivo: (i) se encuadra en la ley 19.628 la regulación legal de los datos llamados "RUN" y "RUT"; (ii) se analizan 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) se proyecta la problemática del tratamiento de datos personales de los ciudadanos al uso de la red Internet, lo que lleva a revisar el Decreto Supremo N°100; (iv) se analiza el marco normativo relacionado con la seguridad que deben observar los servicios públicos en la gestión de los STDP, y un Decreto N°83 que complementa lo establecido en la ley 19.628; (v) se estudia la regulación legal del dato personal *"dirección de correo electrónico",* tanto de los ciudadanos como de los funcionarios públicos, donde los primeros no pueden ser utilizados con fines de *spam*, y la problemática relacionada con la supuesta privacidad o confidencialidad de las comunicaciones de los funcionarios en base a sus casillas de correo institucionales; (vi) se revisa someramente la posibilidad cierta de que, mediando facultades legales expresas, se comercialicen datos personales de los ciudadanos; (vii) se estudia la opción de generarse bases de datos personales para implementar mecanismos de autenticación de los ciudadanos que se conecten en línea a los servidores de la red Internet de los servicios públicos, como así mismo, las consideraciones sobre la confidencialidad de las llamadas direcciones IP de los ciudadanos -que también poseen la naturaleza de datos personales-; y, (viii) se formulan algunas prevenciones respecto a la falta de sustrato legal que a esta fecha se observa para la llamada PISEE o Plataforma Integrada de Servicios Electrónicos del Estado.

5. *En la Parte Segunda del Informe* se intenta conciliar todo el marco normativo de los STDP con las disposiciones y contenidos de la ley 20.285, con el criterio transversal a todos los acápites del Informe 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.

(i) Se analizan en forma comparada, en primer lugar, las normas constitucionales, las políticas legislativas y los conflictos jurídicos que pueden

presentarse, tanto en sede de protección de datos personales como en el ámbito de la ley de acceso y transparencia; (ii) se consignan los contenidos esenciales de la ley 20.285, de cara a su relación con el tratamiento de datos personales; (iii) se formula y se argumenta acerca de la hipótesis central de trabajo de la Parte Segunda del Informe, a saber, que la protección legal de los STDP es una limitante al derecho de acceso a la información administrativa; (iv) se analiza la excepción a la transparencia activa del artículo 7° de la ley, constituida por los datos personales sensibles o personalísimos; (v) 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; (vi) 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; (vi) se analizan los alcances del rol y de la competencia otorgada al Consejo de Transparencia por el artículo 33 letra m) de la ley 20.285; (vii) 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; (viii) y se termina esta Parte Segunda del Informe con la revisión de los criterios sostenidos por el Consejo de Trasparencia en algunos Dictámenes de Amparo relacionados con datos personales.

6. Al final de esta introducción, algunas breves consideraciones *"meta-jurídicas".*

La regulación jurídica del sistema de tratamiento o procesamiento electrónico de datos personales que existe para los servicios públicos es un tema relevante, que también -desde el conocimiento de la realidad práctica- ha sido desperfilado por juristas y medios de prensa. Se ha sugerido que los servicios públicos participarían en un verdadero tráfico de datos personales en conjunto con empresas particulares, olvidándose que los órganos del Estado persiguen fines de orden público y que requieren de procesar y acceder a datos sobre los chilenos sólo para el cumplimiento de sus fines promocionales y asistenciales. Se ha olvidado además, que los servicios públicos actúan con total transparencia y sin anonimato, con lo cual no cabe incluirlos en el *"mercado negro*" en el que si operan las empresas particulares proveedoras y distribuidoras de información, no registradas ni fiscalizadas debido a las omisiones, limitaciones y falencias de la ley 19.628.

Desde Septiembre del año 2009 ONG chilenas como *Proacceso* iniciaron un proceso sistemático de apariciones en los medios de prensa, mediante entrevistas, columnas y cartas al director que apuntaban a cuestionar la regulación y las prácticas relacionadas con tema del procesamiento de datos personales en el sector público, en particular en el Servicio Electoral de Chile. La ONG aspira -con bastante fundamento- a posicionar el debate como Política Pública, poniendo de relevancia el nuevo rol asignado en el artículo 33 letra m) de la ley 20.285 y en

el proyecto de ley del Boletín 6120 -que apunta a modificar la ley 19.628- al Consejo de Transparencia[12].

Pero ella no visualizó:

(i) Que en Chile ningún servicio público procesa datos personales en forma secreta, y que todos deben hacerlo en forma diligente, leal y lícita y sólo para cumplir sus fines promocionales y asistenciales, bajo apercibimiento de aplicárseles las responsabilidades objetivas de Derecho Público que establece la Ley General de Bases de la Administración del Estado;

(ii) Que para el sector público no se requiere un registro obligatorio de responsables de bases de datos porque todos saben que todos los servicios públicos tratan datos de los ciudadanos, y cualquier personas respecto de cualquier servicio público puede ejercer el Habeas Data del artículo 12 de la ley 19.628, sin que se enfrente al anonimato o a la clandestinidad de los responsables de las bases de datos;

(iii) Que la competencia asignada en esta materia al Registro Civil para solo llevar un listado era innecesaria, fue mera burocracia y no importaba una medida de fiscalización de aquellas que le son propias a los entes en el Derecho Comparado que fiscalizan a los órganos registrados, tanto a los públicos como a los particulares dedicados al tratamiento de datos personales[13];

---

[12] En el mes de Diciembre del 2009 ha vuelto a insistir en sus denuncias, nuevamente en torno a la falta de los servicios públicos no anotados en el Registro Público del artículo 22, pero esta vez con una referencia nueva a la falta de seguridad tecnológica en la administración de los sistemas de tratamiento de datos personales de los servicios públicos, respecto a lo cual, demostrando no conocer el Decreto Supremo 83, afirmó que no existían políticas claras ni normas técnicas sobre las reglas de seguridad que se debieran seguir en el manejo de las bases de datos. Véase la URL http://diario.elmercurio.cl/2009/12/28/nacional/politica/noticias/b2e65221-d7a4-4480-915b-ccd75c7eede2.htm

[13] Aún así, la ONG realizó un estudio e informe a partir de un cuestionario de siete preguntas enviado durante el mes de septiembre a los servicios públicos, que involucró a 164 servicios, programas o beneficios de los ministerios de Vivienda, Salud, Educación, Trabajo y Planificación, y el Servicio Nacional de la Mujer, y dentro de sus conclusiones constató: (i) que el 97% de 164 servicios públicos vulneraba la norma de protección de datos personales, porque ellos no entregan los antecedentes que exigen el artículo 22 de la ley 19.628 y su Reglamento al Registro Civil, lo que impediría -según ellos- conocer la información que maneja el Estado sobre los ciudadanos; y, (ii) que sólo el 3% de las reparticiones dependientes de los ministerios sociales tienen inscritas las bases de datos con información de ciudadanos que usan en sus entidades. La ONG calificó como *"un panorama preocupante"* el que exista un escaso cumplimiento de la ley sobre protección de datos y vida privada, porque de los 50 servicios que respondieron formalmente hubo 39 que reconocieron tener bases de datos personales, y de ésos solamente 5 han cumplido con su deber de registrarlas ante la entidad correspondiente, que es el Registro Civil.

(iv) Que la importancia de un registro obligatorio surge para evitar el anonimato en el tráfico de datos personales realizados por los *list brokers* en el sector privado, que son los que operan sólo con fines de lucro, sin autorización, en forma quizás no leal y quizás ilícita; y,

(v) Que esta omisión de la ley de 1999 no fue casual, porque bajo el pretexto de *"no ser burocráticos"* y aprobar una ley para lo cual no se contaba con el patrocinio del Ejecutivo de la época -facultado por la Constitución en forma exclusiva para generar las instancias orgánicas y de fiscalización en la Administración-, el Congreso Nacional se apartó radicalmente de lo que regulaban los dos modelos mencionados como esenciales de la ley 19.628, a saber, la ley de Francia de 1978 y la de España de 1992.

PARTE PRIMERA

REGULACIÓN JURÍDICA DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES AL INTERIOR DE LA ADMINISTRACIÓN DEL ESTADO

A. Normas jurídicas generales y especiales que regulan legalmente los sistemas de tratamiento de datos personales (en adelante indistintamente referido como "STDP") en el Sector Público (referencia).

1. 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.

(i) 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; (ii) por *información innominada*, aquel conjunto de datos reales que se independizan de toda identificación o caracterización del administrado porque son disociados; y, (iii) 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 email-.

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 como se sostiene y fundamenta en este Informe las bases de datos de los servicios públicos no pueden ser calificadas como fuentes públicas de información susceptibles de ser accesadas por cualquier particular, empresa o servicio público, en cualquier tiempo y en forma gratuita, *salvo en condiciones y circunstancias excepcionales como por haberlo establecido una ley general o por ordenarlo 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.

En la Segunda Parte del Informe se analiza en extenso cuáles son las particularidades generadas por la ley 20.285, que en síntesis y al momento de intentar conciliar, armonizar o equilibrar con ella la normativa anterior sobre tratamiento de datos personales -no sólo la ley 19.628-, y no obstante los objetivos de transparencia y publicidad de los actos, contratos, documentos, resoluciones y procedimientos que le son propios, sus disposiciones y las Políticas Públicas que las inspiran no pueden ser entendidas como el desconocimiento de la normativa legal que ampara y regula el tratamiento de datos personales.

La existencia de una específica causal de reserva o secreto, como la del artículo 21 N°2 que alude a la esfera privada de un ciudadano, es un ejemplo que demuestra lo contrario.

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[14];

(ii) La naturaleza de la información solicitada (v.gr. pública; privada, secreta o reservada[15]; nominativa; estadística o disociada; relacionada; etcétera);

[14] 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.

[15] 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.

(iii) Si existe -o no- una obligación expresa establecida por ley para proceder a la entrega de la información[16]; 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:

1°, *Estudiar la procedencia o no teniendo presente lo que establezcan normas legales generales de Derecho Público y Administrativo, 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[17];

2° *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 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 suscribirá con tales servicios un convenio que determine las modalidades operativas y las concretas medidas de seguridad mediante las cuales se apoyará la gestión del órgano y se cumplirá con el mandato legal; y,

[16] 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 la 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.

[17] 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.

3°, *Revisar luego lo que dispongan normas especiales como la ley 19.628 sobre tratamiento de datos personales*[18] *y la ley 20.285 sobre transparencia y acceso a la información administrativa*[19] -si es que este 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; l*a competencia del servicio público para "tratar", procesar, almacenar, generar o difundir los datos personales sobre los ciudadanos*[20]; 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 del servicio público y de la Administración del Estado el entregar o no determinada información nominativa.

2. 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[21].

---

[18] 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 esa no es una de las especificas competencias establecidas por ley para este órgano determinado.

[19] 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 N°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.

[20] 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.

[21] 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.

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, sobre tratamiento de datos personales.

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 establecidas legalmente, o se afecte la seguridad de la nación o el interés nacional.

3. Existen pues, como se ha referenciado, 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 de datos personales, de servidores y de redes telemáticas abiertas (como Internet) o cerradas (como las Intranet o las redes VAN que operan en materia aduanera), que en su conjunto determinan la competencia, las obligaciones y la 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 las 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 este Informe analiza en detalle y dentro de diversos contextos específicos.

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.

Ellas, 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 la red 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 en el Título IV de la ley 19.628 el artículo 20 califica como *"las materias de su competencia"* exclusiva[22].

Así, en concreto y por ejemplo, cuando el artículo 33 letra m) de la ley 20.285 establece que el Consejo de Transparencia debe velar por el cumplimiento de la ley 19.628 al interior de la Administración del Estado, por aplicación de un Decreto Supremo N°100 del año 2006 la 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, accesados, recopilados y registrados mediante los sitios web de los servicios públicos.

Pudiera entenderse que la promulgación de estas normas obedece a una Política Pública previamente determinada. Ello, porque algunos documentos marco de lineamientos de la gestión del Estado han hecho referencia al problema del tratamiento de datos personales.

Es el caso, en el contexto del gobierno electrónico y de la modernización del Estado, que a comienzos del año 2007 se retomó parcialmente el tema de la protección de los datos personales de los ciudadanos que son procesados o *"tratados"* computacionalmente por los servicios públicos. Concretamente, se hizo en el Marco de un *Instructivo Presidencial N°001 que creó el Comité de Ministros para el Desarrollo Digital*, cuya finalidad esencial es la de coordinar, implementar y hacer el seguimiento de una Agenda Digital[23].

En términos específicos, uno de los objetivos iniciales encomendados al Comité fue el de diseñar y consensuar un *Plan Estratégico Nacional en TICs* y una *Política de las Tecnologías de la Información y de las Comunicaciones (PTIC)*. A este respecto, se consignó en el Instructivo Presidencial que la Política debía atender problemas sociales y económicos derivados del avance de las tecnologías de la información que no habían sido considerados adecuadamente, o que habían mostrado ser obstáculos importantes para el crecimiento tecnológico de los países desarrollados. Y se señaló, como uno de los ejemplos de problemas sociales, a "*los derivados de ambigüedades en torno a la privacidad y seguridad de los datos personales procesados y almacenados en medios digitales".*

[22] 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".*

[23] Está disponible en la URL http://www.estrategiadigital.gob.cl/files/instructivo_ComiteMinistrosDesarrolloDigital_02-02-2007.pdf

B. Las disposiciones especiales de la ley 19.628 de 1999, sobre tratamiento de datos personales y su aplicación a los servicios públicos de la Administración del Estado devenidos legalmente en *"Responsables de Bases de Datos"*.

1. Contenidos esenciales de la ley 19.628 y su Reglamento.

1.1 *Fundamentos y visión de contexto de la normativa.*

Si bien es cierto *el problema de la protección legal de datos personales frente al tratamiento computacional de los mismos* es un tema con bastante perspectiva en países extranjeros, en Chile constituye una realidad desconocida y poco estudiada jurídicamente. Desde ya cabe señalar que el tema de los *"datos personales o nominativos tratados o procesados computacionalmente"* va mucho más allá que el problema de los protestos, de la morosidad comercial y de los archivos históricos almacenados en bancos de datos.

Suele afirmarse que el abuso de las posibilidades computacionales -*sea por entes particulares, sea por órganos estatales*- constituye la amenaza por excelencia contra la intimidad, porque cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial del titular de los datos debe ser resguardada porque puede ser creada errada, negligente o dolosamente, lo que eventualmente se traducirá en perjuicios como discriminaciones, la imposibilidad de ejercer algún derecho, o la pérdida de algún beneficio.

Conceptualmente, un *dato* es un antecedente que da cuenta de un hecho o de una característica determinada. Es además una unidad básica de información.

El conjunto organizado de datos constituye *información* y, sociológicamente hablando, es un nuevo bien económico de alto valor y una forma de poder.

Un dato es *personal o nominativo* cuando permite identificar cualquiera característica de una persona para relacionarse en sociedad, por ejemplo al consignarse en una guía de teléfonos datos generales, o cuando son de mayor importancia o sensibilidad como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, la mayor o menor riqueza, las operaciones comerciales que se realizan, las acciones en empresas que se poseen, los depósitos en cuenta corriente o a plazo, los impuestos pagados, etcétera.

Se presenta un conflicto que surge entre tres intereses relevantes.

Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc.

Por otra parte, se presenta un interés –también muy legítimo- que poseen los gobiernos y los particulares para acceder a cierta información: …los Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quienes tienen SIDA al momento de fijar políticas de salud; y los particulares, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

Modernamente se ha visualizado una tercera garantía, a saber, la que posee todo ciudadano para, en aras de la transparencia y probidad de la gestión estatal, acceder a la información sobre actos, contratos, documentos, resoluciones, licitaciones y otros similares que respaldan y dan cuenta de la actividad de los órganos de la Administración del Estado -v.gr subsidios asignados, fundamentos de las adjudicaciones en licitaciones, remuneraciones pagadas y calificaciones aplicadas a los funcionarios, etcétera-, y esa información puede -y de hecho lo hace- contener antecedentes nominativos, personales e incluso sensibles -v.gr nombres de los beneficiarios de los subsidios, nombres de los funcionarios calificados, identidad de las empresas adjudicadas, etcétera-.

Se trata, por ende, de lograr un equilibrio y establecer límites entre el derecho a la intimidad que consagra el artículo 19 N°4 de la Constitución y los derechos de acceso a la información consagrado en los artículos 19 N°12 y 8° de la Carta Fundamental.

La interrogante a dilucidar o la hipótesis de trabajo, en consecuencia, puede ser 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 por cierto, 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 determinados datos personales, sea para fijar políticas de salud o para evitar la morosidad comercial, esto no puede traducirse, al extremo, en abusos contra las personas o titulares individualizados por sus antecedentes.

Los órganos estatales que a partir de nuestro número de identificación nacional procesan información personal, se han preocupado de aclarar que ellos sólo estarían manejando o procesando ciertos *"datos públicos"*. Esto es delicado, porque el límite entre *"la esfera privada"* y *"la esfera social o pública"* de una

persona no se ha establecido legalmente con claridad, y porque el problema de los cotidianos atentados contra la vida privada, la igualdad laboral, la igualdad ante la ley y la libre iniciativa en materia económica -para nombrar algunas garantías fundamentales afectadas- surge cuando se cruzan computacionalmente y con toda facilidad antecedentes personales y se elaboran perfiles.

En la medida que un particular consienta o una norma legal establezca -en Chile lo hace la ley 19.628- que ciertos datos o antecedentes personales sean susceptibles de conocerse[24], éstos pasarán a formar parte de una *"esfera social o pública"* porque lo vincularán con la sociedad.

En el caso contrario, esto es, si cada titular de los datos que lo individualizan opta por mantenerlos reservados o no existe una ley que por razones de orden público permita expresamente conocerlos[25], tales antecedentes, que les pertenecen[26], serán parte de una *"esfera íntima o reservada"*, que no puede ser atisbada, procesada o conocida por particulares, por empresas que quieran comercializarlos e incluso por órganos estatales. Dichos datos en Chile están protegidos por la esfera íntima que consagra la Garantía del artículo 19 N°4 de la Constitución, y a esta esfera privada de los administrados también alude expresamente el artículo 21 N°2 de la ley 20.285.

Ningún órgano de la Administración en Chile podría reivindicar o atribuirse la propiedad de la información nominativa que trata o procesa. Así lo hacen, por ejemplo, una empresa chilena que ofrece productos de bases de datos en Internet (v.gr. guías de empresas) o el ente universitario (pero comercial) administrador de los nombres de dominio (www.nic.cl), que advierten en sus páginas web que están otorgando el derecho de accesar a sus bases exclusivamente a modo de consulta y que el contenido de las bases de datos es de su propiedad y está protegido por el derecho de autor. Estas afirmaciones constituyen un error jurídico, toda vez que son cosas muy distintas *"el continente"* o la estructura de la base o banco de datos que *"el contenido"* o la información almacenada en el mismo[27].

---

[24] Pensemos en los siguientes datos: número de teléfono; profesión; filiación política; origen étnico; situación laboral; cotizaciones previsionales; monto de impuestos declarados; créditos bancarios obtenidos; viajes realizados; valores transados en la Bolsa; participaciones en sociedades; etcétera.

[25] Tal es el caso del prontuario o registro de condenas, de la base de datos del Servicio de Registro Electoral, del Boletín Comercial de la Cámara de Comercio de Santiago, etcétera.

[26] A propósito de los datos patrimoniales, desde 1929 a la fecha la Superintendencia de Bancos ha sostenido que uno de los atributos del dominio lo constituye la facultad exclusiva del dueño para permitir o impedir a terceros que se impongan o no de sus negocios.

[27] Las normas internacionales de mayor importancia que aluden al tema, a saber, el acuerdo TRIP del GATT y la OMC adoptado en 1994 en Marrakech sobre aspectos de la propiedad intelectual relacionados con el comercio (Anexo 1C, artículo 10º), la Directiva de la Unión Europea 96/9/CE de 1996, y el Tratado sobre Derecho de Autor de la OMPI adoptado a fines de 1996 en Ginebra (artículo 5º), establecen claramente que la Propiedad Intelectual ampara a las compilaciones de datos cuya selección o disposición de contenidos sean creaciones originales, y señalan expresamente que dicha protección autoral no abarca a la información compilada o "a los datos en

Se produce -doctrinaria y legalmente- la conciliación entre el Derecho a la Intimidad y el Derecho a la Información a través del control que para el titular de los datos posibilita el denominado *Derecho de Acceso* o *Habeas Data,* (i) una nueva garantía fundamental (o un mecanismo de resguardo y tutela) que contemplan en el Derecho Comparado tanto algunas Cartas Fundamentales como las llamadas Leyes de Protección de Datos, y (ii) una consagración concreta del llamado "*Principio de la Autodeterminación Informativa".*

El *Habeas Data* es una acción cautelar de rango constitucional pero en Chile sólo legal, heredera de otro recurso tan importante como el *Habeas Corpus*, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales -al decir de una sentencia histórica del Tribunal Constitucional alemán- "*autodeterminar"* el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente.

¿Cómo concilian las leyes de protección de datos los intereses involucrados?. Básicamente de la siguiente forma:

(i) no se niega la posibilidad del procesamiento o tratamiento de datos, pero se consagran facultades de acceder, corregir, actualizar o eliminar datos para los titulares de los mismos (enmarcadas en el denominado *Habeas Data*);

(ii) se establecen mayores limitaciones para el procesamiento cuando los datos son de especial relevancia como los llamados "sensibles" o "personalísimos" (vida sexual, salud, raza, credo religioso, filiación política, etcétera);

(iii) se regula separadamente el procesamiento que realice un órgano público, una persona natural o una persona jurídica, estableciendo diferentes requisitos de constitución;

(iv) se regulan acabadamente las obligaciones y prohibiciones del responsable de un sistema;

(v) se radica la operatividad de todas las normas en un órgano autónomo de control y fiscalización, "a priori" -autorizando a procesar y fijando los requisitos para hacerlo- y "a posteriori" -conociendo de los reclamos y sancionando-; y,

---

sí mismos". Las empresas aludidas sólo pueden considerarse propietarias intelectuales del diseño y estructura original del fichero computacional, mas por el hecho de recopilar antecedentes sobre personas naturales y jurídicas, procesarlos, seleccionarlos, organizarlos o almacenarlos no se transforman -porque no existe título ni modo de adquirir alguno- en dueñas de la información nominativa que individualiza a otras personas, de manera tal que posteriormente puedan comercializarla libremente (sobre todo cruzada o en forma de "perfiles"). Incluso más: el carácter de depositarias o tenedoras de datos personales les impone obligaciones de confidencialidad y reserva, tan importantes como aquellas que emanan del secreto estadístico o del secreto bancario.

(vi) se configuran sanciones administrativas y penales para el caso que las normas de la ley no se cumplan.

Todas las *"Data Protection Act"* tienen la siguiente estructura, a saber, una parte dogmática, una parte orgánica, una parte procedimental y una parte sancionatoria o represiva. Revisemos brevemente esta estructura:

(i) Parte Dogmática: Comprende los conceptos esenciales; principios inspiradores; ámbito de aplicación; especies o categorías de datos protegidos; consagración del Derecho de Acceso o *Habeas Data* y de sus garantías derivadas; derechos, obligaciones, restricciones y prohibiciones para los responsables de los sistemas de tratamiento de datos personales; etcétera.

(ii) Parte Orgánica: Se refiere a la autoridad ad hoc independiente, técnicamente competente y con facultades normativas, de control y fiscalización a priori y a posteriori, y sancionatorias sobre los responsables de los bancos de datos personales; alude a la existencia de un registro público de los responsables y los bancos de datos; etcétera.

(iii) Aspectos Procedimentales: Se regulan instancias de reclamos de rápida y breve tramitación y fallo ante el órgano ad hoc (agotamiento previo de la vía administrativa); se contempla la posibilidad de interponer recursos posteriores ante los tribunales superiores de justicia; etcétera.

(iv) Parte Represiva o Sancionatoria: Incluye la cancelación de la autorización de funcionamiento y eliminación del registro; multas; tipificación de delitos; etcétera.

1.2 *El contenido específico de la ley 19.628 de 1999.*

(i) La ley 19.628 consta de un Título Preliminar sobre Disposiciones Generales (artículos 1º, 2º y 3º); de un Título I sobre la Utilización de Datos Personales (artículos 4º al 11º); de un Título II sobre Derechos de los Titulares de Datos (artículos 12º a 16º); de un Título III acerca de la Utilización de Datos Personales relativos a Obligaciones de Carácter Económico, Financiero, Bancario o Comercial (artículos 17º a 19º); *de un Título IV sobre Tratamiento de Datos por Organismos Públicos (artículos 20º, 21º y 22º);* de un Título V acerca de la Responsabilidad por las Infracciones a esta Ley (artículo 23º); de un Título Final que modifica el Código Sanitario (artículo 24º); y de tres disposiciones transitorias.

(ii) En esencia, para la ley 19.628 existen "*datos personales*" o nominativos que le pertenecen a sus titulares, a los que conciernen y a los que permiten que sean identificados o identificables, y que son "*tratados*" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "*responsables del registro o banco de*

datos". No importa el soporte en que se contengan, informático o manual, o que sean imágenes o representaciones de caracteres biométricos como la huella digital o el iris. Sólo le importa a la ley 19.628 que ellos se refieran a personas naturales o físicas -no a las fictas o jurídicas-, identificadas e identificables o determinables a futuro.

(iii) La regla general formalmente declarada por el artículo 4° del texto legal es que dicho "*tratamiento de datos personales*" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "*fuentes de acceso público*" (por lo cual no se requiere de autorización para su tratamiento) y se consagran importantes y amplias excepciones sobre todo en materia de datos "*personales-patrimoniales*", lo cual transforma a la regla general en una mera declaración de principios.

(iv) El mecanismo de resguardo recogido parcialmente del Derecho Comparado también se denomina *Derecho de Acceso* o *Habeas Data*, y éste, después de ejercerse ante quien aparezca como responsable sólo puede reclamarse ante los tribunales ordinarios de justicia, en conformidad al artículo 16° de la ley.

(v) En cuanto al *ámbito de aplicación de la ley*, es el artículo 1º el que establece que se sujetará a las disposiciones de esta ley *el tratamiento de los datos de carácter personal*, definidos por el artículo 2° como los relativos a cualquier información concerniente a *personas naturales identificadas o identificables*, contenidos en registros o bancos de datos procesados tanto por organismos públicos como por entidades particulares.

No estamos frente a una ley relacionada sólo con el procesamiento computacional de datos. Porque el artículo 1° no utiliza la expresión "*tratamiento automatizado*", y porque la letra o) del artículo 2º define muy ampliamente como "*tratamiento de datos*" a "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no...", claramente quedan comprendidos aquí todos los registros, *cardex* o ficheros manuales o soportados en papel, por cierto, hoy en día de menor importancia cualitativa y cuantitativa que los registros informáticos.

Como corolario y sentando algo así como un principio de legalidad o una especie de condición general de licitud para este ámbito, agrega el artículo 1º que cualquier persona podrá efectuar el tratamiento de datos personales siempre que lo haga de manera concordante con la ley y para finalidades permitidas por el ordenamiento jurídico, y que en todo caso se deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la ley les reconoce.

El texto legal distingue lo que es el tratamiento o procesamiento de datos personales al interior de la Administración Estatal o en el Sector Público y lo que ocurre en el sector privado o respecto al tratamiento por particulares, sean personas naturales o jurídicas.

En doctrina y con un afán meramente explicativo, se ha distinguido entre un ámbito de aplicación *"subjetivo"* y otro ámbito *"objetivo o material"* de la ley 19.628.

El primero estaría determinado por los sujetos regulados por la ley, a saber, el responsable de un registro, base o banco de datos (que puede ser una entidad particular natural o jurídica y un servicio público) y que realiza el tratamiento de ellos; la persona natural -sólo ella- titular de los datos e individualizada por los antecedentes nominativos; una supuesta autoridad de registro que sería el Servicio de Registro Civil -y la calificación es *per se* errada, porque mantener un listado de bases de datos existentes sólo en organismos públicos, descartándose a los registros de naturaleza particular o privada, no implica -de modo alguno- asignarle la calidad de *"Autoridad"* fiscalizadora y garante del ejercicio de los derechos de los titulares de los datos nominativos-; y, terceros a los que eventualmente se les transfieran o comuniquen los datos personales, que no son regulados orgánicamente pero si mencionados en las disposiciones de la ley.

El ámbito de aplicación objetivo o material, por su parte, derivaría de la amplia, comprensiva o genérica definición de tratamiento de datos personales, y comprendería tanto a las operaciones o procedimientos técnicos de tratamiento automatizado de datos personales como a las realizadas manualmente o sin sistemas informáticos, que permitan usar *"de cualquier forma"* y relacionar los datos nominativos entre sí.

El artículo 2° letra o) menciona operaciones concretas sólo a título de ejemplo, a saber: *recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir y cancelar* datos personales; y el mismo artículo pero en la letra m), agrega, dentro de las opciones posibles, la operación consistente en *"relacionarlos"* entre sí cuando estén almacenados en una base o banco de datos.

(vi) La ley aprobada distingue *distintas categorías de datos*, sin un tratamiento sistemático en el cuerpo legal. Algunas, como veremos, se definen en el artículo segundo. Otros fueron mencionados en los respectivos debates parlamentarios.

El concepto esencial y genérico es el de *dato personal*, que es *"el relativo a cualquier información concerniente a una persona natural, identificada o identificable"*. El se opone o es radicalmente diverso al dato *"estadístico"*, disociado e innominado, que -en síntesis- no permite individualizar a persona alguna o no pueden ser asociados a su titular de manera de poder identificarlo, y que por ende quedan fuera de la institucionalidad jurídica de la ley 19.628.

Revisten especial importancia los conceptos de datos personales *"sensibles"*, personales *"patrimoniales"* o económicos, financieros, bancarios o comerciales, pudiendo estos últimos ser positivos -referidos en el artículo 4° inciso quinto- o negativos -sobre mora, protestos o insolvencia-, que son los regulados en los artículos 17, 18 y 19 pero sólo de cara a su comunicación a terceros-.

El artículo 2º define 16 conceptos, no siendo las definiciones lo suficientemente claras. Respecto de los datos se define cuando son *"caducos"*[28], no verdaderos, no pertinentes o no necesarios, "*estadísticos*"[29], "de *carácter personal"*[30] o personal *"sensible"*[31]. Respecto de las actividades de las que pueden ser objeto los datos personales, el término más amplio que se define es "*tratamiento de datos"*[32], y derivados de este, los conceptos de *"almacenamiento*"[33], "*bloqueo*"[34], "*comunicación o transmisión*"[35], *"eliminación o cancelación"*[36], *"modificación*"[37] y *"procedimiento de disociación"*[38]. En relación a lo que podemos denominar la infraestructura del procesamiento de datos personales, el artículo define lo que es un "*registro o banco de datos",* el *"responsable del registro o banco de datos"*, el *"titular de los datos"* y los *"organismos públicos*".

(vii) Nada dice la ley sobre el *tratamiento de datos personales de las "personas jurídicas",* donde sus representantes legales serían los titulares de la protección de datos personales y quienes podrían ejercer el derecho de acceso y

---

[28] Conforme lo establece la letra d) del artículo 2º, *"dato caduco"* es el que -en consideración a su calidad o cualificación- ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

[29] Letra e): ...dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

[30] Letra f): ...datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

[31] 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 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.

[32] Es cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

[33] Se entiende por tal la conservación o custodia de datos en un registro o banco de datos.

[34] Consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

[35] La comunicación o transmisión de datos consiste en dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

[36] Es la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

[37] Consiste en todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

[38] Se entiende por tal a todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

sus derivados en conformidad a los artículos 12 y ss. de la ley 19.628. El legislador de la ley 19.628 habría querido entender que la privacidad, la intimidad o la vida privada son sólo atributos, garantías o derechos de las personas naturales.

Debe reconocerse que el punto no es unánime sino discutido en el Derecho Comparado, sobre todo para quienes consideran que existen otros mecanismos jurídicos para resguardar los atributos de las personas jurídicas, a saber, el derecho de sociedades, las leyes sobre propiedad industrial e intelectual, las normas sobre libre competencia, etcétera, todas las cuales, empero, de manera alguna resguardan el eventual tratamiento abusivo que se haga por las empresas que prestan servicios de información.

Pero las personas jurídicas también poseen atributos de su personalidad, aunque su naturaleza jurídica emane de una ficción legal. Ellas son sujetos de información cuyos antecedentes también son “tratados” computacionalmente, y por definición quedan al margen de la ley que sólo rige en relación a “titulares” personas naturales. Ocurre que la información sobre las personas jurídicas es tan relevante como la de las personas naturales y también merece ser resguardada[39].

(viii) *¿Es la ley 19.628 una norma que carece de los contenidos dogmáticos, orgánicos, procedimentales y sancionadores mínimos que una data protection act contiene y requiere?.*

Si desde la perspectiva de la estructura de las leyes de protección de datos, todas poseen una estructura que puede ser resumida en 4 partes: una dogmática, una orgánica (para que lo dogmático no sean meras declaraciones de principios), una procedimental y una sancionadora, la ley 19.628 posee una parte dogmática débil, no tiene parte orgánica, no contempla procedimientos administrativos de tutela sino uno judicial, y no posee un arsenal sancionador adecuado.

La ley 19.628, salvo en lo relacionado con los plazos de publicación de datos sobre mora y protestos -donde es conocida como "*La Ley Dicom"*-, por sus errores de forma y de fondo y por sus insuficiencias no ha tenido casi ninguna aplicación práctica. La gente no la conoce ni percibe su importancia cotidiana, la gente no la utiliza, no existen procedimientos judiciales relevantes o de impacto público de Habeas Data en curso, no existe un registro obligatorio para evitar el

[39] Esta tutela jurídica por ende permanece en el ámbito de las reglas generales del derecho, por lo que cualquier persona jurídica respecto de la cual se abuse de sus antecedentes propios o bien éstos sean procesados en forma errada (datos obsoletos, caducos, inexactos), deberá recurrir a los procedimientos, acciones y recursos generales contemplados en nuestro ordenamiento jurídico. Estimamos que si bien en menor amplitud que las personas naturales, las personas jurídicas también gozan de un necesario derecho a la confidencialidad o reserva de los antecedentes que a ellas se refieren, por cuanto éstos las convierten en sujetos de derechos y en personas identificadas e identificables.

tráfico anónimo de los *"list brockers"* (en Francia, procesar sin estar registrado es delito penal desde 1978) y no existe un órgano administrativo al cual reclamar en forma sumaria y eficaz[40].

2. Un presupuesto esencial para el tratamiento de datos personales en los servicios públicos.

De cara al sector público -y para respaldar su actuación en materia de tratamiento de datos personales- el estudio inicial debe centrarse en el análisis de tres artículos de la ley 19.628, a saber, el 2°, el 4° y el 20°.

En resumen, (i) el *artículo 2°* establece que en Chile la regla general son las llamadas *"fuentes públicas de información"*[41], a saber, las que no sean de acceso restringido o reservado como las cubiertas por el secreto bancario, el secreto tributario, el secreto de filiación política, el secreto estadístico o el secreto sanitario de archivos y exámenes de salud; (ii) el *artículo 4°* consagra -por la vía de las excepciones- un enorme caudal de información nominativa que por provenir de fuentes públicas puede tratarse legalmente sin autorización de los titulares individualizados y propietarios de los datos personales; y, (iii) el *artículo 20°* es perentorio para establecer que un servicio público, actuando dentro de su competencia, no requiere autorización de los ciudadanos para tratar los datos personales que le toque procesar en el marco propio y exclusivo de dicha competencia de Derecho Público.

Estas normas, aplicadas a los servicios públicos, no son abusivas, injustas o perjudiciales para los ciudadanos, como si ocurre en el sector privado, que ha resultado no regulado, no acotado y no fiscalizado idóneamente con la vigencia y las disposiciones de la ley 19.628. Estas normas, por el contrario y como ha dictaminado la Contraloría General de la República posibilitan y habilitan que el Estado cumpla adecuadamente los fines promocionales y asistenciales que le son propios incluso celebrando convenios de intercambio de bases de datos[42].

A modo de anticipo: la Contraloría el año 2001 en un Dictamen 10.322 expresamente alude a la facultad de los servicios públicos para, con el fin de

---

[40] A nuestro parecer, el cambio de una breve pero amplia moción senatorial del año 93 -mediante la cual sólo se buscaba sancionar civilmente algunas intromisiones ilegítimas a la privacidad y consignar algunos principios en materia de protección de datos personales en el ámbito de su procesamiento informático-, a la actual norma vigente -fruto de una indicación presentada en la Cámara de Diputados-, en definitiva fue un aporte parcial que nació trunco de cara a las disposiciones más relevantes de una verdadera ley de protección de datos.

[41] Cuestión esencial será la de determinar si los registros, bases y bancos de datos de los órganos de la Administración son susceptibles de ser calificados como *"fuentes públicas de información"*, en el contexto por cierto de la ley 19.628 y no, digámoslo desde ya, de la ley 20.285 sobre acceso y transparencia de la información administrativa.

[42] Véase la letra D de esta Parte Primera del Informe.

cumplir sus obligaciones de asistencia y bien público, comprender dentro del *"tratamiento"* de datos personales el "*celebrar convenios de intercambio de información"*; esto es, reconoce que poseen facultades amplias para celebrar contratos relacionados con el cumplimiento de sus fines del servicio público, a propósito de datos personales o de información nominativa que sea *per se* pública y no secreta o reservada.

Cuestión esencial será, lo reiteramos, establecer si las bases o bancos de datos personales o nominativos que mantienen los servicios públicos deben ser consideradas legalmente como *"fuentes de acceso público"* o como *"fuentes de acceso reservado o secreto"*. Creemos -dicho a modo de anticipo- (i) que la respuesta sólo puede determinarse considerando la especial naturaleza del dato personal o nominativo tratado[43], y (ii) que por regla general los STDP del sector público no deben ser considerados fuentes accesibles al público o fuentes públicas de información nominativa, a pesar de la amplitud de la definición legal del artículo 2° de la ley 19.628[44].

3. El Título IV de la ley 19.628: "Del tratamiento de datos por los organismos públicos".

El artículo 2º letra k) define lo que son los Organismos Públicos, entendiendo por tales a *"las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado"*.

Respecto a las *bases de datos públicas o administradas por organismos públicos*, la ley contempla un Título específico, compuesto por los artículos Nº20, 21 y 22.

Disponen los artículos 20 y 21:

> *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.*
>
> *Artículo 21. Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o*

[43] En consecuencia, si por ejemplo es un dato personal sensible o sujeto a secreto tributario o estadístico, siempre estará no almacenado en fuentes públicas.

[44] La letra i) las define como los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Exceptuase los casos en que esa información les sea solicitada por los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7º, 11 y 18.

Los órganos de la Administración del Estado sólo pueden procesar todo tipo de datos personales de los ciudadanos actuando dentro de su competencia de Derecho Público y para fines de servicio público. Si así lo hacen y a diferencia de los responsables de bases de datos particulares o del sector privado, la ley los releva de la necesidad de la autorización del titular de los datos para el tratamiento que establece el artículo 4°,

Todo responsable de bases de datos de un servicio público debe, además de cumplir con la norma general del artículo 20 en cuanto a tratar computacionalmente datos personales *"sólo dentro de su competencia exclusiva",* respetar la totalidad de las otras normas de la ley 19.628. A ello se refiere la ley cuando menciona *"a las reglas precedentes"* al Título IV.

La determinación de cuál es la concreta competencia exclusiva de un servicio público será una cuestión que deberá resolverse caso a caso o servicio a servicio, y en consideración a diversas normas especiales, como por ejemplo las Leyes Orgánicas de cada uno. Lo ideal, para evitar cuestionamientos o dudas interpretativas, es que las normas legales especiales confieran expresamente la competencia para el tratamiento de datos personales al órgano público.

Se menciona como ejemplo conflictivo al SERVEL, a cuyo respecto nadie podría discutir su facultad para tratar y mantener registros con los padrones electorales, pero de cara a la venta o cesión de esos padrones en el último tiempo ONG como *Proacceso* han cuestionado abiertamente sus facultades y/o competencias de Derecho Público en este sentido.

Si un servicio público actúa y trata datos nominativos fuera de las materias de su competencia incurriría en una causal de ilegalidad y de nulidad de derecho público. Es la Constitución Política en el artículo 7° la que establece (i) que los órganos del Estado actúan válidamente previa investidura regular de sus integrantes, dentro de su competencia y en la forma que prescribe la ley; (ii) que ninguna magistratura puede atribuirse ninguna otra competencia, autoridad o derechos que los que expresamente se les hayan conferido en virtud de la Constitución y las leyes; y, (iii) *que todo acto en contravención a este artículo es nulo.*

Por tratarse la ley 19.628 de una norma de Orden Público que instrumentaliza el resguardo de una garantía constitucional y concreta el principio de la Autodeterminación Informativa, no es factible que mediando una simple autorización de los ciudadanos titulares de los antecedentes nominativos -y a falta de una autorización legal- los servicios públicos inventen nuevas competencias para, en esos ámbitos ajenos a su competencia exclusiva, realizar tratamientos de datos personales.

Respecto al Título IV de la ley, cabe preguntarse por el alcance de la expresión "*organismos públicos*". Semánticamente cabe pensar que se trata de todos los órganos o poderes del Estado, y que por ende se regula en él el tratamiento de datos personales por el Ejecutivo, por el Legislativo y por el Poder Judicial. Y si la ley no distingue, no es lícito al intérprete distinguir. De lo que establece el artículo 21, en él los tribunales de justicia son expresamente calificados como organismos públicos. Y desde el punto de vista de fondo, el mismo artículo alude a una función que realizan los tribunales, esto es, el tratar datos personales o nominativos relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias.

Ergo, el Servicio de Registro Civil debiera considerar en su listado a los Tribunales de Justicia, lo cual -por cierto- nada aporta desde el punto de vista de dar certeza, publicidad y transparencia al sistema de tratamiento de datos personales en Chile, y paralelamente, ninguna facultad fiscalizadora posee el Registro Civil para el evento –por ejemplo- de un tratamiento indebido de datos personales por el Poder Judicial.

4. Análisis de la competencia que el artículo 22 de la ley y su Reglamento le asignan al Servicio de Registro Civil. Acerca del rol "no fiscalizador" del Registro Civil.

Señala el artículo 22:

Artículo 22. El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.

Cabe destacar al inicio que el artículo 22 contempla la obligación de que sea el Servicio de Registro Civil el ente que llevará un *Registro Público de Bancos de Datos Personales a cargo de organismos públicos*, pero sólo en relación a entes estatales y excluyendo de la obligación de registro a las empresas particulares. La carga legal se agota en la confección y mantención del registro público, porque el Servicio de Registro Civil no almacena ni accede a los *"contenidos"* de esos *"continentes"* llamados bases o bancos de datos.

Esta disposición, fruto de una indicación presentada por el Ejecutivo durante el debate en Comisión Mixta ya que se trata de una materia de iniciativa exclusiva del Presidente, es de difícil comprensión, porque en sí no lleva envuelta el establecer una instancia o grado de fiscalización alguno, que es la razón de ser en las leyes de protección de datos de la existencia de órganos ad hoc[45].

¿Cuáles son las sanciones a aplicar al órgano público que no se registre?; ¿puede el Servicio de Registro Civil realizar algún control al efecto y con qué facultades, si en Derecho Público sólo puede hacerse aquello que esté expresamente permitido?.

A esta fecha todos los servicios públicos debieran haber dado cabal cumplimiento a lo establecido tanto en el artículo 22 de la ley 19.628 como en su Reglamento, que mandata al Servicio de Registro Civil para llevar un registro de los bancos de datos personales a cargo de organismos públicos, registro que es de carácter público y al cual el organismo público responsable del banco de datos debe proporcionar una serie de antecedentes cuando se inicien las actividades del banco, y comunicar cualquier cambio de los elementos dentro de los quince días desde que se produzca.

Que ello no haya ocurrido, aún cuando en el hecho no es tan grave por cuanto los servicios públicos no tratan datos en forma anónima o clandestina y las personas saben que pueden ejercer el Habeas Data del artículo 12° de la ley 19.628 contra cualquier servicio público, es una muestra clara de lo inoperancia y de la insuficiencia de la normativa.

Que ello no haya ocurrido se ha cuantificado y ha sido objeto de denuncias públicas. Como comentamos a pié de página en la Introducción del Informe, entre Septiembre y Diciembre del año 2009 se realizó un estudio a partir de un cuestionario de siete preguntas enviado a 164 servicios, programas o beneficios de los ministerios de Vivienda, Salud, Educación, Trabajo y Planificación, y el Servicio Nacional de la Mujer. Dentro de sus conclusiones se constató: (i) que el 97% de 164 servicios públicos vulneraba la norma de protección de datos

[45] Para entender la importancia y la operatividad práctica del tema, véase en Internet la dirección *www.ag-protecciondatos.es/regis.html,* que conecta con el Registro General de Protección de Datos existente desde 1992 en España.

personales, porque ellos no entregaban los antecedentes que exigen el artículo 22 de la ley 19.628 y su Reglamento, al Registro Civil; y, (ii) que sólo el 3% de las reparticiones dependientes de los ministerios sociales tienen inscritas las bases de datos con información de ciudadanos que usan en sus entidades[46].

De manera particular, y reiterando lo que disponen los artículos 2° y 3° del Decreto Supremo N°779 de Noviembre del año 2000 (el Reglamento de la ley 19.628)[47], a todos los servicios públicos el Registro Civil les ha pedido -sin facultad de apercibir y coaccionar aplicando sanciones- informar en relación a cada uno de sus bancos o bases de datos personales acerca de su nombre, el fundamento jurídico específico de su existencia, su finalidad, la naturaleza de la información personal almacenada o del tipo de datos (personal o nominativa, sensible, estadística, sujeta a secreto o reserva, patrimonial, financiera, sobre seguridad nacional, etcétera), y el universo (cantidad y naturaleza) de las personas o ciudadanos individualizados o identificados en el sistema.

Lo esencial del reparo jurídico que es procedente hacer apunta a cuestionar la opción de Política Pública subyacente en la ley 19.628. Da la impresión, en definitiva, que derechamente no existió tal definición previa. Parafraseando el Mensaje del referido Boletín 6120, ya en 1999 y para velar por el adecuado cumplimiento de las nuevas disposiciones relativas al tratamiento de datos personales se requería una autoridad dotada de competencias y herramientas eficaces, para dictar normativas sobre la materia, para fiscalizar, para adoptar medidas de resguardo y para sancionar los incumplimientos mediante la aplicación de multas.

En efecto, al no haberse contemplado un organismo administrativo, Agencia o Superintendencia que se encargara de velar por el cumplimiento de sus normas, limitándose a entregar al Registro Civil e Identificación el deber formal de llevar un registro de las bases de datos a cargo de organismos públicos como una simple medida de publicidad, era imposible fiscalizar el cumplimiento de las normas de la ley y muchas de sus disposiciones se hicieron ineficaces.

---

[46] La ONG que realizó el estudio, lo reiteramos, calificó como *"un panorama preocupante"* el que existiera un escaso cumplimiento de la ley sobre protección de datos y vida privada, porque de los 50 servicios que respondieron formalmente hubo 39 que reconocieron tener bases de datos personales, y de ésos solamente 5 habían cumplido con su deber de registrarlas ante la entidad correspondiente, que es el Registro Civil.

[47] El Decreto 779 consta de cuatro Títulos. El primero, se refiere a las inscripciones en el Registro de Bancos de Datos Personales; el segundo, a las obligaciones de los organismos públicos responsables de bancos de datos personales; el tercero, a los informes que el Registro civil otorga a todo aquel que lo solicite acerca de un banco de datos determinado; y el cuarto, sobre las correcciones y modificaciones a las inscripciones.

Debe entenderse que en 1999 el legislador no entendía los alcances del problema. Consta en las Actas del debate en Comisiones, que entre otras razones se descartó contemplar la existencia de una Autoridad de Protección de Datos *"para no ser burocráticos",* y que en otra, incluso se debatió acerca de la posibilidad -carente de toda lógica práctica y jurídica- que fuera la Contraloría General de la República la que asumiera este rol.

Ergo, la opción de darle la competencia meramente formal y anodina desde el punto de la fiscalización y las facultades que le son propias en la legislación comparada a las Autoridades de Protección de Datos al Servicio de Registro Civil, quien sólo mantiene un registro de las bases de datos personales del sector público meramente informativo, se acercó -a nuestro parecer- al ámbito de lo que en Derecho Administrativo o Constitucional se conoce como *"la irresponsabilidad del Estado Legislador",* porque en definitiva los únicos perjudicados a la fecha han sido los ciudadanos y/o administrados.

Por cierto, las primeras propuestas acerca de la necesidad de crear para Chile una institucionalidad orgánica relacionada con el procesamiento computacional de datos personales o nominativos las formulamos en 1990-92[48]. Propusimos en aquel entonces la necesidad de reflexionar acerca de la importancia de otorgar a la intimidad, frente a los abusos derivados de la informática, una protección o resguardo "*extrapenal"* -no fue adecuada la denominación, por cierto-. Concretamente, nos preguntamos si estábamos ante una oportunidad para introducir en Chile la institución del *Ombudsman* o Defensor del Pueblo, o si era conveniente la creación de una Superintendencia de Bases y Bancos de Datos.

¿Qué es lo que no puede hacer el Servicio de Registro Civil?; ¿cuáles son las competencias que no posee y que por ende no se le puede conferir la calidad de Autoridad de Protección de datos?.

Parafraseando al contenido del Boletín 6120 que a esta fecha está modificando la ley 19.628, dichas competencias serían, por ejemplo:

(i) mantener un Registro Único Nacional de Bases de Datos;

(ii) fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estimara pertinente;

(iii) inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley;

[48] JIJENA, Renato (1990-92), páginas 62 y ss.

(iv) requerir la inscripción de los bancos de datos que no estén registrados en el Registro Único Nacional;

(v) dictar instrucciones de carácter general o particular respecto de las condiciones de legitimidad de un tratamiento de datos;

(vi) conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos de protección de datos;

(vii) ejercer potestades sancionadoras contra los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos; y,

(viii) requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro.

Cabe hacer una referencia, sobre la cual volveremos en el acápite G de la Parte Segunda de este Informe, acerca de la relación de este artículo con lo dispuesto en los artículos 10° y 33 letra m) de la ley 20.285, que establece el acceso a la información administrativa el primero y que mandata al Consejo de Transparencia para velar por la aplicación de la ley 19.628 en el sector público el segundo.

Sobre la competencia del Consejo, debe tenerse presente que ella no significa que pueda asumir como propias las competencias que la ley 19.628 asigna al Registro Civil; antes, muy por el contrario, significa que el Consejo debiera instruir a los servicios públicos para que den cumplimiento a la obligación de registro, en los términos establecidos por el Decreto Supremo 779 que reglamenta este artículo 22.

Y en cuanto al artículo 10°, a nuestro parecer él no es la vía jurídica para acceder al contenido específico de estas bases de datos que administra el Registro Civil, salvo que se quiera conocer acerca de la existencia y el estado del Registro Público, u objetar un informe o certificado específico que administrativamente o mediante un acto administrativo haga el Registro Civil acerca del listado de bases de datos de los servicios públicos que administra.

En primer lugar, porque la información se encuentra disponible en la página web del Registro civil -cuestión de hecho-, y en segundo lugar, porque cuando el artículo 10° alude a *"toda otra información del Estado"* esa mención no puede extenderse a los datos personales o nominativos de los ciudadanos. Aunque por cierto, como consignamos, el Servicio de Registro Civil no conoce de modo alguno el contenido concreto de las bases de datos, sino sólo las descripciones e informaciones que los propios órganos de la Administración le remiten.

De hecho, el propio Servicio informa que él no posee información actualizada porque no mantiene el control acerca de la creación, la posible modificación o la eliminación de una base o banco de datos nominativos.

5. Aplicación de la regla general del artículo 4° a los servicios públicos.

5.1 Ubicada en el Título I sobre la utilización de datos personales, se trata de la norma más conflictiva y confusa, misma que, en nuestra opinión, es clave para entender que estamos frente a una normativa que apuntó a proteger y legalizar el negocio del procesamiento de datos personales desde la perspectiva de las empresas del ramo, más que a resguardar los derechos de los titulares a quienes aluden o a quienes se refieren los datos personales o nominativos.

El artículo sienta un principio general en materia de procesamiento de datos personales, el que, atendidas las excepciones que luego consagra, no es sino una mera declaración de principios.

Señala que *el tratamiento de los datos personales sólo podrá efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o cuando el titular consienta expresamente en ello*.

Respecto a la *autorización* mediante la cual el titular de los datos personales consiente expresamente en el *tratamiento,* señalan los incisos segundo, tercero y cuarto que tanto su otorgamiento como su revocación deben *constar por escrito*[49], que la revocación se produce sin efecto retroactivo, y que la persona que autoriza debe ser *debidamente informada* respecto del propósito del almacenamiento de sus datos personales y de su posible "*comunicación"* al público. Como nada se dice, creemos que tal autorización podrá ser otorgada antes -en forma previa- o después de iniciado el procesamiento, con lo cual tendría lugar la denominada *ratificación*.

Fácil es concluir que dicha autorización del titular se transformará en una amplia cláusula tipo, especialmente en los contratos de adhesión[50].

---

[49] Entendiéndose además, en conformidad al artículo 3° de la ley 19.799 del año 2003, que homologa y hace equivalentes los soportes documentales o en papel con los magnéticos, electrónicos o digitales, que la exigencia de escrituración legalmente también resiste ser cumplida en forma electrónica, por ejemplo mediante un *email* o un *click* en un formulario llenado *on line* y que quede registrado en un *log* específico. Señala la ley que se si realizan actos por medios electrónicos ellos se reputarán como escritos, y la firma de la autorización podría verificarse o con mecanismos de PKI o criptográficos o con claves de acceso o password que, aplicadas, permitan identificar formalmente al titular de los datos que suscriba la autorización.

[50] Estas cláusulas no son ajenas al actual sistema financiero chileno. Así por ejemplo, en las Condiciones Generales de la solicitud de productos de una Financiera se señala que el solicitante faculta a la entidad "para proporcionar a sus empresas relacionadas todos los datos referidos a mi individualización que he facilitado en la presente solicitud de crédito, tales como nombre y

La ley 19.628 permite excepcionalmente el tratamiento, sin que sea necesaria la autorización del titular, cuando se trate de fuentes de datos personales accesibles al público, y, como hemos visto a propósito del artículo 20°, cuando el tratamiento lo realicen los servicios públicos actuando dentro de su competencia[51].

La norma consagra diversas excepciones en los incisos quinto y sexto, en relación a la autorización del titular requerida para el tratamiento de los datos.

Establece que en determinados casos no requiere autorización el tratamiento de datos personales que provengan o que se recolecten de *fuentes accesibles al público,* que son, por la ambigua definición del artículo 2°, la verdadera regla general que surge cuando a *contrario sensu* no sean de acceso secreto, restringido o reservado, como es el caso de los datos sujetos a secreto bancario, a secreto estadístico, a secreto tributario o sobre filiación política.

Dichas situaciones de excepción son, taxativa pero muy ampliamente formuladas, las siguientes:

a) Cuando los datos personales sean de carácter económico, financiero, bancario o comercial.

Esta excepción debe ser analizada distinguiendo entre datos patrimoniales *"positivos"* y *"negativos"* y en relación con lo dispuesto en los *artículos 17º, 18º y 19º* (Título III de la ley, únicamente referido a comunicación a terceros de datos personales patrimoniales negativos).

En materia de datos patrimoniales *"positivos",* relacionados con los ingresos, ahorros, gastos e inversiones de las personas, esta excepción legal sumada a la amplía definición de fuentes de acceso público, se puede estimar que es inconstitucional, toda vez que vulnera al artículo 19 N°4 de la CPE.

Distinto es el caso de los "*negativos"* o referidos a insolvencia, mora y protestos, los que, en atención al cuidado del orden público económico y a la luz

---

apellidos, estado civil, domicilio, profesión u oficio, Carnet de Identidad Nacional, Rut, y si fuera requerido para ello, lo faculto para informar a sus empresas relacionadas acerca de los depósitos y captaciones que mantengo y las obligaciones que he contratado...".

[51] Otras normas legales que permiten y regulan el tratamiento de datos personales son, por ejemplo, las Leyes Orgánicas de los servicios públicos, la ley 20.285 en casos de transparencia activa, la ley 19.970 que permite la creación de un registro de ADN, la ley que permite al Consejo de la Cultura crear un banco de datos personales, la ley 19.799 que obliga a los prestadores de servicios de certificación a tratar con confidencialidad los datos personales de sus clientes o signatarios y mantenerlos en bases de datos, la ley 20.120 sobre investigación científica en el ser humano; la ley 19.397, que establece la Autoridad Sanitaria y faculta al Ministerio de Salud para mantener registros o bancos de datos respecto de las materias de su competencia y tratar datos personales o sensibles; etcétera.

del artículo 19 N°12 de la CPE, sí deben poder ser procesados –con ciertos límites- y obviamente sin el requisito de la autorización previa de sus titulares. En consideración a éstos, y junto con no requerirse autorización para su tratamiento, el artículo 17 se encarga más adelante de precisar cuáles son los que específicamente o en qué casos los datos sobre incumplimiento de obligaciones pueden ser *comunicados* (concepto específico y modalidad de tratamiento) a terceros.

Particularmente grave es la no exigencia de autorización o consentimiento de los titulares de los datos para la actividad consistente en "tratar" (recopilar, procesar, almacenar, cruzar, comunicar, etcétera) antecedentes personales económicos, comerciales, patrimoniales y financieros positivos -que no dan cuenta de insolvencia patrimonial o de protestos-, quizás los más relevantes para las empresas de marketing directo, ya que la naturaleza o el contenido de la información que administran o su cartera de clientes es su principal activo.

b) Cuando los datos personales se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento.

La expresión *"tales como"* demuestra que se trata de una enumeración sólo ejemplar o *numerus apertus.* El uso de la expresión se traduce en que será una cuestión de hecho que en definitiva determinarán los tribunales para cada caso concreto sometido a su decisión, definir si un dato personal o nominativo es o no de aquellos contenidos en listados relativos a una categoría de personas que pueden ser tratados –con la amplitud de operaciones que involucra el término- sin autorización de sus titulares.

c) Cuando los datos personales sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

La ley aprobada, a diferencia de toda la legislación extranjera, legaliza con mínimas limitaciones el marketing directo. El artículo 4º en comento establece como amplia excepción y perentoriamente, que no se requiere autorización para el procesamiento de datos personales que provengan de fuentes públicas cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, lo que, sumado a las dos excepciones anteriores o perfilados con los datos a que ellas aluden, declara exento de autorización o control para el titular a un cúmulo demasiado grande de datos nominativos o personales[52].

[52] Difícil tarea tendrán los congresistas que impulsaron la ley para explicar en el futuro la razón de que frente a una actividad esencial para las empresas de marketing directo y que sólo persigue fines de lucro o comerciales, inconstitucionalmente optaron por impedir que los chilenos

d) Cuando el tratamiento de datos personales lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

5.2 Los servicios públicos sólo pueden procesar, tratar, comunicar o publicar los datos cuando una ley los faculte expresamente, o porque, no habiendo autorización legal, previamente obtienen autorización expresa y fundada para ser tratados asociados al nombre de los ciudadanos (*no en forma desagregada o estadística, lo que no requiere autorización ni legal ni expresa*), titulares y propietarios[53] de los datos personales o nominativos que los individualizan.

Repetimos: que no se requiera autorización previa, consentimiento expreso o implícito para recoger, tratar o procesar datos personales de los ciudadanos se debe a que *"la ley"* -fundamentalmente la ley 19.628 en sus artículos 2º, 4º y 20º, los instructivos presidenciales de Gobierno Electrónico, las Leyes Orgánicas de cada servicio, normas especiales, y la Ley de Bases Generales de la Administración del Estado, así lo permiten. Son normas que *"reemplazan a la voluntad, al consentimiento o a la autorización de los ciudadanos"*. En lo que compete al tratamiento de datos personales en los servicios públicos existen además, para algunos, normas especiales que los facultan para operar en forma privativa.

A modo de anticipo, porque volveremos con detalle sobre este punto en la Parte Segunda de este Informe: ...estimamos que no existe fundamento jurídico alguno para entender que las normas del artículo 5°[54] o la del artículo 10°[55] de la

---

"autodeterminen", autoricen y controlen el uso de sus antecedentes. Del mismo modo, se ha permitido legalmente que AFP, ISAPRE, multitiendas, Universidades, Asociaciones Gremiales, órganos públicos, etc. puedan comercializar grandes cúmulos de información, siempre con la ignorancia y sin el consentimiento de los titulares y propietarios de los antecedentes que los individualizan.

[53] Si los ciudadanos son los propietarios de sus datos, los servicios públicos son meros poseedores o tenedores de ellos sujetos a la responsabilidad de los artículos 11 y 23 de la ley 19.628.

[54] Señala: *"En virtud del principio de transparencia de la función pública, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo y esencial, y los procedimientos que se utilicen para su dictación, son públicos, salvo las excepciones que establece esta ley y las previstas en otras leyes de quórum calificado. Asimismo, es pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, a menos que esté sujeta a las excepciones señaladas".*

[55] Dispone: *"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. 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*

ley 20.285 constituyen una de aquellas autorizaciones legales para tratar los datos nominativos con prescindencia de la voluntad de su titular, a que alude esta regla general del artículo 4° de la ley 19.628.

En consecuencia, solicitados por un tercero sin expresión de causa o motivo y denegados de entregarse por un servicio público, en sede del amparo al derecho de acceso del artículo 24 de la ley 20.285 el Consejo de Transparencia debería abstenerse de fallar ordenando su entrega, cesión o comunicación. Máxime, cuando el artículo 33 letra m) lo obliga expresamente a velar por la correcta aplicación de la ley 19.628 entre los órganos de la Administración.

6. El concepto de "tratamiento de datos personales" en los órganos de la Administración.

Revisar esta definición es esencial, por cuanto su amplitud es muy grande. Es decir, implica un variado y amplio conjunto de operaciones en relación de los datos personales de los ciudadanos, las que, interpretadas literalmente, significa que actuando dentro de su competencia los servicios públicos pueden desarrollar diversas funcionalidades. Así por ejemplo, si el *"tratamiento"* implica la "*comunicación, cesión o transferencia"* de datos personales, cabe interpretar que se encuentran permitidos los convenios de intercambio de datos personales y la comunicación que se haga a terceros mediante su publicación en sitios web.

El amplísimo artículo 2° letra o) señala que es tratamiento de datos personales, lo siguiente:

> *"...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".*

No obstante lo amplio de la expresión, tratándose de su uso respecto de servicios públicos no siempre va a significar que éstos puedan realizar todas y cada una de las operaciones descritas. Así por ejemplo, la ley autoriza al INE a tratar la información recopilada de los censos para el cumplimiento de sus funciones, pero esa misma ley, de cara a su necesaria restricción consagra el llamado *"secreto estadístico"*[56], lo que le impide al INE el poder comunicar o transmitir a terceros la información respectiva en forma nominada o que se permita con ella identificar a los ciudadanos censados.

---

presupuesto público, cualquiera sea el formato o soporte en que se contenga, salvo las excepciones legales".

56

La característica de que el tratamiento de datos personales pueda no ser electrónico, informático, telemático o automatizado sino sólo mediante soportes manuales, guarda relación con otra definición, la del artículo 2° letra m, que dispone que legalmente debe entenderse por "registro o banco de datos", al 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.

7. El concepto de "fuentes accesibles al público" aplicable al sistema de tratamiento de datos personales en el Sector Público.

El concepto legal a esta fecha, en la ley 19.628, es el siguiente:

> *"i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".*

El artículo 4° establece que determinadas especies de datos que provengan de fuentes accesibles al público excepcionalmente no requieren autorización de sus titulares para ser tratados.

El artículo 5° inciso quinto señala que no se establecen limitaciones para la transmisión vía redes de "*datos personales accesibles al público en general".*

El artículo 9° establece, a *contrario sensu*, que los datos personales que provengan o se hayan recolectado de fuentes accesibles al público pueden usarse para fines diversos de aquellos con que fueron recolectados.

Por sus deficiencias, ambigüedades y posibles inconstitucionalidades, existe un proyecto en trámite que apunta a reemplazarlo y asignarle el debido alcance y naturaleza al concepto[57]. El gran problema de la definición es que no

[57] El artículo, una vez modificado en la forma propuesta por el Boletín 6120 en trámite en la Cámara de Diputados,, quedaría con el siguiente tenor: i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, cuyo acceso no se haya restringido o reservado sólo a los titulares e interesados en los datos personales que contiene, y que no hayan sido calificados como reservados o secretos en la normativa específica que les rija, tales como, (i) la estadística de los censos; (ii) los listados telefónicos en los términos previstos por su normativa específica; (iii) las listas de personas pertenecientes a grupos de profesionales que voluntariamente se hayan incorporado, consintiendo en el tratamiento público de sus datos, y que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, domicilio o residencia e indicación de su pertenencia al grupo; (iv) los diarios y boletines oficiales; y (v) los medios de comunicación social. El responsable del banco de datos deberá arbitrar las medidas necesarias para la correcta identificación por los titulares de datos, de la condición de fuente accesible al público.

aclara lo que debe entenderse por *"acceso no restringido o reservado a los solicitantes"*, lo que nos ha dado pie para, desde antes de su entrada en vigencia, reparar las consecuencias de esta mala y ambigua tipificación conceptual.

Parafraseando: fuentes -de datos personales o nominativos- accesibles al público, serán todas aquellas que no sean de acceso restringido o reservado; fuentes no accesibles al público, serán todas aquellas que sean de acceso restringido, secreto o reservado, no de hecho, sino porque la restricción, el secreto o la reserva, al ser de excepción, la establece una norma legal.

A modo de ejemplo, las bases de datos personales del Registro Civil no deben ser consideradas legalmente como *"fuentes accesibles al público"* o fuentes públicas de información, y por ende, son por regla general de acceso restringido o reservado, e incluso secreto, salvo, respecto de los antecedentes personales que pueden obtenerse por la vía de los certificados y porque la ley obliga a este servicio público a entregarlos a los ciudadanos y le permite comercializarlos.

En todas las leyes de protección de datos del Derecho Comparado, el concepto es claro, y alude a fuentes, bases o bancos de datos que por su naturaleza son accesibles al público o públicas, como los diarios oficiales, los listados telefónicos, los medios de prensa, los registros de los Conservadores de Bienes Raíces, etcétera.

En Chile no es así, y la definición debe interpretarse *a contrario sensu*, pero con un alcance distinto según se trate de (i) *bases de datos de los particulares o del sector privado*, o de los (ii) *bancos de datos mantenidos por los servicios u órganos del sector público.*

(i) Para los primeros, bastará determinar cuáles admiten ser consideradas legalmente en Chile como bases de datos de acceso no restringido, reservado o secreto.

Si tenemos presente que los únicos casos *"legales"* de secreto o reserva son -por excepción- el secreto bancario, el secreto tributario, el secreto estadístico, el secreto profesional, el secreto sanitario y el secreto de filiación política, puede considerarse que por regla general y al no existir una ley que establezca lo contrario -que existe reserva o secreto de la fuente o base de datos- todos las restantes registros o bancos de datos personales serán de acceso público, no restringido y no reservado, aplicando el principio de que en Derecho Privado puede hacerse todo aquello que no esté expresamente prohibido.

(ii) Para los segundos, esto es, para que las bases de datos nominativos de los servicios públicos con datos personales o nominativos sean calificables como fuentes accesibles al público y su acceso no considerado restringido o reservado, ello no puede depender sólo de que no exista una norma legal expresa que establezca la restricción o la reserva al acceso de la data personal.

Junto con no existir una prohibición expresa de procesar, "tratar", ceder o comunicar computacionalmente los datos personales, copulativamente debería existir una norma de Derecho Público que -también expresamente y con una concreta finalidad de servicio público- permitiera realizar la comunicación, cesión o publicación ante terceros, es decir, que habilitara al órgano del Estado para ser proveedor de antecedentes nominativos.

Ergo, cabe concluir que por regla general los servicios públicos no son proveedores gratuitos u onerosos de datos personales para el mercado ni para los particulares -terceros diversos del titular individualizado y al que le pertenecen los datos nominativos-.

Lo anterior está, por ejemplo: (i) expresamente permitido para el SERVEL, al que se le autoriza la comercialización de los padrones electorales y esencialmente el número de RUT; (ii) expresamente permitido al Servicio de Registro Civil, que puede comercializar certificados (documentos que contienen datos personales) referidos al estado civil de los ciudadanos como una de sus competencias esenciales de servicio público; (iii) *"al parecer permitido"* al Servicio Nacional de Aduanas (no hemos tenido las normas respectivas a la vista), que comercializa datos de las empresas importadoras y exportadoras referidos a las mercancías (valores, orígenes o proveedores, características, etc.) a cuyo respecto ellas son consignatarias; y, (iv) la ley obliga a los municipios a exhibir públicamente el avalúo de los predios y bienes raíces.

Es factible hacer el análisis aislado de un dato disponible en un servicio público determinado. Así por ejemplo:

(i) En primer lugar *la base de datos con los domicilios de los ciudadanos que administra el Servicio de Registro Civil* no admite ser calificada como una fuente de datos personales accesibles al público en forma masiva y sistematizada, sino que a su respecto incluso regiría la obligación legal de secreto del artículo 7° de la ley 19.628.

(ii) En segundo lugar, la autorización para el tratamiento del dato personal *"domicilio de los ciudadanos"* la otorga la ley en forma supletoria a la voluntad del ciudadano, tanto en los artículos 4° y 20° de la ley 19.628 como en la Ley Orgánica del Registro Civil.

(iii) Y en tercer lugar, la ley no faculta al servicio para entregar en forma masiva bases de datos con los domicilios a requerimiento de cualquier particular o de un a empresa con fines de lucro, sino sólo para emitir certificados (sea en

papel, sea electrónicamente en virtud del artículo 3° de la ley 19.799) en que pudiera constar el dato[58].

8. Finalidad del tratamiento de datos personales.

Los servicios públicos deben necesariamente procesar los datos personales cumpliendo con la finalidad tenida en vista y declarada al momento de su recopilación o recogida, lo que es un principio esencial en materia de protección de datos personales desde fines de la década de los 70. Cumplida esta condición el tratamiento que se haga podrá calificarse de legítimo o ajustado a derecho.

Así por ejemplo, los hospitales públicos no podrían usar los datos personales de sus pacientes para afiliarlos a un partido político o a un movimiento anti VIH; el MINVU no podrían usar los datos de los beneficiarios de subsidios de vivienda para ofrecerles seguros de incendio y de vida en conjunto con una empresa particular; y, el MIDEPLAN no podría usar datos de becarios de Conicyt para en conjunto con una línea aérea ofrecerles pasajes rebajados.

Establece el artículo 9°:

"*Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos".*

La segunda parte del artículo consagra el llamado *"Principio de la calidad de los datos nominativos".*

9. Acerca del tratamiento de datos personales sensibles o personalísimos en los órganos de la Administración.

Dispone a este respecto el artículo 2° letra g), que se trata de una especie del género datos personales, y que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad. Señala, sólo a modo de ejemplo, a (i) los hábitos personales, (ii) el origen racial, (iii) las ideologías y opiniones políticas, (iv) las creencias o convicciones religiosas, (v) los estados de salud físicos o psíquicos y (vi) la vida sexual.

[58] Nada podría objetarse si una empresa o un particular con recursos adquiriera por esta vía certificado impresos de, por ejemplo, dos millones de chilenos.

El uso de la expresión *"tales como"* se traduce en que se trata de una cuestión de hecho que en definitiva determinarán los tribunales el definir si un dato personal o nominativo es o no sensible. Es un concepto general, amplio y abierto,

Dispone a este respecto el artículo 10° de la ley 19.628, que *por regla general los datos sensibles no pueden ser objeto de tratamiento*, …salvo (i) cuando la ley lo autorice, (ii) exista consentimiento del titular o (iii) sean datos de salud necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Esto significa, primero, (i) que para la ley 19.628 las condiciones legales o de legitimidad del tratamiento dependerán de la naturaleza o especie de dato personal tratado, y en segundo lugar, (ii) que los datos sensibles o personalísimos gozan de una protección jurídica mayor que la de los restantes datos personales, que por regla general siempre pueden tratarse si el titular consiente expresamente en que se haga, o si la ley 19.628 u otra ley lo permiten.

Para los sensibles la regla general es la contraria; si no concurren algunas de las tres condiciones de excepción, ellos no pueden tratarse, o si se hace, el tratamiento sería ilegítimo, ilegal o contrario a derecho.

Existen además leyes expresas que aluden al tratamiento de datos personales sensibles por los entes públicos. Es el caso ya mencionado a pie de página de la ley 19.397, que junto con permitirle al Ministerio de Salud tratar y mantener registros respecto de las materias de su competencia y solicitar o requerirle datos personales a otros servicios públicos, *lo faculta expresamente para tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud.*

10. La institución del responsable del registro de la base o de los bancos de datos personales de los servicios públicos.

La letra n) del artículo 2° señala que reviste tal calidad *"la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal"*.

El mismo artículo define lo que debe entenderse por *"registro o banco de datos",* a saber, *"el conjunto organizado de datos de carácter personal, sea automatizado o no"* (pensemos en el cardex de un archivo con tarjetas) *"...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".*

El artículo 5° faculta al responsable para establecer un procedimiento automatizado de datos personales.

El artículo 6° señala que el responsable tiene la obligación de eliminar, modificar o bloquear datos personales sin necesidad de requerimiento del titular (léase *“de oficio*”).

El artículo 8° dispone que el responsable puede ser un *"mandatario"* para el tratamiento de datos personales, debiendo aplicarse las reglas generales, otorgándose el contrato de mandato por escrito y dejándose especial constancia de las condiciones para el uso de los datos personales, estipulaciones, atribuciones, competencias y funciones que el responsable -y la ley consigna una obviedad- deberá respetar en el cumplimiento del encargo de su mandante; de no hacerlo -...otra obviedad, pero nuestra- le generará responsabilidad ante los eventuales perjuicios ocasionados, tanto contra el titular de los datos como contra el mandante que le encargó contractualmente la gestión del tratamiento y por no haberse cumplido el cometido mandatado en la forma establecida.

El artículo 11° establece que el responsable de los registros o bases de datos personales deberá cuidar de ellos con la debida diligencia. Obviamente agrega que lo hará “*con posterioridad a su recolección”* y que se hará responsable de los daños producidos. Entendemos, en consecuencia, que responde de la culpa leve.

El artículo 12° lo indica como la persona ante quien se ejerce el denominado *Habeas Data* o *Derecho de Acceso.*

El artículo 16° señala que su domicilio determina la competencia de los tribunales.

El artículo 17° faculta al responsable para comunicar a terceros los datos patrimoniales negativos.

Veremos en el acápite sobre los convenios de intercambio de datos personales entre los servicios públicos y empresas particulares las hipótesis de externalización de funciones, esto es, por ejemplo, cuando el servicio y el funcionario público responsable no asumen directamente la gestión de tratamiento, sea porque se transfieren datos personales a empresas externas con las cuales contratan por ejemplo cobranzas judiciales, sea porque se contratan servicios de respaldo de la información de servidores y bases de datos. Pero esta "externalización", tan conveniente desde el punto de vista de los costos de gestión, no exime de responsabilidades al órgano de la Administración que externaliza.

Un comentario final respecto del responsable y su importancia en el sector privado. Atendido que la ley eliminó la obligación que los responsables queden anotados en un registro público, es factible que los titulares de los datos personales nunca sepan de la existencia del banco de datos o el origen de los

datos y que los responsables actúen en total anonimato y carentes de toda fiscalización por la autoridad.

Paradojalmente, en el Derecho Comparado la conducta consistente en actuar en el ámbito del procesamiento de datos personales sin haberse registrado y sin autorización previa se sanciona con fuertes multas, e incluso es constitutiva de delito penal.

11. Obligación de secreto para los responsables de bases de datos de los servicios públicos.

Por regla general, el procesamiento o el tratamiento de datos personales genera la necesidad de cumplir con una obligación general de secreto para los funcionarios públicos responsables de las bases de datos que expresamente establece la ley, y que de ser vulnerado por el responsable incluso configura el delito informático del artículo 4° de la ley 19.223.

La excepción está dada en el evento de que la base de datos no sea de acceso restringido, reservado o secreto y pueda por ende legalmente calificarse como *"accesible al público".*

Establece el artículo 7°:

> *"Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con la base de datos, obligación que no cesa por haber terminado sus actividades en ese campo".*

Esta obligación de secreto *"general"* es complementaria de otras cargas legales *"especiales"* establecidas por ley, como ocurre en materia de secreto tributario para el Servicio de Impuestos Internos y la Tesorería General de la República, el secreto estadístico para el Instituto Nacional de Estadísticas, o el secreto de filiación política para el Servicio Electoral.

Y sostenemos que se trata de una obligación general por cuanto, conforme a lo ya analizado más arriba, estimamos que las bases de datos personales de los servicios públicos no son fuentes accesibles al público, cosa que no guarda relación alguna con las obligaciones de transparencia que recientemente ha establecido para ellos la ley 20.285, en relación al acceso a la información administrativa administrada o generada por los órganos de la Administración, porque estas obedecen a otra Política Pública, poseen otros fundamentos constitucionales, y exigen otros supuestos de procedencia. Volveremos sobre ello en la Parte Segunda.

12. Transferencia telemática o vía redes de datos personales, dentro de Chile y hacia el extranjero.

Lo que nosotros denominamos transferencia telemática algunos *paper* doctrinarios lo mencionan como la comunicación o la cesión de datos personales a terceros, y se visualiza como un tema central de la ley 19.628, que determina en su articulado las condiciones y requisitos que se deben cumplir para que un órgano de la Administración pueda, por ejemplo, transferir datos personales de los ciudadanos a terceros -sea a otro servicio público, sea a una entidad particular- mediante un procedimiento automatizado.

El artículo 2° letra c) dispone que la *"comunicación o transmisión de datos"* -ambos términos sinónimos para la ley- consisten en dar a conocer los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas, y *"de cualquier forma"* o mediante cualquier soporte o canal electrónico o telemático, como son hoy en día -por ejemplo- los mecanismos de webservice de la red Internet.

También, a propósito de la definición legal de *"tratamiento"* del artículo 2°, la ley 19.628 usa la expresión *"interconectar"* datos personales o, más precisamente, a los sistemas o bases de datos que los contienen, y se mencionan las operaciones de comunicar, transferir y transmitir información nominativa.

Se trata de un tema que no es de poca relevancia para los servicios públicos en el plano de las transferencias o transmisiones internacionales, ante la existencia de Convenios de doble tributación que implican intercambios de información, o ante la continua conexión vía redes internacionales de los organismos policiales y de seguridad pública.

Y es relevante en el plano local, (i) porque a esta fecha existen procesos telemáticos de cruces de información entre servicios y entre éstos y empresas particulares que se verifican mediante la red Internet y mecanismos de *"webservice";* (ii) porque algunos servicios públicos transfieren datos personales a empresas externas con las cuales contratan por ejemplo cobranzas judiciales o servicios de respaldo de la información de servidores y bases de datos; o, (iii) porque se están desarrollando -sin el adecuado apego a la legalidad requerida- proyectos como el de la Plataforma Integrada de Servicios Electrónicos del Estado (la PISEE). Volveremos sobre estos temas a propósito de los Convenios suscritos al efecto.

Este artículo 5° en vigencia posee, en si mismo y en el contexto de la ley, cuatro grandes limitantes que justifican u ocasionan su poca aplicación.

La primera, que se señala en el inciso 5° que no se aplicará este artículo cuando se trate de datos personales accesibles al público en general, que, como sabemos, son prácticamente todos los datos personales en conformidad a lo que establecen los artículos 2° letra i) y 4° (la norma no rige para la generalidad de los datos).

La segunda, que alude a responsables de bases de datos personales o nominativos que los *"transmiten"* y que los *"reciben",* pero estos necesariamente deben estar localizados físicamente dentro del territorio de Chile para que a ambos se les puedan aplicar las restricciones o limitantes.

La tercera, que las restricciones mencionadas son sólo formales o declarativas ya que no existe un ente administrativo que vele, a priori o a posteriori, por su cumplimiento, y porque el titular de los datos no debe ser obligatoriamente informado por el servicio público acerca de la realización de la transferencia.

Y la cuarta, que se presenta particularmente grave en los STDP del sector privado, es que al no existir un registro obligatorio de responsables las transferencias de datos personales, tanto locales como internacionales, pueden verificarse en el más absoluto anonimato.

Preceptúa el artículo 5° que el responsable del registro o banco de datos personales podrá establecer –obviamente es facultativo- un procedimiento automatizado de transmisión, siempre que –es lo declarado formalmente- *"se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes"*. Se repite en otro inciso que *"el receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión",* lo que es coincidente con el artículo 9° de la ley.

No compartimos de modo alguno la sugerencia de que esta norma desconocería la regla general del artículo 4°, y que por ende, nunca se exigiría autorización previa -o ratificación- del titular de los datos para realizarse la comunicación. Las normas deben interpretarse como un todo armónico, y si bien el artículo 5° intenta regular la comunicación y señala que es facultad del responsable comunicar o no, de haber querido el legislador de la ley 19.628 prescindir de la autorización lo habría señalado expresamente y, probablemente, incluido dentro de las excepciones respectivas.

Se establece además –siempre como una interesante declaración de principios- que frente a un requerimiento de datos personales mediante una red electrónica deberá dejarse constancia (i) de la individualización del requirente, (ii) del motivo y el propósito del requerimiento y, (iii) del tipo de datos que se transmiten, y que la admisibilidad del requerimiento será evaluada por el responsable del banco de datos del servicio público que lo reciba pero la responsabilidad por dicha petición será de quien la haga.

Es también cuestionable lo que establece el inciso final a modo de excepción, esto es, que la disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes. *¿Y si esas instancias internacionales no aseguran la confidencialidad de las transferencias desde el punto de vista de la seguridad de sistemas y, por ende, de la privacidad de los titulares de los datos transmitidos telemáticamente?.*

El análisis sólo académico que hasta la fecha se había realizado del artículo 5° de la ley 19.628 no ha reparado en que la omisión de abordar el tema de la transferencia de datos personales hacia o desde el extranjero ha sido una de las falencias importantes de la ley[59].

El Boletín 6120 ha propuesto introducir importantes modificaciones en este sentido, agregando un artículo 5 bis expresamente referido al tema.

El establece que no podrán realizarse transferencias de datos personales a países que no proporcionen un nivel de protección adecuado, conforme a la presente ley, salvo autorización previa del *Consejo de Transparencia y de Protección de Datos* -o quien en definitiva sea el órgano ad hoc-, la que sólo podrá otorgarse si se obtienen garantías adecuadas, y que la adecuación del nivel de protección proporcionado por el país de destino será evaluada a la luz de las circunstancias que rodeen a la transferencia, tomándose en consideración (i) la naturaleza de los datos, (ii) la finalidad y duración del tratamiento, (iii) el país de origen, (iv) el país de destino y (v) las reglas relativas al tratamiento que existan en ese país[60].

El Mensaje había anticipado que se regulaba el flujo transfronterizo de datos, exigiéndose autorización del Consejo (autoridad controladora) respecto de

[59] Basta considerar el tema además desde la perspectiva práctica de un banco o de una empresa transnacional que posea filiales en Chile y que opere de la mano de un servidor *"ASP"*[59] o central ubicado en el extranjero, donde en definitiva se realizarán las transacciones o donde se almacenará la data personal o nominativa de los cuentacorrentistas o de los clientes de la empresa transnacional.

[60] Agrega el propuesto artículo 5° bis: *"se exceptúan de la prohibición prevista en el inciso primero, la transferencia consentida por el titular de datos, y los casos en que ésta fuere necesaria para la ejecución de un contrato entre el interesado y el responsable del registro o base de datos; para la aplicación de medidas precontractuales adoptadas a petición del interesado; para la celebración o ejecución de un contrato entre el responsable del registro o banco de datos y un tercero en interés del interesado; para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; o para la protección del interés vital del interesado. Queda asimismo exceptuada la transferencia internacional de datos personales que resulte de la aplicación de tratados o convenios internacionales en los que el Estado de Chile sea parte, o bien cuando la transferencia fuere necesaria o legalmente exigida para salvaguardar un interés público o cuando se haga a efectos de prestar o solicitar auxilio judicial internacional".*

aquellos países que no cumplan con un nivel de protección adecuado para realizar la comunicación de los antecedentes nominativos.

13. Gestión diligente y normas sobre responsabilidad del administrador o funcionario público "responsable" de la base de datos del servicio público.

Establece el artículo 11° que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos *"con la debida diligencia",* haciéndose responsable de los daños.

Y en el Título V, sobre la responsabilidad por las infracciones a esta ley, el artículo 23° dispone que la persona natural o jurídica privada *"o el organismo público"* responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare *"por el tratamiento indebido de los datos",* sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en caso, lo ordenado por el tribunal[61].

Adicionalmente y como veremos, todo servicio público que trate datos personales debe implementar las medidas de seguridad de sistemas que en forma obligatoria establece el Decreto Supremo N°83 del año 2005, definidas en base a estándares internacionales o a las normas ISO sobre el tema. La base esencial de este trabajo fue una norma publicada el año 2003 por el INN; de hecho, el Decreto 83 se refiere a ella reiterada y expresamente, y fue la que tradujo, a su vez, la Norma ISO 17799 (sobre seguridad de sistemas, servidores y bases de datos).

La norma del INN es la *NCh2777.of2003*, y se denomina como "*Código de Práctica para la gestión de la seguridad de la información".*

Veremos más adelante el tema de la seguridad que legalmente cabe esperar de los responsables de los STDP de los servicios públicos. Esta obligación llega, a la luz de los dispuesto por el Decreto Supremo 83 sobre seguridad y confidencialidad de los documentos electrónicos, incluso a la necesidad de determinarse previa y expresamente a un funcionario *"Responsable de la Seguridad de los Sistemas"* del servicio público, nombrado mediante resolución expresa; este encargado, por ejemplo, deberá permanentemente monitorear, auditar y fiscalizar el desempeño de las labores de procesamiento que les sean encomendadas, en conformidad a mecanismos técnicos de monitoreo y control de cumplimiento que en su momento se determinen.

Y veremos como mediante el Boletín 6120 modificatorio de la ley 19.628, al decir de su Mensaje, el proyecto establece para el futuro -mediano plazo tal vez, a

[61] En el acápite G de este informe se analizan los cambios propuestos en este ámbito por el Boletín 6120 en actual trámite parlamentario.

riesgo de equivocarnos- (i) que el responsable del tratamiento de datos deberá adoptar todas las medidas técnicas y organizativas que garanticen la seguridad de los datos; y, (ii) que para fijar las condiciones de seguridad ellas serán definidas reglamentariamente y no quedarán a discreción del responsable del tratamiento de datos, salvo que se disponga otra cosa en un tratado del que Chile sea parte, exista interés público comprometido, o ello sea en interés del propio titular.

De cara a la naturaleza de la responsabilidad que para los servicios públicos establece el artículo 11, esto es, si es subjetiva o por falta de servicio u objetiva o por riesgo, no conocemos -salvo error u omisión- fallos de los tribunales que hayan resuelto el tema.

Una opción es la de entender que se establece un sistema de responsabilidad objetiva, donde se prescinde de la existencia de culpa o dolo en el funcionario público, y donde bastaría la constatación de que el tratamiento de datos personales haya sido sin *"la debida diligencia"* que establece el artículo 11 o *"en la forma indebida"* que menciona el artículo 23 y a consecuencia de lo cual un titular de datos resulta perjudicado o *"conculcado en el legítimo ejercicio de sus derechos a consecuencia del tratamiento"* -como alguna vez propuso un proyecto de ley hoy abandonado de tramitación-, en un ámbito de alta complejidad técnica donde son reales y concretos los riesgos derivados del uso de la informática o de la telemática, de los servidores, de las redes y de bases o bancos de datos.

Otra opción, también con fundamento plausible, es la de considerar que por el uso de las mismas expresiones se exigiría falta de diligencia culposa o dolosa en la conducta del funcionario público responsable del tratamiento.

A nosotros nos acomoda aplicar respecto de los servicios públicos, supletoriamente y por vía de interpretación e integración de la norma, lo que establece el artículo 42 de la LGBAE, esto es, que los servicios públicos serán responsables del daño que causaren por falta de servicio, agregándose que el Estado tendrá el derecho de repetir en contra del funcionario que hubiere incurrido en falta personal[62].

14. Carácter personalísimo y limitaciones de Orden Público del ejercicio del derecho de acceso o Habeas Data del artículo 12.

[62] Esta norma, sobre la cual volveremos, es la que sustenta en doctrina el afirmar que el Estado Chileno y sus funcionarios son subjetivamente responsables, y que la falta de servicio exige expresamente probar la falta; es decir, no bastaría con la relación de causalidad sino que es necesaria la existencia real de la falta, sea de funcionamiento, de funcionamiento tardío o de deficiente funcionamiento del servicio público, causándose un perjuicio a los usuarios o destinatarios del servicio.

14.1 Esta garantía esencial de toda ley de protección de datos y las facultades que de ella derivan, mismas que por su importancia en varios países tienen rango constitucional, están reguladas en los artículos 12º, 13º, 14º, 15º y 16° de la ley, que son los primeros del Título II sobre *Derechos de los titulares de datos*, y se ejercen precisamente ante quien aparezca como responsable del registro.

La norma establece -en su inciso primero- que toda persona natural y titular de los datos -único legitimado activo del Habeas Data (sea que actúe personalmente o jurídicamente representado)- tiene el *derecho de exigir a quien sea responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales, "información sobre los datos relativos a su persona"* -no respecto de terceros-, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente[63].

Agrega que -*habiéndose en síntesis tomado conocimiento de su exactitud o inexactitud y veracidad o falsedad*- ...en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, *tendrá derecho a que se modifiquen* o rectifiquen y que sin perjuicio de las excepciones legales podrá exigir que *se eliminen, cancelen o bloqueen*, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Dos acápites más abajo volveremos sobre el análisis de estos derechos.

En el contexto del sector público y en el marco de los controles legales y administrativos de la gestión del Estado, este artículo 12 es el elemento esencial que permite e instrumentaliza en derecho un control directo y -en teoría- ejecutivo acerca de la legalidad del tratamiento de datos, control o examen administrativo que se verifica *"a posteriori"* por el titular de los antecedentes nominativos que busca autodeterminar y fiscalizar que el tratamiento no sea ilegal, arbitrario o abusivo. *Es dable calificar este Habeas Data, ejercido contra los órganos de la Administración, como un procedimiento contencioso administrativo especial.*

Este titular debe recurrir obligatoria e inicialmente -a modo de agotamiento de la vía previa- ante el responsable del registro, base o banco de datos en un servicio público determinado[64], para ejercer extrajudicialmente su derecho de acceso.

Si aquel responsable del registro o banco de datos nada dice, no se pronuncia dentro de un plazo de 48 horas o de dos días hábiles dice la ley, frente

[63] Esta garantía procesal se espera que en el mediano plazo adquiera rango constitucional. Ya se han presentado dos Mociones al efecto para agregar la facultad como un nuevo inciso segundo del artículo 19 N°4 de la Constitución. Sobre el tema, véase la URL http://www.habeasdataorg.cl/2009/05/15/nuevamente-se-avanza-en-materia-de-constitucionalizacion-del-habeas-data/.

[64] De acá deriva la importancia de que el ciudadano conozca claramente su identidad.

a o incluso también denegando una solicitud de acceso, de modificación, de eliminación, de cancelación o de bloqueo, el titular posee un segundo ámbito de reclamo y de control ya no administrativo, ante los Tribunales de Justicia ordinarios, mediante la acción de derecho de acceso o de Habeas Data y un procedimiento sumario que establece el artículo 16°[65].

El artículo 6°, extrañamente, repite varios de los conceptos también contenidos en el artículo 12. Ambos artículos debieron haberse refundido en uno solo. Repite la idea de que los datos personales pueden *eliminarse o cancelarse* cuando hayan sido almacenados sin fundamento legal o cuando estén caducos[66]. Señala que deberán *modificarse* cuando sean errados, inexactos, equívocos o incompletos[67]. Lo que es nuevo y exclusivo de este artículo es el establecer perentoriamente que deberán *bloquearse* cuando no se pueda establecer su exactitud o su vigencia sea dudosa, y en cualquiera de ambos casos no corresponda su *cancelación*[68].

14.2 Una distinción y/o aclaración desde ya, a modo de anticipo, porque incluso Tribunales Ordinarios de Justicia (en concreto la I. Corte de Apelaciones de Santiago) se han confundido conceptualmente en cuanto a su naturaleza y alcance[69].

---

[65] En conformidad a las reglas generales del Derecho, y así ha ocurrido, no existe impedimento alguno para optar por interponerse recursos de protección invocando la violación del artículo 19 N°4 de la Constitución, los llamados recursos de amparo económico o demandas de indemnización de perjuicios mediante juicios ordinarios, todos ellos, para buscar que se sanciones posibles tratamientos arbitrarios o ilegales y el uso ilícito o indebido de datos personales, y que se reparen los posibles perjuicios causados por la negligencia del servicio público.

[66] El inciso tercero del artículo 12 señala que "*sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos".*

[67] El inciso segundo del artículo 12 repetirá más adelante que "*en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen".*

[68] El artículo 15º establece que *"no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional",* y que *"tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva".*

[69] En fecha reciente, un fallo de la I. Corte de Apelaciones de Santiago, al conocer de un reclamo de ilegalidad ante la declaración de incompetencia del Consejo de Transparencia para pronunciarse respecto a la denegación de una solicitud de información interpuesta ante el Banco del Estado (véase la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091026/pags/20091026114231.html) ha confundido al acceso del artículo 10° con el habeas data de la ley 19.628. Hoy, al invocarse el ejercicio del *Derecho de Acceso a la Información Pública* consistente en actos y documentos de los órganos estatales, resulta preocupante ver como se desnaturaliza esta otra garantía muy poco conocida-, que posee un objeto y una razón de ser radicalmente diversa.

La causa original que dio lugar al Recurso de Ilegalidad fue un Amparo por denegación de solicitud de información -contemplado en la ley 20.285 y no en la 19.628- interpuesto por un señor Pérez Castro en contra del Banco Estado, respecto al cual el citado Consejo resolvió que no era

(I) En Chile legalmente a esta fecha existe este "*Habeas Data"* del artículo 12 de la ley 19.628 en estudio.

(ii) Con otra finalidad jurídicamente distinta que el control y la autodeterminación de los propios datos personales, existe también legalmente el derecho de acceso del artículo 10° de la ley 20.285[70], mediante el cual cualquier ciudadano o toda persona tiene derecho a solicitar y a recibir información pública sobre la gestión de cualquier órgano de la Administración, conforme a ciertos principios y con el amparo y/o la tutela del Consejo de Transparencia.

(iii) Con una finalidad similar pero en el contexto de un procedimiento administrativo en curso, el artículo 17 de la ley 19.880 sobre el tema, contempla el derecho de las personas en sus relaciones con la Administración -entre otros- para conocer en cualquier momento el estado de la tramitación de los procedimientos en que sean interesados, para obtener copia autorizada de los documentos del expediente y la devolución de los originales, y para *"acceder a los actos administrativos y sus documentos en los términos previstos en la ley".*

El nuevo inciso primero que se propone incorporar al artículo 12 en el Boletín 6120 mencionado y en trámite en la Cámara de Diputados a esta fecha, establece que si se desconoce la identidad del responsable de la base de datos en un servicio público, toda persona podrá solicitar información sobre la existencia de tratamientos de datos de carácter personal que pudieran afectarle, sus finalidades y todos los antecedentes necesarios para la identificación del responsable del tratamiento, acudiendo al *"Registro Único Nacional de Bancos de Datos".* Pero esta opción, es independiente de quien sea la entidad o él órgano que en definitiva administre dicho banco de datos, a saber, una Secretaría ad hoc, una Agencia de

---

competente para conocer del amparo por tratarse de un recurso en contra de una empresa pública a cuyo respecto sólo tenía competencia en materia de Transparencia Activa (esto es, para fiscalizar lo que obligatoriamente debe publicarse en Internet). Más específicamente, el Consejo había estimado por mayoría que no se trataba de una denegación ante el Amparo deducido sino de una declaración de incompetencia. La Corte de Apelaciones de Santiago hizo público un fallo de la Séptima Sala en el cual resolvió por unanimidad rechazar el Recurso de Ilegalidad por considerarlo "extemporáneo" (se había presentado fuera de fecha, ya que la ley 20.285 otorga un plazo máximo de 15 días para la interposición ante la Corte de Apelaciones), pero -y acá radica el error conceptual y jurídico- en la misma resolución determinó que el Consejo para la Transparencia era "*plenamente competente para conocer del reclamo de habeas data deducido por el recurrente contra el Banco del Estado".*

[70] Señala la norma: *"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".*

Protección de Datos, o el Consejo de Transparencia de la ley 20.285 devenido además en Consejo de Protección de Datos[71].

Es un grave error jurídico el creer que esta nueva opción nace o deriva de la existencia de la ley de acceso a la información administrativa, la 20.285, o que este Habeas Data para la autodeterminación de los datos personales necesita o evidencia su naturaleza de ser complementario con el acceso a los actos, contratos, documentos y resoluciones de la Administración.

Esta modificación del Boletín 6120, en cuanto a la creación de un órgano ad hoc que administre un registro para terminar con el anonimato que desde 1999 existe en Chile acerca de la identidad de los responsables de bases de datos en el sector privado, deriva de que se trata de un elemento esencial de las leyes de protección de datos que existen desde 1978 a la fecha, y no podía evitarse de ser agregada de cara al objetivo de cumplir con los estándares europeos en general y de la OECD en particular, que es el objetivo central de las modificaciones en curso. Todo se podía haber propuesto legislar, aún cuando no se hubiera creado en Chile el año 2008 el Consejo de Transparencia.

No es efectivo que el derecho a la vida privada, en su aspecto positivo o de control, autodeterminación y fiscalización[72] esté directamente relacionado con el derecho de acceso a la información del Estado. Al contrario, como desarrollaremos, no guardan relación alguna, en cuanto a sus fundamentos, finalidad u objetivos y legitimados activos o titulares.

A mayor abundamiento: cuando se afirma que *"….los derechos que pueden ejercer los titulares de los datos personales registrados en bancos de datos exigen, como requisito previo, ejercer el derecho de información y acceso a la misma, …pues sin éste derecho esencial la protección de datos personales se volvería ilusoria, dejando sin contenido los derechos de rectificación, cancelación e indemnización*"[73], no debe olvidarse que este acceso es el del Habeas Data que

---

[71] Como veremos, si se acogiera la tesis de que el concentrarse ambas funciones —la de promover el acceso a la información administrativa o del Estado y la de velar por la protección de datos de carácter personal— en el Consejo de Transparencia, la labor de ponderación frente a un requerimiento en sede de la ley 20.285 que contenga o aluda a datos o antecedentes personales o nominativos quizás si podría ser realizada de una manera más eficiente. *Pero, esto sólo tratándose de habeas data presentados contra los servicios públicos,* porque nada puede decir -a esta fecha- el Consejo de Transparencia cuando se alude a la problemática del tratamiento de datos personales en el sector privado.

[72] La perspectiva *"negativa"* dice relación con la forma en que surgió el concepto de privacidad, como opción de ser eliminado o dejado a solas, y esto no es socializante.

[73] Calificándose como una *"estrategia emergente para el desarrollo de la protección de datos en Chile"*, esta propuesta se ha formulado por dos abogados del Consejo de Transparencia en la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

nació en la jurisprudencia, las leyes y la doctrina extranjera para que el titular de sus propios antecedentes pueda controlar y autodeterminar únicamente el uso que se haga de ellos.

En la Parte Segunda nos hacemos cargo de la tesis -para refutarla- que sostiene que cuando el derecho de acceso de la ley 19.628 se ejerce respecto de un organismo público, responsable del banco de datos, existiría coincidencia eventual entre el derecho de acceso a que alude la ley 20.285; este sería de carácter general -se afirma-, y el derecho de acceso a los datos a que se refiere la ley19.628 sería de carácter particular[74].

14.3 Los servicios públicos sólo deben atender las peticiones de Habeas Data o derecho de acceso que presenten los ciudadanos para controlar y autodeterminar los datos personales cuando sean realizadas por los propios titulares individualizados y por el sólo hecho de serlo, sin necesidad de acreditar o manifestar otro interés legítimo que el de querer autodeterminar y controlar sus propios antecedentes personales, pero sin que puedan entrabar la gestión de la Administración del Estado, salvo -por cierto- que provengan de fuentes accesibles al público.

Esto lo consagra el artículo 15°, en los siguientes términos:

"*No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva".*

---

[74] 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".* No existe fundamento jurídico alguno, en las actas de la tramitación legislativa, para sostener esta afirmación.

15. Regulaciones para la gestión de los servicios públicos desde la perspectiva de los "Principios del Derecho de Protección de Datos Personales" recogidos por la ley 19.628.

No es libre la gestión administrativa que realicen los servicios públicos mediante STDP; pero además de las normas expresas ya referidas, subyacen en la ley 19.628 diversos *"principios esenciales"* que inspiran la regulación, recogidos de la legislación y la doctrina extranjera y que pueden configurar un verdadero *"Código Deontológico"* para los funcionarios públicos responsables del tratamiento de los datos nominativos de los ciudadanos.

Ellos son, y a ellos alude el Mensaje del Boletín 6120 ya referido, el principio (i) *del consentimiento del titular*, el (ii) *de los datos personales especialmente protegidos*, el (iii) *de la calidad de los datos*, el (iv) *de seguridad -y agreguemos de la responsabilidad*, el (v) *de secreto* y el (vi) *de la cesión o transferencia telemática de datos personales.*

La ley dispone que el titular de los datos es la persona natural a la que se refieren los datos de carácter personal, y establece formalmente como principio general que el tratamiento de los datos personales que haga el órgano de la Administración sólo puede efectuarse cuando disposiciones legales lo autoricen o *el titular consienta expresamente en ello*, precisándose que la autorización puede ser revocada por escrito y sin efecto retroactivo. Si es una ley la que lo autoriza, por cierto, la voluntad general del legislador viene a suplir la voluntad particular del titular.

Se menciona el *principio de los datos especialmente protegidos*, porque las leyes de protección de datos tratan de un modo especial a los datos sensibles, una especie del género dato personal.

Si por definición el género lo forman los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, la especie "datos sensibles" son -para el artículo 2° de la ley 19.628 y para la ley 20.285 y su Reglamento por cierto- 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 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.

El principio general es que este tipo de datos *"personalísimos"* no pueden ser objeto de tratamiento, salvo cuando la ley lo autorice, cuando exista consentimiento del titular, o cuando se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

En cuanto al *principio de la calidad de los datos nominativos* que procesen los servicios públicos, se dispone que la información que se trate en los STDP debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos, y por ende se define el dato personal caduco y se contemplan varios instrumentos para resguardar este principio. A saber: los datos personales deben ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado; los datos han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos; y los datos deben bloquearse cuando su exactitud no pueda ser establecida o cuando su vigencia sea dudosa.

En cuanto al *principio de seguridad*, él se manifiesta en alguna medida en la existencia de un procedimiento de disociación o desagregación de datos personales, a saber, cuando el servicio público debe garantizar que el tratamiento de datos personales y la información que se genere no podrá asociarse a persona determinada o determinable (lo que ocurre en la práctica cotidiana de los servicios públicos, por ejemplo, mediante el uso de datos fictos o sólo referenciales).

Pero la consagración del principio de la seguridad es más evidente cuando se establece que el responsable de los registros o bases de los servicios públicos donde se almacenen datos personales de los ciudadanos, con posterioridad a su recolección debe cuidar de ellos con la debida diligencia y haciéndose responsable de los daños.

El *principio del secreto*, con una dimensión general, se recoge cuando se dispone que los funcionarios públicos que operan en el tratamiento de datos personales están obligados a guardar secreto sobre los mismos, en la medida que provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con la o las bases de datos, obligación que permanece en el tiempo y no cesa por haber terminado sus actividades en el ámbito del STDP.

Por último, se menciona -y así lo recoge el Boletín 6120 que a esta fecha se tramita para modificar la ley 19.628-, el llamado *"principio de cesión"* o para nosotros de la transferencia telemática que realicen los servicios públicos, relevante en la práctica, como señalamos más arriba, porque existen procesos telemáticos de cruces de información entre servicios y entre éstos y empresas particulares que se verifican mediante la red Internet y mecanismos de *"webservice",* o porque a esta fecha se están desarrollando proyectos como el de la *Plataforma Integrada de Servicios Electrónicos del Estado.*

En síntesis, de acuerdo a este principio: (i) los datos que existan en una base, pueden darse a conocer, y se define comunicación o transmisión de datos como dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas; (ii) la comunicación puede surgir a consecuencia de una iniciativa del responsable de la base o a

requerimiento de un tercero; (iii) el responsable del registro o banco de datos personales puede establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes; y (iv) el receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

Salvo, haciendo excepción a todo lo anterior, que se trate de datos personales accesibles al público en general o que se transmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en tratados y convenios vigentes.

Por cierto, debe considerarse el c*arácter internacional de los principios del derecho de protección de datos personales*. Un reciente encuentro realizado en la ciudad de Madrid ha generado un documento que merece ser referido y tenido a la vista si se desea profundizar en sus contenidos y alcances[75].

16. Regulaciones para la gestión de los servicios públicos desde la perspectiva de los "Derechos para la protección de datos personales" recogidos por la ley 19.628.

De cara a los específicos derechos que consagra la actual regulación en los artículos 12, 13 y 14, para que los ciudadanos titulares de los datos personales registrados en bases y bancos de datos de los servicios públicos puedan controlar y autodeterminar el tratamiento de sus antecedentes propios y nominativos, e*l responsable del STDP del órgano del Estado podría ser objeto de un (i) derecho de información y acceso, de un (ii) derecho de rectificación, de un (iii) derecho de cancelación o eliminación, de un (iv) derecho de bloqueo y de un (v) derecho de indemnización.*

Derecho *"de acceso o información"*, porque toda persona titular de datos personales puede exigir al funcionario público que sea responsable de un banco de datos dedicado al tratamiento de datos personales, información sobre (i) los datos relativos a su persona, (ii) su procedencia y (iii) destinatario, (iv) el propósito o finalidad del almacenamiento y (v) la individualización de las personas u organismos a los cuales sus datos son transmitidos *"regularmente"* -dice la ley-. Incluso más, dispone el artículo 14 de la ley que si los datos personales están en un banco de datos al cual tienen acceso diversos organismos o servicios públicos, el titular puede requerir información a cualquiera de ellos.

[75] El documento puede verse en la URL https://www.agpd.es/portalweb/canaldocumentacion/common/estandares_resolucion_madrid.pdf.

De este derecho principal derivan los restantes; sabido que sea que se están tratando datos personales en un STDP de un servicio público, y conocida además su exactitud o inexactitud, licitud o ilicitud y finalidad debida o no, su titular podrá rectificarlos, cancelarlos, eliminarlos o bloquearlos.

Derecho *"de rectificación o de modificación",* definido legalmente como la solicitud de todo cambio en el contenido de los datos almacenados en registros o bancos de datos, cuando ellos sean *"erróneos", "inexactos", "equívocos"* o *"incompletos"*, y se acredite esta falta de idoneidad o de calidad de ellos.

Un derecho *"de cancelación o de eliminación"* definitiva*,* que es procedente en caso que el almacenamiento de datos personales *"carezca de fundamento legal"* o cuando *"estuvieren caducos"*, cuando se hubieren proporcionado voluntariamente los datos personales, o cuando se usen para comunicaciones comerciales y el titular no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Y un derecho *"de bloqueo"*, que se le confiere al titular de los datos para pedir la suspensión temporal de las operaciones de tratamiento de datos y que estos no sean comunicados o transferidos a terceros, cuando los antecedentes nominativos no sean susceptibles de ser determinados en cuanto a su exactitud o a su vigencia, y no puedan ser cancelados o eliminados.

Con el propósito de asegurar la efectividad de estos derechos, complementariamente la ley 19.628 establece tres "*garantías legales".*

(i) En primer lugar, *la información, modificación o eliminación* de los datos es gratuita -y los mismo debe estimarse cuando se pida el *"bloqueo"* de los datos-, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente, siempre y cuando hayan transcurrido seis meses desde la última vez que se hizo uso de este derecho.

(ii) La segunda garantía consiste en que si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos del servicio público debe avisarles a la brevedad posible la operación efectuada; y si no es posible determinar las personas a quienes se les comunicó, debe ponerse un aviso que pueda ser de general conocimiento para quienes usen la información.

(iii) La tercera garantía consiste en que por regla general el derecho de las personas a la *información, modificación, cancelación o bloqueo* de sus datos personales no puede ser limitado por medio de ningún acto, contrato o convención (actos prohibidos por esta ley especial que, de concretarse, serían nulos y sin ningún valor), ...salvo, que la solicitud de información, modificación, cancelación o bloqueo de datos personales impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o

secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.

Y existe un cuarto derecho esencial a favor del titular, a saber, el de obtener una *"indemnización"* del servicio público responsable del banco de datos personales, que debe indemnizar el daño patrimonial y moral que se cause por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal[76].

Como ya vimos, el artículo 15° limita el ejercicio de estos derechos en algunos casos.

17. Competencia de los servicios públicos para publicar datos personales patrimoniales y negativos de los ciudadanos en el sistema de información comercial vigente en Chile.

17.1. La hipótesis de trabajo es la siguiente: *¿aplica el Título III de la ley 19.628 a las deudas y a la morosidad de los ciudadanos frente a las obligaciones patrimoniales de Derecho Público que establece la ley y que no se cumplan?.*

Existen fallos expresos de los Tribunales Superiores de Justicia (ICA de Santiago el 2001, ICA de Concepción el 2002, ICA de Punta Arenas el 2006 y la Corte Suprema) que han establecido la opción de la negativa.

17.2. Sobre el c*ontenido del Título III de la ley 19.628.*

Nada tiene que ver este tópico con la protección de la intimidad o privacidad, tanto en cuanto datos personales o nominativos. Ocurre que la publicidad de la data sobre mora y protestos comerciales es necesaria para mantener la vigencia del orden público económico, y solo un análisis sesgado podría considerar que quien ha vulnerado recurrentemente la buena fe comercial incurriendo en conductas de incumplimiento de obligaciones posee la facultad, constitucional y legal, de invocar el resguardo de su privacidad para evitar la publicación de sus antecedentes negativos.

Los temas de fondo que subyacen son, en consecuencia, los de la necesidad de conocer la solvencia económica de las personas naturales y

[76] Procesalmente, la acción consiguiente puede interponerse conjuntamente con la reclamación destinada a establecer la infracción y se sujeta al procedimiento sumario; en el juicio, el juez debe tomar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que la ley establece; la prueba se aprecia en conciencia; y el monto de la indemnización debe ser establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

jurídicas, y el del acceso al crédito para quienes en el pasado han incurrido en el incumplimiento de obligaciones comerciales; respecto a lo segundo se argumenta que ellos tienen un *"derecho al olvido*", y que en consecuencia la data personal y patrimonial negativa sólo debiera ser publicada y conocida por un determinado lapso de tiempo[77].

En síntesis:

(i) Los datos personales patrimoniales negativos siempre serán tipos de datos públicos, porque así se ha establecido –por la ley 19.628 y antes por un Decreto Supremo Nº950 de 1928- al ser necesario su conocimiento para velar por el orden público económico;

(ii) No se requiere autorización previa del titular individualizado para su comunicación, lógicamente porque él siempre se opondría a que se publiquen sus antecedentes irregulares y, jurídicamente, porque estamos en uno de aquellos casos en que la ley o la voluntad colectiva del legislador prescinde de la voluntad individual del titular;

(iii) Siempre podrán ser corregidos o eliminados si se subsana la situación de mora o protesto patrimonial de que dan cuenta, pero ya no gratuitamente sino que pagando por dicha aclaración, lo cual en derecho también se cuestiona; y,

(iv) No son el único caso legal de información patrimonial que puede ser publicada sin autorización de sus titulares, porque en conformidad a los artículos 2º y 4º también pueden publicarse -en el sector privado- los datos patrimoniales "*positivos"*.

Debiera además precisarse la denominación del Título, ya que sólo alude a aquellos datos que resultan del incumplimiento doloso y/o culposo de las obligaciones comerciales a la mora y a los protestos que queda respaldada con los documentos específicos que la ley señala. Se trata únicamente de los que denominamos *"datos patrimoniales negativos"*, y no de los datos patrimoniales *"positivos",* que como sabemos, en conformidad al artículo 4º de la ley 19.628 provienen de fuentes públicas y pueden tratarse sin autorización de sus titulares.

El aartículo 17 es la ley que, en el contexto de obligaciones que se originan en un previo incumplimiento patrimonial, establece que *"los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial*" con la condición de que ellas consten en los siguientes documentos: i)

[77] El Título III sobre la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, por ende, podría incluso no estar en la ley 19.628.

letras de cambio y pagarés protestados; ii) cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa.

Alude luego a la posibilidad de comunicarse "*el incumplimiento*" -sigue siendo el supuesto básico- "*de obligaciones derivadas de*" (el ordenamiento es nuestro): i) mutuos hipotecarios y de préstamos o créditos de bancos, ii) sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, iii) organismos públicos y empresas del Estado sometidas a la legislación común, y, (iv) sociedades administradoras de créditos otorgados para compras en casas comerciales. Legalmente se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario (INDAP) a sus usuarios.

Agrega la norma que "*también podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo*" -el que a la fecha no ha sido citado ni sabemos si existe la voluntad política de hacerlo-. El requisito instrumental se repite, porque la ley exige que las obligaciones estén sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales además debe constar el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. Y nuevamente excepciones: la ley señala que no podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas.

El artículo 18 es la norma que establece plazos para publicar la información sobre mora y protestos. Después de su última modificación, dispone que *"en ningún caso pueden comunicarse los datos"* -no caben acá las interpretaciones-, a que se refiere el artículo anterior y que se relacionen con una persona identificada o identificable, luego de transcurridos 5 años desde que la respectiva obligación se hizo exigible. El plazo inicial en 1999 era de 7 años, y las consideraciones para su rebaja no fueron de índole técnica. Agrega que *"tampoco se podrá continuar comunicando los datos"* ya referidos cuando la obligación sea pagada o se extinga por otro modo legal.

El artículo 19 dispone que el pago o la extinción por cualquier otro modo de las obligaciones en estudio, no produce *"la caducidad"* o *"la pérdida de fundamento legal de los datos respectivos"* para los efectos del artículo 12, es decir, para que sea posible recurrirse de derecho de acceso ante el responsable del sistema, obviamente -agrega la ley- mientras estén pendientes los plazos que establece el artículo 18.

Agrega que al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, *"éste avisará tal hecho"* -lo que en la práctica nunca ocurre-, y *"a más tardar dentro de los siguientes siete días hábiles"*, al responsable del registro o banco de datos accesible al público que en su

oportunidad comunicó el protesto o la morosidad, con el objeto de consignarse el nuevo dato que corresponda.

17.3 *El fallo contra la Tesorería General de la República que le impidió publicar antecedentes de mora de los contribuyentes en los sistemas de la empresa Dicom S.A.*

La Tesorería General de la República, como una forma de cobrar las deudas de los contribuyentes en el pasado optó por informar de las situaciones de morosidad, lo que fue judicialmente declarado ilegal por falta de competencia el año 2002 (Rol 3713-2002) y ratificado por la Corte Suprema el año 2003 (Rol N°211-2003).

Nos referimos a la causa *Recurso de Protección Cáceres Arévalo/Dirección Regional del Servicio de Tesorería Octava Región,* acogido por infracción del Nº 4 del artículo 19 de la Constitución Política, ante la publicación encargada de información de deudas tributarias en la empresa DICOM.

En primer lugar el recurrente fue una persona natural afectada, y lo que se resolvió fue que a pesar de que la Tesorería poseía facultades administrativas y judiciales de cobro que difieren de los derechos de cualquier otro acreedor y la ley le otorga una posición relevante para tal objeto, en el caso del recurso interpuesto *la ley 19.628 no la autorizaba expresamente y los artículos 17, 18 y 19 no permitían la inclusión de deudas de carácter tributario, patrimoniales y negativas (estar moroso) en los registros de DICOM, máxime cuando la Tesorería no poseía facultades legales para hacerlo.*

Concretamente, se consideró en el fallo en comento que la cobranza sólo podía ejercerla en forma administrativa, actuando el Tesorero como juez sustanciador; judicialmente, ante los tribunales de justicia, incluso ejerciendo la coacción sobre los deudores, y extrajudicialmente mediante los procedimientos reglados que establece la ley, pero carecía de facultades para emplear otros arbitrios no expresamente autorizados en su Ley Orgánica o en el Código Tributario. Dijo la resolución en el voto de mayoría:

> *"CON LO RELACIONADO Y CONSIDERANDO: 3° ...se desprende que el Servicio de Tesorerías cuenta con facultades especiales y determinadas para efectuar el cobro de los tributos, multas y demás créditos en conformidad a la ley, pero esta cobranza sólo puede ejercerla en forma administrativa, actuando el Tesorero como juez sustanciador; judicial, ante los tribunales de justicia, incluso ejerciendo la coacción sobre los deudores, y extrajudicialmente mediante los procedimientos reglados que establece la ley, pero carece de facultades para emplear otros arbitrios no expresamente autorizados en su Ley Orgánica o en el Código Tributario, como es el caso de enviar la nómina de sus deudores a Registros de Morosidades y Protestos, como ha ocurrido en la especie, lo cual resulta ilegal y una forma*

arbitraria de presión para el cobro, pues es público y notorio que quien figure en tales registros de DICOM queda inhibido de realizar diversas operaciones comerciales y crediticias".

"El bien jurídico protegido por la ley Nº 19.628 de 28 de agosto de l998, es la honra de las personas y por eso se regula la protección de datos de carácter personal y especialmente el tratamiento de los datos en registros de bancos de datos, cuidando siempre la garantía constitucional mencionada. Dicha ley tampoco autoriza la inclusión de deudas de carácter tributario en tales registros, que es el caso planteado en el presente recurso, en que los impuestos están reclamados y pendientes las apelaciones".

La sentencia fue acordada con el voto en contra del Ministro Sr. Juica (que, sin señalarlo, recogió el criterio del Dictamen de la Contraloría):

"...atendido al mérito de los antecedentes y lo dispuesto en el artículo 147 del Código Tributario en relación con el artículo 161 Nº 6 del mismo cuerpo legal estuvo por revocar la sentencia apelada y rechazar el recurso de protección por estimar que no ha existido de parte del recurrido acto ilegal o arbitrario, susceptible de enmendar por esta vía, por considerar que las actuaciones reclamadas de la Tesorería, tienen su fundamento en información que por su naturaleza es pública, en consideración a que dice relación con un proceso en actual tramitación al cual la ley no le ha dado el carácter de secreto o confidencial".

Nuestros comentarios al fallo:

(i) Estimamos errada la interpretación, porque si bien es cierto no se alude expresamente a las obligaciones relativas a la morosidad tributaria, del tenor literal del artículo 17 la publicación de los antecedentes de los deudores morosos tributarios cabe considerarla comprendida en la expresión *"...incumplimiento de obligaciones derivadas de organismos públicos".*

(ii) No obstante que el punto no fue debatido en el parlamento, a mayor abundamiento la lectura a contrario sensu del artículo 21 de la misma ley -que no fue considerado por la Corte Suprema- establece que si pueden comunicarse a terceros los datos por los servicios públicos, sólo que hasta antes de haber prescrito la acción administrativa -en este caso de cobro de impuestos devengados y no pagados (mora tributaria)-.

(iii) Como se consigno en el voto de minoría, el *artículo 169* del Código Tributario consagra, dentro de los procedimientos administrativos y judiciales para el cobro de los tributos morosos y de las obligaciones tributarias, que el Servicio de Tesorerías puede confeccionar listas o nóminas de deudores que se encuentren en mora, con la individualización completa de los mismos y de la cantidad adeudada. Complementariamente, el *artículo 185* señala que se deben emplear todos los medios posibles para dar publicidad a las subastas que resulten

de los procedimientos de cobro que tramite la Tesorería General de la República. Estas medidas, necesarias para efectuar el cobro de los tributos, multas y demás créditos en conformidad a la ley, pueden incluir la opción de publicar los datos sobre morosidad vía bases de datos especializadas.

Empero, frente al mismo tema lo dictaminado por la Contraloría General de la República en Octubre del mismo año -como veremos- fue diverso a lo resuelto por los Tribunales Superiores de Justicia[78].

Porque es discutible constitucional, legal y procesalmente proyectar la Garantía Constitucional que asegura a todas las personas en el artículo 19 N°4 -*el respeto y protección de "la vida privada... de las personas y sus familias*"- al ámbito de datos personales o nominativos procesados computacionalmente -como los comunicados por la Tesorería al sistema de información comercial- cuando éstos por su naturaleza son antecedentes públicos y no privados o íntimos.

A esta fecha, existe pendiente de tramitación un proyecto de ley tendiente a otorgarle expresamente la competencia a la Tesorería General de la República, contenido en el Boletín 4959 y que busca precisar el ámbito de aplicación de la ley 19.628.

El proyecto recoge los argumentos de los tribunales, rechaza los de la Contraloría, califica de ilegal y arbitraria la comunicación a esta fecha de datos sobre morosidad vía Convenio[79], y propone modificar el artículo 20 de la ley 19.628. Junto al hecho de que una vez sometido este proyecto de ley a trámite necesariamente se presentarán indicaciones y argumentos que pueden darle mayor amplitud a lo que se busca legislar, lo que se propone puede interpretarse a futuro como la determinación del único contenido posible para los convenios de intercambio de información.

Dice al artículo propuesto:

---

[78] En síntesis: en Octubre del año 2002 y mediante el ***Dictamen 25.336*** la CGR dictaminó que la Tesorería podía celebrar convenios de intercambio de información sobre datos de mora y protestos de los contribuyentes. Posteriormente, el año 2003 y en un ***Dictamen 43.866***, complementa y precisa que ella puede celebrar dichos convenios -sobre datos tributarios y sobre obligaciones morosas o patrimoniales negativos- aún cuando el artículo 17 de la ley 19.628 no los mencione expresamente. El criterio anterior atiende a considerar que la TGR posee facultades amplias que le otorga su Ley orgánica, para celebrar contratos relacionados con el cumplimiento de los fines del mismo, en este contexto y a propósito de información que es *per se* pública y no secreta o reservada.

[79] Se cuestiona, en concreto, el que la Tesorería General de la República celebró un convenio en octubre del 2002, con las empresas de información (Dicom, Data Business y posteriormente Sinacofi) para publicar la lista de deudores que en los últimos tres años habrían tenido una deuda tributaria demandada y notificada, requerida de pago o probablemente con algunos embargos trabados, que no se hubiesen acercado a la entidad a plantear su caso y a manifestar la voluntad de celebrar algún convenio.

Artículo único: Reemplazase el artículo 20 de la ley N° 19.628[80], por el siguiente: *"Artículo 20.- El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia, que se encuentren incluidas expresamente en el artículo 17 de esta ley, con sujeción a las reglas. En esas condiciones, no necesitará el consentimiento del titular.".*

En cuanto a los fundamentos:

(i) Interpretan el artículo 17 de manera restrictiva, y de la referencia a que sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial que cumplan ciertos requisitos de constancia de la obligación, concluyen que clara e imperativamente ello no ocurre con la información tributaria[81].

(ii) No obstante referirse al Dictamen 25.336 del año 2002 de la Contraloría, señalan que el Convenio firmado es arbitrario e ilegal.

(iii) Citan a la Sala Constitucional de la Corte Suprema, que resolvió expresamente que la Tesorería General de la República, al ordenar la publicación de la deuda del recurrente en el Boletín de Dicom, incurrió en una conducta ilegal y arbitraria contemplada en el N° 4 del artículo 19 de la Constitución Política de la República, que se refiere a la protección de la vida privada de las personas, por lo que la presente acción constitucional debe ser acogida.

(iv) También la citan, cuando señala que el Servicio de Tesorería únicamente puede informar datos de carácter personal en la medida que éstos versen sobre algunas de las obligaciones a que se refiere el *artículo 17* de la citada ley (la 19.628, por cuanto así lo ordena el *artículo 20* del mismo cuerpo legal, y no aquellos que se originan en obligaciones provenientes de impuestos y multas de carácter tributario.

---

[80] Dice la norma, ya analizada en extenso, a esta fecha: *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.*

[81] Cuando se toma como fundamento un artículo 17 de la ley 19.628, que estableció un listado taxativo o *"numerus clausus*" de antecedentes comerciales negativos susceptibles de ser publicados "por primera vez" por empresas particulares (listado que obviamente no podía ni necesitaba mencionar expresamente a la morosidad tributaria) , y ello se le hace aplicable a las funciones de la Tesorería, se opta por desconocer su competencia y aplicársele reglas generales que, como se comprende del estudio de las Actas, no fueron establecidas ni pueden tener preeminencia sobre intereses superiores de orden y servicio público. Estos son, en concreto, la recaudación fiscal, evitar la morosidad tributaria e informar a todos los actores del sistema comercial las irregularidades que, de mantenerse anónimas bajo una supuesta protección de la privacidad consagrada como garantía fundamental en la Constitución, sólo generará inestabilidad.

(v) Consideran que parte importante de los cobros que aplica Tesorería se fundamentan en giros basados en liquidaciones que se encuentran pendientes judicialmente, pues el afectado generalmente ha recurrido a la justicia ordinaria, y que no parecería razonable que dicho Servicio exponga ante terceros, y como deudas efectivas, montos que aunque girados, se encuentran judicialmente controvertidos.

Somos de la opinión que los reparos se han hecho en base a la errada interpretación de los alcances de lo establecido en los artículos 17 y 20 de la ley 19.628. En síntesis, ellos establecen un listado taxativo de casos en los cuales se pueden publicar datos patrimoniales (negativos, aunque no se dice), lo que no obstante aplicarse sólo a empresas particulares, se hace extensivo a los servicios públicos en general y a la Tesorería en particular, porque el artículo 20 establece que 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".*

La interpretación y lo resuelto judicialmente desconoce un artículo clave, el 4° (que también es "regla precedente" según el artículo 20), que permite el tratamiento o procesamiento de datos cuando otras leyes -diversa de la 19.628- así lo dispongan. Es precisamente lo que establece el Código Tributario, no como una forma de *"violar la privacidad*" o *"afectar a la honra*" de los contribuyentes, sino como un medio para aportar a la vigencia del Orden Público Económico[82] en materia tributaria[83].

Reiteramos: el *artículo 169* consagra, dentro de los procedimientos administrativos y judiciales para el cobro de los tributos morosos y de las obligaciones tributarias, que el Servicio de Tesorerías puede confeccionar listas o nóminas de deudores que se encuentren en mora, con la individualización completa de los mismos y de la cantidad adeudada. Complementariamente, el *artículo 185* señala que se deben emplear todos los medios posibles para dar publicidad a las subastas que resulten de los procedimientos de cobro que se tramiten. Estas medidas, necesarias para efectuar el cobro de los tributos, multas y demás créditos en conformidad a la ley, claramente incluyen la opción de publicar los datos sobre morosidad vía bases de datos especializadas.

---

[82] Siempre, en materia de tratamiento de datos personales y patrimoniales "negativos", cuando exista un conflicto entre una garantía individual como la privacidad o intimidad y el orden público económico, debe primar el segundo. Nunca, salvo error o caducidad, un incumplidor legal o comercial podría reivindicar la defensa de su privacidad, intimidad o confidencialidad para mantener anónimo su incumplimiento.

[83] Es relevante este tema, porque en base a una errada interpretación de la ley 19.628 -sobre tratamiento de datos personales- y sus fundamentos, se menoscaban facultades inherentes al ente fiscalizador y, en definitiva, se atenta contra la estabilidad del Orden Público Económico.

La Tesorería General de la República, de la mano además de competencias otorgadas por su Ley Orgánica, con un fin de servicio público y como una forma de apoyar el cobro de las deudas de los contribuyentes optó por informar las situaciones de morosidad. Y lo ha hecho en base a información que por su naturaleza ya es pública, no íntima, no privada, no confidencial y no secreta, al tratarse de morosidad tributaria (impuestos y multas) existente con posterioridad al término de todas las instancias de cobro administrativo.

Debe tenerse nuevamente a la vista (…debe hacerse constantemente la verdad) la llamada "*Teoría de las Esferas",* para entender que existen datos que pertenecen a una esfera *"pública"* y otros a una *"privada o íntima"*, y que la información que un servicio público genera por el hecho de cumplir con los fines que por ley debe asumir, claramente forma parte de la primera esfera y no es privado, no es íntimo y no puede ser privado del conocimiento de la sociedad toda por la mera voluntad de su titular, máxime cuando se trata de un contribuyente infractor de la normativa legal-tributaria.

La información personal sobre la situación tributaria de un contribuyente –tanto en cuanto no sea de aquella amparada por el secreto tributario consagrado en el Código Tributario- cabe dentro de lo que la doctrina constitucionalista denomina la *"esfera social*" de las personas. Los órganos estatales y las empresas comerciales que a partir de nuestro número de identificación nacional procesan información personal están manejando o procesando en consecuencia ciertos "*datos públicos".*

La modalidad implementada por la Tesorería de informar sobre la situación tributaria de los contribuyentes no constituye una práctica ilegal atentatoria contra la garantía constitucional consagrada en el artículo 19N°4 de la CPE, toda vez que se persiguen fines de Orden Público Económico en materia tributaria y que, sin necesidad de requerirse autorización previa, se trata de dar a conocer antecedentes personales de aquellos que constituyen información pública –de naturaleza no secreta o reservada-, en los términos de la ley 19.628 cuando se trata de personas naturales o de las normas tributarias cuando se trata de personas jurídicas, sobre todo si se trata de antecedentes sobre un eventual comportamiento tributario irregular.

17.4 *Recurso de protección en contra de la Dirección del Trabajo (referencia).*

En Junio del 2007 la Tercera Sala de la Corte Suprema determinó que la Dirección del Trabajo incurrió en una conducta arbitraria e ilegal al enviar al Boletín Laboral de Infractores a la Legislación Previsional los datos de mora de un

particular (cinco cotizaciones declaradas e impagas en una AFP), registro administrado por la empresa Equifax S.A[84].

Este fallo vino a reforzar la tesis de que los órganos de la Administración no pueden enviar información de esta naturaleza a publicarse en los sistemas de información comercial, salvo que el afectado -en conformidad a la regla general del artículo 4° de la ley 19.628- haya expresado previamente su consentimiento.

18. Modificaciones en curso a la ley 19.628. Cuadro comparativo con lo establecido por el Boletín 6120, a esta fecha en trámite parlamentario en la Cámara de Diputados.

18.1 *Breves explicaciones sobre los objetivos, fundamentos y contenidos de la modificación legal en curso.*

Este proyecto ha sido, sin duda alguna, el más importante de todos los relacionados con las modificaciones a la ley 19.628, e implicó un cambio radical o un viraje de 180° en comparación a la institucionalidad jurídica existente. Hubo un cambio notable de escenario o de perspectiva, porque desde lo que era una normativa dictada para legalizar, validar o blindar jurídicamente el negocio de las empresas responsables de bases de datos, se migró o se pasó a centrarse en la real protección de los derechos de los titulares de datos personales o nominativos, tanto para las personas naturales como para las personas jurídicas o empresas -mismas que, sin justificación válida, habían sido preteridas como titulares de derechos en la ley 19.628 del año 1999-.

Embarcado el Gobierno de la época en un proceso de incorporación a una entidad comercial e internacional como la OECD, quedó en evidencia que las deficiencias de la legislación nacional estaban siendo e iban a seguir siendo una barrera de entrada -solucionada en la práctica con verdaderos *"parches"* jurídicos[85]- para la incorporación de Chile a la entidad, y a consecuencia de esta

[84] A esta fecha y al cierre del Informe no hemos logrado tener el fallo a la vista. Una nota de prensa puede verse en la URL http://www.conadecus.cl/index2.php?option=com_content&do_pdf=1&id=350

[85] En efecto, y a modo de ejemplo: *"…al ser considerado actualmente Chile como un país con un nivel no adecuado de protección en materia de datos personales, ha debido someterse al mecanismo de las cláusulas tipo en los respectivos contratos que se suscriben con empresas españolas, con el fin de alcanzar las autorizaciones que correspondan por la Agencia Española de Protección de Datos cuando se pretenden realizar transferencias internacionales de los mismos (servicios globales). Es este el obligado camino que nuestro país deberá seguir mientras no se estatuya una legislación que le permita solicitar a la Comisión Europea la declaración de adecuación de la protección".* Citado de la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

traba, no tuvieron otra opción que la de presentarse ante los evaluadores europeos promoviendo e impulsando los cambios en materia de Políticas Públicas y las normas chilenas relacionadas, y comprometiendo formalmente ante el ente internacional la posterior aprobación en el Parlamento de las modificaciones legales necesarias para la estandarización o adecuación normativa a las directrices y Políticas del órgano europeo.

El proyecto buscó cambiar radicalmente el nivel jurídico de protección de los datos personales o nominativos de los chilenos y transformar al Consejo de Transparencia en la autoridad de control que en Chile administre un registro obligatorio de responsables de bases de datos personales, tanto en el sector público como en el privado.

Desde que fue aprobada en 1999 la ley 19.628 habían transcurrido varios años, que demostraron cabalmente y sin lugar a dudas que la norma era insuficiente y que no se ajustaba a los estándares internacionales; ella puso énfasis en el derecho a tratar datos de carácter personal para las empresas y entidades gremiales y no reconoció, como primer derecho, el de los titulares de datos personales a controlar los mismos, de la mano de la falta de anonimato que posibilita un registro y del apoyo administrativo de un órgano ad hoc.

Parar terminar estas ideas preliminares. El proyecto contenido en el Boletín 6120 buscó, esencialmente y adecuándose a los estándares de la Unión Europea y de la OECD, lo siguiente:

(i) subsanar la inexistencia de un registro de responsables privados de bases de datos y de un órgano fiscalizador autónomo o Autoridad de Control;

(ii) mejorar los estándares de protección y resguardo de los derechos de los titulares de datos personales y, conferir las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos;

(iii) establecer como regla general que la información no sea pública y que requiera de la autorización de sus titulares para procesarse;

(iv) prohibir la transferencia internacional de datos personales a terceros países que no tuvieran un adecuado sistema de protección;

(v) aumentar las condiciones de seguridad de sistemas en el tratamiento de datos;

(vi) establecer infracciones y sanciones; y,

(vii) otorgar protección a las personas jurídicas.

18.2 *Fundamentos del Mensaje.*

Alude el Mensaje *-que es, por cierto, el elemento clave para posteriormente entender e interpretar el articulado-,* a las razones de los cambios legislativos propuestos, y a que *"paradojalmente"* la ley 19.628 puso énfasis en el derecho a tratar o procesar computacionalmente datos de carácter personal y no reconoció como primer derecho, el de los titulares de datos personales a controlar -o autodeterminar- los mismos.

Constató que se trataba de una *"regulación insuficiente",* y que a su respecto las principales críticas vertidas eran (i) la inexistencia de un registro de responsables privados de bases de datos y de un órgano fiscalizador autónomo; (ii) el haberse establecido que *"la verdadera regla general"* era que la información fuese pública y que no se necesitaba la autorización de sus titulares para procesarse, contemplándose un gran caudal de excepciones a la exigencia de autorización previa del titular; (iii) el no haberse prohibido la transferencia internacional de datos personales a terceros países que no posean un adecuado sistema de protección; y, (iv) el no haberse otorgado protección a las personas jurídicas.

En cuanto a la *"necesidad de una autoridad de control"*, consignó que para velar por el adecuado cumplimiento de las disposiciones relativas al tratamiento de datos se requería una autoridad dotada de competencias y herramientas eficaces, para dictar normativas sobre la materia, para fiscalizar, para adoptar medidas de resguardo y para sancionar los incumplimientos mediante la aplicación de multas.

Reconoce el Mensaje que el no haberse contemplado un organismo administrativo, Agencia o Superintendencia (cosa que personalmente propusimos el año 1990) que se encargara de velar por el cumplimiento de sus normas -limitándose a entregar al Registro Civil e Identificación el deber de llevar un registro de las bases de datos a cargo de organismos públicos-, era imposible fiscalizar el cumplimiento de las normas de la ley y muchas de sus disposiciones se habían tornado fútiles.

Siempre en cuanto al *"establecimiento de una autoridad de control",* se mencionaba que el proyecto establecía que la autoridad encargada de velar por el cumplimiento de la normativa, tanto la contenida en esta ley como en otros cuerpos normativos, sería el Consejo para la transparencia creado por la ley N° 20.285, que pasaba a denominarse "*Consejo para la transparencia y protección de datos personales"*.

Atendida esta nueva competencia, según el Mensaje el órgano o la autoridad de protección de datos de Chile tendría entre sus funciones esenciales las siguientes:

(i) mantener un Registro Único Nacional de Bases de Datos;

(ii) fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estimara pertinente;

(iii) inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley;

(iv) requerir la inscripción de los bancos de datos que no estén registrados en el Registro Único Nacional;

(v) potestad normativa, para dictar instrucciones de carácter general o particular respecto de las condiciones de legitimidad de un tratamiento de datos;

(vi) conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos;

(vii) ejercer potestades sancionadoras contra los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos; y,

(viii) requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro.

Se refirió luego a *"la necesidad de adecuarse a estándares internacionales"*, concretamente, a las recomendaciones de la OCDE (Organización para la Cooperación y el Desarrollo Económico), y a cumplir con el estándar de protección de datos personales de la Unión Europea.

Se abocó luego el Mensaje a la *"descripción de la propuesta"*, afirmando que el proyecto tenía por objeto modificar dos cuerpos normativos; por una parte la ley 19.628 sobre protección de la vida privada y, por otra, la ley 20.285, de transparencia de la función pública y de acceso a la información de la Administración del Estado, para *"...dar una eficaz respuesta a las exigencias de protección, ya que, por una parte, se mejoran los estándares de protección y resguardo de los derechos de los titulares de datos personales y, por otra, se confieren las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos".*

Se refirió luego el Mensaje al *"reconocimiento explícito de derechos"*; en concreto, a los siguientes: (i) a consagrar explícitamente el derecho de las personas a controlar sus datos, en el art. 1° de la ley, porque en la ley 19.628

únicamente se hacía referencia al derecho a efectuar tratamiento de datos personales; y, (ii) a que se ampliaba el margen de sujetos protegidos, porque se partía de la base que la información sobre las personas jurídicas era tan relevante como la de las personas naturales y también merecía ser resguardada, considerándose en consecuencia como legitimados activos del derecho de acceso y titulares del habeas data tanto a las personas naturales como a las jurídicas.

18.3 *Cuadro comparativo*.

Ley 19 628 vigente - Normas específicamente referidas a servicios públicos.	**Proyecto de ley en trámite en la Cámara de Diputados - Normas específicamente referidas a servicios públicos**
Título IV: Del tratamiento de datos por los organismos públicos - *artículo 21*.	Se precisa que la información relativa a sanciones administrativas o penales (v.gr. multas de la TGR) sólo podrán ser "tratadas" (concepto amplísimo, que incluye su comunicación a terceros…) por organismos públicos y dentro del marco de su competencia. * *No queda claro si pueden publicarse en sistemas de mora y protestos; pareciera que no; antes se le ha negado en el Parlamento la facultad a la TGR.*
Título IV: Del tratamiento de datos por los organismos públicos - *artículo 22*. A esta fecha existe un registro público sólo nominal e informativo, administrado por el Registro Civil, lo que no importa grado de fiscalización alguno.	Se establece que los registros o bancos de datos "de titularidad pública" poseen la obligación de anotarse en un registro público (RUNBD), diverso al administrado por el Registro Civil (sólo nominal) que se suprime, para la fiscalización de los titulares de los datos y de la Autoridad de Protección de Datos Personales.
Ley 19 628 vigente - Normas generales que también aplican a los servicios públicos	**Proyecto de ley en trámite en la Cámara de Diputados - Normas generales que también aplican a los servicios públicos**

A esta fecha los responsables de bases de datos (particulares sobre todos) se consideran de hecho propietarios de la información que almacenan (contenido), lo que sólo es correcto respecto del continente y de cara a terceros que quieran acceder a la base de datos.	La nueva ley aclara de hecho la calidad de "poseedores o meros tenedores" de los datos, respecto de sus titulares, y al exigir autorización previa o información posterior restringe la posibilidad de disponer del contenido nominativo de las bases de datos. Se enfatiza expresamente que lo central del objeto de la ley es permitir que los titulares de los datos controlen y fiscalicen el procesamiento de sus antecedentes.
Las eventuales medidas de seguridad de sistemas dependen solo del criterio del servicio público responsable de la base de datos.	Obligación de implementar las medidas ("técnicas y administrativas" dice la ley) de seguridad de sistemas que *por Reglamento* (lo cual hace rígido un tema que per se es cambiante) determinará la Autoridad de Control, las que serán fiscalizadas. * Habría que cambiar la exigencia de un reglamento, por ser muy rígido y engorroso de modificarse, y establecer que se exigirá el cumplimiento de normas como las ISO, debiendo los servicios públicos ajustarse a ellas en la medida de sus posibilidades.
	Restricciones especiales nuevas para la eventual transferencia de datos a una entidad ubicada fuera de Chile (se complica la posibilidad de almacenar información en servidores no ubicados en Chile a través de Internet).
La autorización previa y expresa del titular de los datos que serán procesados sólo se exige nominalmente, para casos que no sean *fuentes públicas de información*, y puede ser conseguida mediante fórmulas contractuales amplias o no	Cuando el responsable solicite registrar datos personales o cuando los obtenga de terceros (otra empresa), deberá informar un cúmulo de antecedentes al titular individualizado (existencia de registro, fin, obligatoriedad o no de entregarlos, derechos que posee, etcétera), ...con lo cual, *la futura ley contempla una real*

específicas - artículo 4°.	*exigencia de autorización previa, informada, clara, inequívoca, precisa y expresa del titular de los datos*. Cuando la autorización no se requiera legalmente (como es el caso de los servicios públicos), existe obligación complementaria de *informar o comunicar* el registro y/o cualquier operación (v.gr, una cesión de la base de datos a otra empresa) en un plazo de tres meses. * Un servicio público no podrá ser cedente ni cesionario de datos personales, ni canjearlos con otras bases de datos para elaborar o mejorar perfiles (minería de datos) sin autorización expresa y/o sin comunicar posteriormente la operación realizada al titular de los datos. Habría que precisar o agregar la facultad que esa obligación los servicios públicos podrán cumplirla vía e-mail.
Conforme los artículos 2° y 4°, la regla general en Chile es que todas las fuentes de información son públicas, y pueden tratarse datos personales sin autorización de sus titulares y con fines diversos a los declarados al recopilarse.	Se terminan las categorías amplias de *"fuentes públicas de información*", que pasan a ser excepcionales y definidas taxativamente, y que permiten que los datos personales sean procesados sin autorización de sus titulares.
No existe a la fecha real obligación de secreto, porque por regla general las bases de datos son fuentes públicas de información.	La obligación de guardar secreto y reserva pasa a ser la regla general para los "responsables" y "encargados" de bases de datos personales, y su violación, es delito informático en conformidad al artículo 4° de la ley 19.223. * Esto es diverso del secreto tributario o del secreto estadístico; es un secreto amplio de toda base de datos personales.

Los titulares sólo pueden reclamar ante tribunales de justicia; hasta la fecha son casi nulos los recurso de "derecho de acceso" interpuestos.	Los titulares de los datos podrán reclamar breve y sumariamente ante la autoridad de protección de datos, sin necesidad de recurrir ante los tribunales de justicia. Consecuencia: ...las multas se aplicarán en forma rápida, y la reiteración en su aplicación puede ocasionar la cancelación de la autorización para ser responsable de bases de datos y la eliminación del registro.
Nadie fiscaliza el uso de los datos de acuerdo a los fines declarados al registrarse.	La autoridad de control fiscalizará especialmente el uso de los datos conforme a los fines declarados e informados al momento de la recopilación.
Sólo las personas naturales son amparadas por la ley 19.628 como titulares del derecho de acceso.	Los representantes legales de las personas jurídicas también podrán fiscalizar el uso de sus antecedentes.
No existe claridad legal acerca de la identidad del "responsable de la base de datos"; por ser el que toma decisiones sobre ella, en Doctrina se considera que serían los Directores de los servicios públicos.	El servicio público deberá definir y registrar formalmente a los "responsables" y a los "encargados" de las bases de datos personales.
El derecho de acceso sólo puede ejercerse ante el responsable de la base de datos, si es que se conoce su existencia.	Antes de accionar contra el responsable de la base de datos, el titular y respecto de sus antecedentes puede acudir al Registro Único Nacional de Bancos de Datos para identificar al responsable.
Ante la negativa del responsable de la base de datos o si nada dice en 48 horas, puede accionarse ante los tribunales.	Ante la negativa del responsable o si nada dice en 10 días, podrá accionarse ante el Consejo de Transparencia en forma sumaria y administrativa.
No se contemplan sanciones administrativas.	Se establecen infracciones administrativas leves, graves y gravísimas, que llegan hasta 10.000 UTM. Ejemplo de sanciones: (i) si el responsable

	no responde "oportunamente", 200 UTM; (ii) si no informa legalmente al recoger los datos, 200 UTM; (iii) si trata datos con fines distintos a los que motivan la recogida, 5000 UTM; (iv) si trata datos son consentimiento expreso del titular, 5000 UTM; (v) si comunica o cede datos en forma ilegal, 10.000 UTM; etcétera.

C. Acerca de la naturaleza jurídica de los datos personales "RUN" y "RUT" y su procesamiento por los servicios públicos.

1. *El concepto RUN alude al Rol Único Nacional.*

Este código identificativo en el hecho suele usarse o asociado a los nombres y apellidos de la persona natural registrada bajo él, o en forma independiente de los nombres. En materia de sistemas informáticos, basta el uso del RUN para asociar y cruzar en torno a él otros antecedentes o datos personales, y siempre se entenderá y se sabrá que se alude a una persona determinada, identificada e identificable. Lo mismo vale para el denominado "RUT", que analizamos más abajo[86].

Fue establecido o implantado este instrumento en el mes de Julio del año 1973, para fines de identificación y estadística, mediante un Decreto Supremo N°18 de Enero del mismo año. En virtud de esta norma, es que los servicios públicos (v.gr. Aduana, TGR, SII, INP, SENCE, etc.) no necesitan la autorización expresa *"de los ciudadanos"* identificados para operar con RUN o RUT a que alude el artículo 4° de la ley 19.628, porque es la ley la que los faculta para hacerlo.

Se consideró al efecto en 1973 que la propuesta fue el resultado del trabajo de una Comisión Coordinadora para la implantación de un Rol Único a través de un sistema de computación; que atendidos los avances demostrados por el Rol Único Tributario, el número nacional de identificación que otorgaba el SRC sería el

[86] Se ha dicho que "*...el hecho de poseer en Chile un sistema de identificación con un Rol Único Nacional ahorra costos de levantamiento de información y evita errores y duplicidades, lo que en muchos casos compensa la pérdida de libertad de los ciudadanos que renuncian…."* (en estricto rigor no lo hacen ellos, sino la ley que está por sobre la voluntad de ellos) *"…a su privacidad frente al Estado, al otorgarle la información".* No se debe olvidar que es el Estado el que asigna ese número al ciudadano cuando se inscribe el nacimiento, porque una ley faculta al efecto al Registro Civil para otorgarlo, lo mismo que ocurre en relación al RUT tributario en materia de inicio de actividades.

elemento básico para la implantación del Rol Único Nacional; y que su inmediata aplicación era consecuencia de las ventajas para el procesamiento electrónico y el intercambio de información estadística derivadas del RUN. Y se determinó, para las personas naturales, que el RUN estaría contenido o sería el mismo número que el ya existente RUT.

El objetivo esencial fue el de permitir que la información estadística referida a cada persona, sea natural o jurídica, pudiera ser procesada electrónicamente sobre la base de un número de identificación válido para todos los registros en que debieran inscribirse esas personas, sea en razón de su estado, de su actividad, del ejercicio de derechos políticos de sus obligaciones tributarias o de cualquiera otra actuación que les concerniera.

Se estableció que el Servicio de Registro Civil llevaría un archivo maestro en el que se anotarían los datos comunes de las personas, para que luego, los distintos organismos e instituciones, en forma obligatoria y en base al RUN, completaran sus registros sectoriales con aquellos que correspondieran a sus actividades o funciones. Y de cara a su aplicación obligatoria, se estableció una implementación progresiva y fiscalizada para que todos los órganos estatales regularan los detalles de la implantación del RUN en sus propios registros que les competa elaborar o fiscalizar.

2. *El concepto RUT alude al Rol Único Tributario.*

Si un dato es un antecedente que da cuenta de un hecho o de una característica determinada, el RUT da cuenta de que una persona natural o jurídica, correctamente individualizada, ha iniciado actividades para efectos tributarios, en una fecha determinada, señalando un domicilio legal al efecto, y demostrando poseer nombres y apellidos o razones sociales para el caso de las empresas. Legalmente el dato RUT sólo es de aplicación tributaria y su objetivo no es el de identificar personas sino "*contribuyentes".*

En el hecho o en la práctica, este número e identificativo que permite indexar computacionalmente información nominativa referida o atribuida a las personas naturales y jurídicas se usa en diversos sectores de la sociedad, y *aisladamente considerado se percibe como un dato público per se porque nace para operar en la esfera social de una persona,* salvo que sea asociado con otros antecedentes o datos personales o que sea procesado por servicios públicos con un fin distinto que aquel que corresponda según sus competencias de Derecho Público.

No obstante, por entenderse que un RUT es un dato publico *per se* ante los servicios públicos, no significa que ellos puedan entregarlo libremente a terceros en forma masiva y sistematizados (salvo casos como el SERVEL, porque la ley lo faculta expresamente), o que los particulares deban legalmente o en derecho comercializarlos sin autorización del titular *(…sólo de hecho pueden, y lo hacen*),

precisamente porque lo comercializado seria la identidad de las personas. Más claro quizás, sería partir el análisis de entender que ni el nombre ni el RUT deben ser considerados datos públicos *per se*, y que si por ejemplo el Registro Civil o la Aduana lo usan es sólo porque la ley los faculta expresamente, y que una autorización de esta naturaleza no existe para los particulares[87].

El RUT, heredero del antiguo *"Rol General de Contribuyentes"*, fue creado y sus normas de aplicación fueron establecidas mediante el DFL N°3 del año 1969, del Ministerio de Hacienda, para que existiera un sistema que permitiera identificar a todos los contribuyentes del país -en los diversos impuestos-, para mantener un control del cumplimiento tributario, y porque una adecuada identificación de los contribuyentes (personas naturales, jurídicas, comunidades y asociaciones que causen y/o deban retener impuestos) permitiría simplificar y agilizar los procedimientos administrativos tanto de la Tesorería General de la República como del Servicio de Impuestos Internos.

Su concordancia con el RUN es obligatoria, por cuanto el artículo 1° del DFL 30 establece que el sistema y la numeración que identifique a las personas naturales debe guardar relación con aquellos usados para los mismos propósitos por el SRC, y su confección, mantención y actualización es responsabilidad del SII, el que debe dictar las normas técnicas que sean necesarias y mantener y concentrar en su Dirección Nacional "la información de todos los contribuyentes del país". En base a este RUT, la TGR posteriormente crea para cada contribuyente una Cuenta Única Tributaria.

Su real importancia surge cuando no se le considera en forma aislada, sino que se le relaciona o se solicita su acceso a él pero asociado con otros datos personales o nominativos; acá, lo pedido no es propiamente el dato identificativo sino el asociado.

Es el caso -por ejemplo- (i) del RUT de las empresas asociado a la importación de mercancías que ellas hacen ante la Aduana; (ii) cuando se le vincula con los roles de avalúo de las propiedades raíces, porque se conoce la

[87] Del mismo modo que tratándose de los ciudadanos o administrados, los servicios públicos no necesitan la autorización expresa del artículo 4° de parte de *"los funcionarios que ellos han contratado"* para operar internamente y dentro de su competencia con sus RUT, por ejemplo para calcular sus remuneraciones, conceder licencias o días administrativos, conceder vacaciones, realizar nombramientos o instruirles un sumario. Adicionalmente a este Decreto 18, son también la ley del Estatuto Administrativo, la de Bases Generales de la Administración del Estado, la de Procedimientos Administrativos, la del artículo 4° y la del artículo 20° de la ley 19.628 y sus respectivas Leyes Orgánicas las que los facultan para hacerlo, siempre dentro de su competencia de Derecho Público. Por cierto: si el Consejo de Transparencia ha dictaminado que el RUT *"de los funcionarios públicos*" debe ser secreto y no entregado a terceros porque la ley 20.285 en su artículo 7° sólo permitiría la publicidad de sus nombres y apellidos, esta conclusión, discutible además, no admite ser fácilmente aplicada para casos de RUT *"de los ciudadanos".*

situación patrimonial raíz de un contribuyente; (iii) cuando se asocia a datos sobre mora y protestos, porque se conoce la conducta comercial irregular; (iv) cuando se publican los resultados de exámenes de admisión a la Universidad, porque se conoce la aptitud o idoneidad académica del postulante; (v) cuando se asocia con el número de registro electoral, porque se sabe su calidad de ciudadano legalmente habilitado o no e incluso su filiación política; (vi) cuando se asocia con los beneficios obtenidos en el INP *-hoy IPS-;* o, (vii) cuando se relaciona con el hecho de que una persona sea el beneficiario de un subsidio de vivienda.

3. *Ambos son datos personales o nominativos*.

No cabe duda que al tenor de la definición legal de datos personales contenida en el artículo 2° letra f) de la ley 19.628 -sobre tratamiento o procesamiento electrónico de datos personales y nominativos, aunque denominada "sobre protección de la vida privada"-, los datos RUN y RUT, considerados aisladamente, poseen la naturaleza de datos personales, no sensibles.

La norma establece que son datos de carácter personal o datos personales los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, y ambos, RUN y RUT, permiten que una persona (la ley chilena excluye sin motivo justificado a las personas jurídicas de su tutela) sea posteriormente y en forma exacta y sin errores, identificable al ser referida al parámetro RUN o RUT, sobre todo en un sistema computacional.

¿Cuál sería la naturaleza jurídica del RUT, además de poseer la calidad de *"dato personal"*?. Nada se ha escrito, salvo error u omisión, al respecto, en otro ámbito que no sea el de la protección de datos personales, donde incluso se ha resuelto expresamente que su equivalente en España, el DNI, considerado aisladamente es un dato personal *"porque son números cuya finalidad es identificar a las personas físicas"* y por ende una base de datos que los contenga queda sometida a la institucionalidad de la protección de datos[88].

¿Puede asimilarse el RUT al nombre, y por ende, jurídicamente, sería un derecho personalísimo y un atributo de la personalidad?; creemos que si. No es que legalmente o "*en derecho"* exista una norma que diga que el nombre o los nombres -que definen los padres al inscribirlos- y los apellidos -que se determinan por filiación y también consignan los padres o quienes registran a la persona- son lo mismo que el código identificador que asigna correlativamente el Estado, sino que *"de hecho",* de cara a los sistemas informáticos, lo ha reemplazado.

Y si al nacer una persona natural se le asigna un RUN o si al iniciar actividades una persona natural o jurídica se le asigna un RUT con el único objeto de facilitar la operatoria jurídica de los servicios públicos en general y en materia

[88] Véase la URL http://www.samuelparra.com/wp-content/uploads/2008/09/dni-si-dato-personal.pdf

tributaria en particular -así lo establecen las normas que lo crean-, el dígito identificador que los denomina e individualiza, con poco margen de dudas, sería un atributo de su personalidad[89].

Dicho de otra forma: nombre, RUN y RUT son en el hecho lo mismo; el nombre lo ponen al inscribirse en el Acta de Nacimiento una persona natural o al constituirse una sociedad; el RUN lo asigna el Estado al registrase un nacimiento; el RUT lo asigna el Estado al iniciarse actividades tributarias; cualquiera sea el dato personal identificativo que se use, con todos se atribuye identidad. Por esa atribución e individualización, que identifica a una persona en su atributo *"identidad"*, creemos que ambos son derechos personalísimos en el contexto de las bases de datos.

Otra perspectiva de análisis es la de considerar la distinción entre *"dato personal"* e "*información personal".* A propósito de la protección de datos y la determinación de qué es lo protegido, un autor aclara que aunque se afirma que lo protegido son los datos considerados en forma aislada (nombre o domicilio) en realidad lo que se protege es la información que pudiera surgir de la relación entre datos[90]. Por eso, cita a un informe que consigna que se considera más correcto aludir al término "*datos"* y no a *"información",* donde él segundo sería el resultado final de la elaboración en base a los primeros, a las informaciones iniciales a partir de las cuales se realizan todas las operaciones sucesivas y sobre ellas debieran recaer -por ende, por su proyección futura- los controles y la tutela jurídica que se dispone para el titular individualizado.

¿Cuál sería -relacionado con el párrafo anterior- el alcance cuando la ley chilena alude a datos personales relativos a cualquier información concerniente a personas naturales "identificables" a futuro?.

La definición no es original. Ella está copiada textualmente de la Directiva Europea de 1995, y como queda de manifiesto del estudio de las Actas del trabajo parlamentario, nunca se consideró su alcance específico. Pero como conocemos la fuente, ella sirve para el objetivo del análisis, y para entender que aún cuando el objetivo real de la tutela sea la información personal que resulta de asociar dos o más datos personales, intencional y extensivamente se optó por proteger a los datos originarios que posteriormente serían procesados o tratados computacionalmente y a partir de los cuales una persona sería identificable.

---

[89] Este código identificativo en el hecho suele usarse o asociado a los nombres y apellidos de la persona natural registrada bajo él, o en forma independiente de los nombres; que en materia de sistemas informáticos basta el uso del RUN para asociar y cruzar en torno a él otros antecedentes o datos personales, y que al hacerlo siempre se entenderá y se sabrá que se alude a una persona determinada, identificada e identificable; y que lo mismo vale para el denominado "RUT".

[90] PUCCINELLI, Oscar (1999).

Señala el artículo 2a) de la Directiva 95/46/CE que identificable es toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. En consecuencia, estos "*datos identificativos originarios*", que son siempre de carácter personal y permiten identificar a una persona única, aún aisladamente considerados son objeto de tutela legal, salvo por cierto, que sean ambiguos y no referenciados a nadie como *"nacionalidad chilena", "militancia en x partido", "determinado credo religioso*"; etcétera.

4. *No son datos sensibles o personales de especial naturaleza*, por cuanto en conformidad a la definición de la letra g) del mismo artículo 2°, los indicadores RUN y RUT no se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, *"tales como"* -son sólo ejemplos los que da el legislador- 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.

5. Una conclusión que estimamos esencial. Si bien es cierto ya ha quedado claro que los órganos del Estado tienen amplias facultades legales para procesar o -ampliamente- *"tratar"* los datos personales RUN y RUT, en especial el Registro Civil y el Servicio de Impuestos Internos respectivamente, ello no significa que estén obligados a entregar a terceros en forma masiva y sistemática, mediando pago o no, la correspondencia de los identificadores con los nombres propios de sus titulares.

Porque no existe norma legal -salvo error u omisión- que les asigne esta competencia, sino que ellos están facultados -por ejemplo- para realizar certificaciones, confirmaciones de vigencia, autenticaciones o validaciones, más siempre con fines exclusivos de servicio público.

La duda surge respecto de otros servicios públicos como el SERVEL, que si comercializan listados de RUT asociados a nombres y domicilios, en base a normas legales que no son muy categóricas al momento de asignarle la competencia, y existiendo bastante fundamento para cuestionar la finalidad de servicio público de su actuación[91].

D. Dictámenes de la Contraloría General de la República respecto a los convenios de intercambio de información *"entre servicios públicos y empresas privadas".*

91

1. Recuérdese lo ya dicho, en cuanto a que legal y conceptualmente los acuerdos de intercambio de información de los servicios públicos, en general, sea entre ellos o entre servicios y empresas particulares, se encuentran validados por el artículo 2° de la ley 19.628. En efecto, si conceptualmente el *"tratamiento"* implica la *"comunicación, cesión y transferencia"* de datos personales, cabe interpretar que -por regla general[92]- se encuentran permitidos los convenios de intercambio de datos personales o nominativos y la comunicación que se haga a terceros mediante su publicación en sitios web.

Los elementos jurídicos esenciales para analizar este tipo de convenios son el considerar que deben realizarse para fines de servicio público y no fines de lucro, que los datos personales intercambiados no deben estar sujetos a algún tipo de reserva o secreto establecido por ley (v.gr secreto estadístico, secreto de filiación política, secreto sanitario y secreto tributario) y, que esos datos no deben de ser de aquellos que la ley 19.628 califica como sensibles o personalísimos.

Los órganos estatales que a partir de nuestro número de identificación nacional procesan información personal están manejando o procesando en consecuencia ciertos "*datos públicos",* porque en la medida que un particular consienta o una norma legal establezca que ciertos datos o antecedentes personales sean susceptibles de conocerse[93], éstos pasarán a formar parte de una esfera social o pública porque lo vincularán con la sociedad.

Un presupuesto básico esencial debe siempre tenerse presente y lo reiteramos: ...los servicios públicos recogen, procesan y tratan datos personales o nominativos con apego irrestricto a la ley y actuando sólo dentro de sus competencias exclusivas, que es, por cierto, lo que establece el artículo 20° de la ley 19.628.

Que no se requiera autorización previa, consentimiento, expreso, implícito o del que sea para recoger, tratar o procesar datos personales de los ciudadanos y de los contribuyentes se debe a que *"la ley"* -fundamentalmente la ley 19.628 en sus artículos 2º, 4º y 42, los instructivos presidenciales de Gobierno Electrónico, las Leyes Orgánicas de cada servicio, normas especiales como el Código Tributario, y la Ley de Bases de la Administración del Estado así lo permiten, porque *"reemplazan a la voluntad, al consentimiento o a la autorización de los ciudadanos".*

2. *Convenios de transferencia de información nominativa funcionales, de apoyo y necesarios para la gestión cotidiana del servicio público*.

---

[92] Una excepción, por ejemplo, sería el que el convenio no puede referirse a datos sensibles; otra, que no tenga fines de servicio público sino sólo de lucro.

[93] Pensemos en los siguientes datos: número de teléfono; profesión; filiación política; origen étnico; situación laboral; cotizaciones previsionales; monto de impuestos declarados; créditos bancarios obtenidos; viajes realizados; valores transados en la Bolsa; participaciones en sociedades; etcétera.

Ya anticipamos el tema. Señalamos que la regulación de la comunicación de datos personales del artículo 5° de la ley 19-628 era relevante en el plano local, (i) porque a esta fecha existen procesos telemáticos de cruces de información entre servicios y entre éstos y empresas particulares que se verifican mediante la red Internet y mecanismos de *"webservice";* y porque algunos servicios públicos transfieren datos personales a empresas externas con las cuales contratan cobranzas judiciales o servicios de respaldo de la información de servidores y bases de datos.

Y comentamos que se presentaban convenios de intercambio de datos personales entre los servicios públicos y empresas particulares para materializar las hipótesis de externalización de funciones, esto es, por ejemplo, cuando el servicio y el funcionario público responsable no asumen directamente la gestión de tratamiento, sea, nuevamente, porque se transfieren datos personales a empresas externas con las cuales contratan servicios de cobranzas judiciales, sea porque se contratan servicios de respaldo de la información de servidores y bases de datos. Precisamos además que esta "externalización", tan conveniente desde el punto de vista de los costos de gestión, no eximía de responsabilidades al órgano de la Administración ni al funcionario público responsable del tratamiento que se externalizaba.

Revisamos que si se opta por encargar contractualmente estos servicios mediante un mandato, deberán cumplirse los requisitos del artículo 8° de la ley 19.628[94]; pero no es la práctica más común. Lo más recurrente es celebrar un *contrato de prestación de servicios externalizados o de outsourcing,* y este, debiera ser acompañado de un anexo o convenio específico de cara a los datos personales que serán recíprocamente transferidos durante la vigencia del primero, entre el funcionario público o el servicio responsable que externaliza y el tercero que asume la prestación del servicio externalizado.

Obviamente, para volver a lo establecido en el artículo 20 de la ley 19.628, esta externalización del tratamiento de datos personales sólo resultará procedente y válida si alude a materias de la competencia del servicio público y de cara al cumplimiento de los fines promocionales y asistenciales que le competan, con una particularidad que se ha puesto de relieve: ...de conformidad a una ley 18.803, lo que el servicio público -de cara a optimizar su gestión- puede externalizar son las llamadas acciones de apoyo auxiliares o complementarias de sus funciones y no el ejercicio mismo o directo de sus potestades públicas o competencias. Dicho de otra forma, si se externalizan los tratamientos o procesamientos computacionales,

[94] A saber: *"En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales. El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos. El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo".*

no será externalizable por ejemplo la decisión de tratar-transferir o no determinados datos personales a otro servicio público, o la decisión de eliminarlos por caducos.

3. No uno sino al menos tres han sido los pronunciamientos de la Contraloría General de la República sobre esta materia, los años 2001, 2002 y 2003 respectivamente. Y no han sido emitidos, como es sabido y se señala frecuentemente, en abstracto o para resolver dudas sobre aspectos instrumentales o de gestión, sino que han sido dictados respecto de servicios públicos determinados y ante cuestionamientos de fondo e imputaciones -erradas e infundadas- de supuestas actuaciones ilegales.

Los servicios públicos pueden celebrar convenios de intercambio de información conforme al ***Dictamen 10.322 de Marzo del 2001.*** El Dictamen expresamente permite al Servicio de Impuestos Internos celebrar convenios con empresas particulares, y en consecuencia, con mayor razón respecto de servicios públicos para cumplir con sus fines de tales.

Los convenios serán procedentes, según el Dictamen, cuando no se trate de datos secretos, no se vulnere la ley 19628, no se vulnere la garantía constitucional de la privacidad, se trate de información *"generada"* por el servicio público en el marco de su competencia y se adopten los resguardos para que la información no sea utilizada para objetos no queridos por el Servicio.

Por cierto, dicho pronunciamiento será citado posterior y expresamente en un segundo ***Dictamen 43.866***, para aludir a la facultad de la Tesorería General de la República también para celebrar convenios de intercambio de información.

La Contraloría el año 2001 en el Dictamen 10.322 expresamente alude a la facultad del Servicio de Impuestos Internos para celebrar convenios de intercambio de información, esto es, que posee facultades amplias que le otorga su Ley Orgánica, para celebrar contratos relacionados con el cumplimiento de los fines del mismo, y que en este contexto y a propósito de información que es *per se* pública y no secreta o reservada, se encuentra habilitado para suscribir con empresas especializadas en el manejo de bases de datos acuerdos de voluntades de intercambio de información.

El SII posee la facultad de celebrar convenios de intercambio de información con empresas particulares, pero además a él le compete evaluar y ponderar tanto la conveniencia como la procedencia legal de hacerlo y el contenido de la información que será intercambiada es una decisión discrecional del servicio público. Así lo señala expresamente el Dictamen 10.322 del año 2001: *"...la sola circunstancia de que un servicio público efectúe tratamiento de datos personales no implica que se encuentre facultado para ceder esos datos a terceros. Esta última posibilidad debe ser analizada a la luz de la naturaleza de la*

información que se pretende ceder y de las competencias que desarrolla el órgano pertinente".

El Dictamen de la Contraloría del año 2001 no alude a qué tipo de datos o de información específica debe incluirse en sus convenios de intercambio de información, ya que determinar este ámbito es una facultad privativa del servicio que celebra el convenio sujeta a las restricciones legales vigentes a esa fecha, esto es, para el caso del Servicio de Impuestos Internos, fundamentalmente a las normas del secreto tributario y a las disposiciones de la ley 19.628.

En los convenios vigentes a esta fecha no existe infracción a lo establecido por el Código Tributario ni por la ley 19.628 sobre protección de datos personales, porque se alude a datos que provienen de fuentes de información pública que nos sitúan en el ámbito de la esfera social de las personas y de aquella que para ser tratada computacionalmente no requiere de autorización expresa y previa de sus titulares o de aquellos a quienes alude.

Por si hubiera alguna duda acerca de la finalidad de servicio público, téngase presente que a través de esta opción el SII además proporciona indirectamente información a los contribuyentes respecto de su situación tributaria, de manera que puedan conocer el estado en que se encuentran y los problemas eventuales –como una posible suplantación de identidad comercial o que una empresa haya sido víctima de irregularidades tributarias-, o los problemas pendientes de solución, y posibilita –precisamente- alertar para el futuro a aquéllos que efectúan operaciones con contribuyentes con comportamiento tributario irregular. No hay fines de lucro, no hay vulneración de esfera privada alguna, no hay comunicación de información secreta o reservada, y la información que se obtiene de las empresas permite -a consecuencia del canje o intercambio-, por ejemplo, verificar los domicilios donde se realizarán notificaciones.

En este mismo orden de ideas y en el plano de la interpretación de las normas legales, la Ley Orgánica del SII (en el artículo 7º letra ñ) establece expresamente que al Director le compete ejecutar los actos que estime necesarios para el cumplimiento de los fines del Servicio, y la difusión de por ejemplo la *"situación tributaria"* de los contribuyentes precisamente es uno de esos actos, porque al tratarse de un comportamiento público y al darse a conocer se consigue que exista estabilidad para el Orden Público Económico.

Sólo un análisis muy parcial, por ende, podría llevar a considerar que estos nuevos servicios prestados al contarse con las facilidades provenientes de las nuevas tecnologías –léase consulta en bases y bancos de datos- no están vinculados a la naturaleza o finalidad tradicional del SII, quien no se está atribuyendo facultades, competencias o atribuciones no conferidos previa y legalmente.

La Contraloría también tuvo presente que, *a diferencia de la Tesorería, el SII no encarga la publicación de datos, menos sobre mora y protestos en DICOM u otras empresas similares, referidos a antecedentes patrimoniales, económicos, financieros y comerciales que se originen en el previo incumplimiento de una obligación legal-patrimonial.* Efectivamente, el SII no ha optado por contratar los servicios de empresas comerciales distribuidoras de información, ni les ha solicitado o encargado que publiquen tales o cuales datos.

La razón de ser de los convenios de intercambio o canje de información es la de posibilitar que el ente fiscalizador acceda a la mayor cantidad de antecedentes posibles únicamente para cumplir sus fines de recaudación y fiscalización, y los antecedentes públicos que entrega como contrapartida a las empresas que suscriben los referidos convenios no son condicionados a determinados fines ni es del conocimiento del SII la forma en que ellos son distribuidos a terceros. Si una vez recibidos los datos públicos por las empresas distribuidoras se produce algún abuso o mal uso en base a los datos que ellos reciben, es algo que no puede ser imputado a la responsabilidad del ente público.

Volviendo al articulado de la ley 19.628, y teniendo nuevamente a la vista la llamada "*Teoría de las Esferas",* se debe entender que la información que un servicio público genera por el hecho de cumplir con los fines que por ley debe asumir, forma parte de la esfera pública de una sociedad, no es privada, no es íntima y no puede ser privada del conocimiento de la sociedad toda por la mera voluntad de su titular, porque existen normas legales expresas y de Derecho Público que así lo establecen. Desde esta perspectiva, los datos que procesa el SII respecto de las personas naturales son de aquellos económicos y financieros que provienen de fuentes de naturaleza pública para el órgano de la Administración[95], y que, en conformidad a los artículos 2°, 4° y 20° de la ley 19.628, (i) pueden procesarse sin autorización de sus titulares por mandato legal y (ii) pueden comunicarse porque la ley le ha conferido esa facultad.

Ubicado en el Título I sobre la utilización de datos personales, el artículo 4° sienta un principio general en materia de procesamiento de datos personales. Señala que el tratamiento de los datos personales sólo podrá efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o cuando el titular consienta expresamente en ello, pero consagra diversas excepciones en los incisos quinto y sexto, en relación a la autorización del titular requerida para el tratamiento de los datos cuando estos provienen de fuentes públicas.

El artículo 4° pues, complementa. Primero señala que no requiere autorización el tratamiento de datos personales cuando una ley o varias leyes -como las que definen la competencia tributaria del ente fiscalizador- lo permitan. En segundo lugar, en el inciso quinto, señala que se pueden procesar sin

[95] De lo cual no se sigue que lo sean para los administrados de manera que deban serle entregados en forma masiva y sistematizada los datos.

autorización los datos personales que provengan o que se recolecten de fuentes accesibles al público y sean de carácter económico, financiero, bancario o comercial, donde los datos *"tributarios"* son obviamente "*económicos"* y *"financieros".*

Por último, téngase presente que con el mérito de todo lo dicho, ha sido el propio SII, en el marco de las potestades normativas que le confiere su Ley Orgánica, quien reguló y preciso esta materia. Puede consultarse en Internet el contexto de la Resolución Exenta 3509 de Julio del año 2000 y la modificación que se le hizo en Diciembre del mismo año mediante la Resolución Exenta 5395 (que instruye o resuelve en materia de canjes de "información computarizada" con empresas especializadas en materia de servicios de información y con órganos estatales), donde se indican una serie de contenidos de información que no podrá nunca incorporarse a los Convenios.

La redacción de la cláusula cuarta de la Resolución Exenta, sobre especificación de contenidos de información o la "naturaleza" de los datos que podrán ser incorporados en los convenios es clara, precisa y detallada, y su interpretación, a efectos de determinar la procedencia o no de un convenio o del tipo de información a entregarse a particulares en el contexto de un acuerdo, debe ser necesariamente restrictiva.

4. *El año 2002 la CGR dictaminó (N°25.336)* que la Tesorería podía celebrar convenios de intercambio de información sobre datos de mora y protestos de los contribuyentes.

El criterio anterior atiende a considerar que la Tesorería posee facultades amplias que le otorga su Ley Orgánica, para celebrar contratos relacionados con el cumplimiento de los fines del mismo, en este contexto y a propósito de información que para el órgano de la Administración es *per se* pública y no privada, íntima, secreta o reservada.

Debe considerarse un supuesto clave: que se trata de antecedentes sobre deudas tributarias o créditos morosos del sector público en proceso de cobranza, y por ende es información nominativa generada o procesada por el Estado en el marco de su actividad pública de cobranza. Esta *"actividad pública de cobranza"* que debe realizar la Tesorería, que apunta a que se cumplan con obligaciones legales y a que se mantenga el orden público económico en materia tributaria, incluye la posibilidad de confeccionar listas o nóminas de deudores, empleándose todos los medios posibles para dar publicidad a las subastas que resulten de los procedimientos de cobro que tramite la TGR.

En efecto, mediante el ***Dictamen 25.336*** se determinó claramente que la Tesorería tenía facultades para suscribir convenios de intercambio de información referente a obligaciones de contribuyentes y deudores morosos del Fisco, con

empresas especializadas que existiesen en el país y que mantuviesen bases de datos.

5. Si el año 2002 la CGR dictaminó que la Tesorería podía celebrar convenios de intercambio de información sobre datos de mora y protestos de los contribuyentes, posteriormente, ***el año 2003 y en un Dictamen 43.866,*** complementó y precisó que ella puede celebrar dichos convenios -sobre datos tributarios y sobre obligaciones morosas o patrimoniales negativos- aún cuando el artículo 17 de la ley 19.628 no los mencione expresamente[96].

El criterio anterior reitera que se debe considerar que la Tesorería posee facultades amplias que le otorga su Ley Orgánica para celebrar contratos relacionados con el cumplimiento de los fines del mismo, en este contexto y a propósito de información que es *per se* pública y no secreta o reservada.

Sería un despropósito que ante la comunicación mediante convenios previamente firmados conforme a derecho de antecedentes verdaderos, públicos, fidedignos y que dan cuenta del incumplimiento por parte del recurrente de obligaciones legales-tributarias, se permitiera, al acogerse un recurso de protección, que una persona pudiese ocultar su calidad de infractor.

En efecto, *la información personal sobre la situación tributaria de un contribuyente…* (tanto en cuanto no sea de aquella amparada por el secreto tributario consagrado en el Código Tributario, los que son antecedentes que son parte de una esfera íntima o reservada que no puede ser atisbada, procesada o conocida por particulares, por empresas que quieran comercializarlos e incluso por otros órganos estatales), *...cabe dentro de lo que la doctrina constitucionalista y los sociólogos denominan la "esfera social" de las personas.*

Desde otra perspectiva, también resulta improcedente constitucional, legal y procesalmente proyectar la garantía constitucional que se asegura a todas las personas en el artículo 19 N°4, que consiste en el respeto y protección de *"la honra... de las personas y sus familias",* al ámbito de los datos procesados y publicados por la Tesorería, cuando éstos por su naturaleza son antecedentes públicos, exactos, verdaderos y fidedignos, que se generan únicamente por la infracción legal del contribuyente que no cumple con sus obligaciones tributarias. No puede considerarse, con fundamento serio, que con esta publicación lo que se busca es menoscabar la honra de los ciudadanos morosos.

El cuestionamiento nació de un Oficio enviado a la Contraloría por el Senador *Baldo Prokurika* que, en lo esencial, sostuvo que la Tesorería no podía publicar antecedentes sobre morosidad tributaria porque, atendido el tenor del artículo 17 de la Ley 19.628 sobre protección de datos personales, no podría publicitarse mediante su almacenamiento en bases de datos ya que la norma

[96] Véase lo analizado en el número 17 del acápite B de este Informe.

enumeraría taxativamente las obligaciones que pueden ser procesadas, almacenadas y comunicadas computacionalmente, no habiéndose incluido las relativas a morosidad tributaria. Señaló además que la Ley Orgánica de la Tesorería no la facultaba para divulgar las deudas por concepto de impuestos y créditos del sector público que se encuentren en mora, y que el contrato celebrado al efecto con la empresa DICOM podría implicar vulnerar la garantía del artículo 19 N°4, sobre protección de la honra de las personas.

Cabe destacarse que, en primer lugar, la Contraloría señala y reitera lo consignado y concluido no sólo en el Dictamen 25.336 del año 2002, sino también el año 2001 en el Dictamen 10.322, esto es, que el Servicio de Tesorerías posee facultades amplias que le otorga su Ley Orgánica, para celebrar contratos relacionados con el cumplimiento de los fines del mismo, y que en este contexto y a propósito de información que es *per se* pública y no secreta o reservada, se encuentra habilitado para suscribir con empresas especializadas en el manejo de bases de datos acuerdos de voluntades de intercambio de información, concretamente relacionada con contribuyentes y deudores que se encuentren en mora con el Fisco.

Tal conclusión considera un supuesto clave, que se reitera: ...aquel de que la información objeto de los convenios es pública para los órganos de la Administración, porque se trata de antecedentes sobre deudas tributarias o créditos morosos del sector público en proceso de cobranza, y por ende es generada o procesada por el Estado en el marco de su actividad pública de cobranza, actividad de servicio público que apunta a que se cumplan con obligaciones legales y a que se mantenga el orden público económico en materia tributaria. Y esto incluye la posibilidad de confeccionar listas o nóminas de deudores, según expresamente lo establece el artículo 169 del Código Tributario.

Al amparo de las normas de la ley 19.628, sobre protección de datos personales, la Contraloría consideró que la Tesorería es un órgano público (artículo 1°), que "trata" datos públicos (artículo 2°) y que actúa dentro de su esfera de competencia (artículo 20°), por lo cual, de manera alguna requiere contar con el consentimiento de los titulares de los datos.

Se acoge y ratifica la tesis que estima que se trata de información pública, porque sólo se están publicitando datos sobre procedimientos ejecutivos de cobro de deudas en casos en que el deudor ya ha sido notificado y requerido de pago, y que por ende puede ser *"intercambiada"* vía convenios o directamente "*publicada"* en el sitio web de la entidad.

E. Situación jurídica de los convenios de intercambio de datos personales *"entre los propios servicios públicos".*

1. La necesidad de contar con información acerca de los ciudadanos y/o administrados puede no verse satisfecha con los antecedentes personales o nominativos disponibles en los sistemas de un sólo servicio público, situación que puede obstar al logro de los fines promocionales y asistenciales que les son propios.

La realidad práctica demuestra que es así, por ejemplo cuando el INP o Instituto de Normalización Previsional (hoy IPS) para asignar beneficios previsionales requiere conocer y certificar las edades o fechas de nacimiento y de defunción de los beneficiarios y de sus cargas, y ello se obtiene accesando directamente on line los sistemas del Servicio de Registro Civil.

Otro ejemplo: cuando el Mineduc debe asignar beneficios de pase escolar o de becas de estudio, la ley expresamente lo faculta para requerir del Servicio de Impuestos Internos -el que es obligado a entregarlos- antecedentes personales patrimoniales del grupo familiar del postulante o solicitante de los beneficios.

Otro ejemplo, referido en la letra B a propósito de la ley 19.628 y sus disposiciones, es la ley 19.397, que junto con permitirle al Ministerio de Salud tratar y mantener registros respecto de las materias de su competencia y facultarlo expresamente para tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud, también lo faculta para solicitar o requerirle datos personales que se estimen necesarios a otros servicios públicos o personas jurídicas públicas.

Uno más, también ya anticipado a pie de página: el artículo 2° letra i) de la ley 19.913 del año 2003, que al crear la UAF o Unidad de Análisis Financiero la 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[97].

Una perspectiva diferente. Los artículos 20º y 21º de la ley 17.374, Orgánica de la Dirección de Estadísticas y Censos establecen la obligación de entregarse la información, datos o antecedentes que el Instituto Nacional de

[97] Si además hacemos el ejercicio de aplicarle las categorías ya vistas de la ley 19.628, se trata de un caso en que una ley expresa autoriza el tratamiento/comunicación (artículo 4°), en que la transferencia deberá cumplir ciertos requisitos legales (artículo 5°), y en que no puede discutirse que el tratamiento/recepción de los datos personales es de competencia exclusiva de la UAF (artículo 20).

Estadísticas solicite acerca de hechos que por su naturaleza y finalidad tengan relación con la formación de estadísticas oficiales. Sumado a ello o como norma complementaria general, todo servicio público, en conformidad al artículo 5° de la LBAE, deberá colaborar con el INE siempre que no interfiera con sus funciones ni irrogue gastos imposibles de ser absorbidos o no presupuestados, y si se trata de datos personales -esta es *"la perspectiva diferente",* debiera hacerse con el resguardo de que nunca se entregue información de manera nominada o individualizada.

Similar es la situación del artículo 53 de la ley 18.840, Orgánica del Banco Central, que señala que el Banco deberá compilar y publicar, oportunamente, las principales estadísticas macroeconómicas nacionales, incluyendo aquellas de carácter monetario y cambiario, de balanza de pagos y las cuentas nacionales u otros sistemas globales de contabilidad económica y social. Agrega que para los efectos previstos en la norma el Consejo deberá establecer, mediante acuerdo publicado en el Diario Oficial, la naturaleza, contenido y periodicidad de la información que dará a conocer, y que para el cumplimiento de estas funciones el Banco está facultado para exigir a los diversos servicios o reparticiones de la Administración Pública, instituciones descentralizadas y, en general, al sector público, la información que estime necesaria.

Además de los ejemplos mencionados, a esta fecha existen en Chile -salvo error u omisión- otra serie de convenios de colaboración y de intercambio de datos personales entre servicios públicos en vigor. Tal sería el caso: del ex INP con la Dirección de Previsión de Carabineros; del MINVU con el Registro Civil; del SII con la Dirección General de Aeronáutica; del SII con el Registro Civil; de la TGR con las Cajas de Compensación; de la TGR con la Dirección del Trabajo; etcétera.

A nuestro parecer y para observar o cumplir con el deber de diligencia que la LGBAE impone a todos los funcionarios públicos, todos los intercambios de datos personales debieran estar respaldados por un convenio o acuerdo expreso de intercambio, donde al menos se deberán explicitar restricciones y medidas de seguridad específicas y la forma en que se da cumplimiento al artículo 5° de la ley 19.628.

2. *Plena legalidad de los convenios entre servicios públicos.*

2.1 El *fundamento legal general* de estos convenios de intercambio de información entre servicios públicos se encuentra en los artículos 3° y 5° de la Ley General de Bases de la Administración del Estado. Existen además, como hemos mencionado, otras normas legales especiales o específicas que al establecer la obligación de entrega de información de un servicio público al otro abren el espacio a la necesidad de formalizar un acuerdo o convenio de intercambio.

El artículo 3° dispone que la Administración del Estado está al servicio de la persona humana; y agrega que su finalidad es promover el bien común atendiendo

las necesidades públicas en forma continua y permanente y fomentando el desarrollo del país a través del ejercicio de las atribuciones que le confiere la Constitución y la ley, y de la aprobación, ejecución y control de políticas, planes, programas y acciones de alcance nacional, regional y comunal.

Dispone además que la Administración deberá observar los principios *de responsabilidad, de eficiencia, de eficacia, de coordinación, de impulsión de oficio del procedimiento, de impugnabilidad de los actos administrativos, de control, de probidad, de transparencia y de publicidad administrativas.*

Si nos situamos en el contexto de los convenios de intercambio de datos personales, conviene detenerse en los principios de eficiencia, eficacia y coordinación. *"Mientras la eficacia mira a la capacidad de lograr el efecto que se desea o se espera"* -se ha dicho-, *"la eficiencia atiende a la capacidad para disponer de alguien o de algo para conseguir un efecto determinado".* Como se mire, ambos conceptos apuntan a fortalecer las capacidades de la Administración del Estado para el cumplimiento de sus fines.

Por su parte la expresión *"coordinación"* busca que el accionar de la Administración del Estado implique una disposición metódica de las cosas, esto es, el concertar medios y esfuerzos para una acción común.

Esta interpretación de las disposiciones de la ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado (que no nos pertenece pero que hacemos nuestra), aparece corroborada por su artículo 5°, que literalmente dispone:

> "*Las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública. Los órganos de la Administración del Estado deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones".*

2.2 Nuevamente, legal y conceptualmente, los acuerdos de intercambio de información de los servicios públicos entre ellos, también se encuentran validados por la ley 19.628.

El artículo 2° letra c) define a la comunicación o transmisión de datos como el dar a conocer de cualquier forma los datos personales a personas distintas del titular, sean determinadas o indeterminadas. En efecto, si conceptualmente el *"tratamiento"* implica la *"comunicación, cesión y transferencia"* de datos personales, cabe interpretar que se encuentran permitidos los convenios de intercambio de datos personales y la comunicación que se haga a terceros mediante su publicación en sitios web.

Se trataría de casos en que una ley expresa autorizaría el tratamiento/comunicación sin autorización de sus titulares (artículo 4°), en que la transferencia deberá cumplir ciertos requisitos legales (artículo 5°), y en que habrá de determinarse si el *tratamiento-comunicación-recepción* de los datos personales es de competencia exclusiva de los servicios públicos que los intercambian (artículo 20°). De no tratarse de datos intercambiados y/o tratados que sean de competencia de los servicios públicos -*v.gr. recopilarse y difundirse las direcciones de email de los ciudadanos no es carga pública de ningún servicio*-, la única válvula de salida sería solicitar autorización previa a los ciudadanos titulares de los datos.

Siempre *en sede de la ley 19.628*, los convenios debieran explicitar cómo se cumple con lo establecido en el artículo 5° ya analizado en el acápite B, esto es, que el responsable del registro o banco de datos personales cautela los derechos de los titulares y que la transmisión guarda relación con las tareas y finalidades de los organismos participantes; que el receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión; y que se deja constancia (i) de la individualización del requirente, (ii) del motivo y el propósito del requerimiento y (iii) del tipo de datos que se transmiten.

2.3 *Los elementos jurídicos esenciales para analizar este tipo de convenios* serían, en consecuencia, el considerar:

(i) Que sólo deben realizarse para fines de servicio público y por la vía de canjes de información, evaluándose caso a caso su celebración porque celebrarlo o no es una facultad privativa de la Jefatura Superior de cada servicio y entendiéndose que los convenios son excepcionales, *salvo que exista una obligación legal expresa de celebrarlos o de realizar los intercambios de información*[98];

(ii) Que los datos personales intercambiados no deben estar sujetos a algún tipo de reserva o secreto establecido por ley (v.gr secreto estadístico, secreto de filiación política, secreto tributario o secreto sanitario);

(iii) Que los datos personales intercambiados sean objetivos y generados por el servicio público en el marco de su competencia y actividad de servicio público, y no obtenidos desde otro servicio público o primer generador de la data;

[98] Además de lo mencionado para la UAF, el INE o el Banco Central, es el caso de la TGR y el SII, que han celebrado un convenio de intercambio para dar cumplimiento a la obligación de colaboración en la entrega de información que establece perentoriamente el artículo 82 del Código Tributario; ella señala que *"la Tesorería y el Servicio de Impuestos Internos deberán proporcionarse mutuamente la información que requieran para el oportuno cumplimiento de sus funciones".*

(iv) Que esos datos no deben de ser de aquellos que la ley 19.628 califica como sensibles o especialmente importantes para los ciudadanos personas naturales;

(v) Que se están adoptando todos los resguardos necesarios para evitar que la información objeto del convenio sea usada para objetos o fines no considerados y no permitidos por la ley, y por ende fines solicitados y declarados expresamente en los fundamentos, considerandos o motivos del texto del acuerdo;

(vi) Que se establezca con claridad que toda la data personal accesada por los funcionarios correspondientes en el marco de un convenio bilateral será para uso exclusivo de la Institución, sin que ella pueda ser entregada a terceros; y,

(vii) Que *salvo que exista una ley expresa que obligue a un servicio público a entregar datos personales al otro*[99], la ley marco que fundamenta el convenio y el intercambio es la Ley de Bases Generales de la Administración del Estado en sus artículos 3° y 5°.

3. *Legalidad de los convenios bilaterales de intercambio de información entre los servicios públicos que participan en la Plataforma Integrada de Servicios Electrónicos del Estado (PISEE). Referencia.*

Legalmente la verificación de los convenios bilaterales de intercambio de información entre los servicios públicos no merece ni merecía reparo alguno[100].

Como veremos a propósito del por nosotros reparado Proyecto PISEE o la *Plataforma Integrada de Servicios Electrónicos del Estado*, no se necesitaban nuevos análisis jurídicos ni se discutía la validez de una práctica como la celebración de convenios de intercambio de datos que incluso desde hace años había sido validada por la Contraloría General de la República[101], para concluir:

---

[99] Es el caso, se reitera, del artículo 82 del Código Tributario, que señala que la Tesorería y el Servicio de Impuestos Internos deberán proporcionarse mutuamente la información que requieran para el oportuno cumplimiento de sus funciones. El artículo 82 anticipa el mismo principio de colaboración en base a antecedentes cuyo contenido sea tributariamente relevante, que luego consagran los artículos 168 y 195. Y lo hace en el contexto de la fiscalización realizada mediante el análisis documental de los antecedentes que deben remitir al SII el SRC, las Aduanas, los Conservadores, los notarios, otros ministros de fe, los arrendadores los tesoreros fiscales, los jueces de letras, los alcaldes, los bancos y los tesoreros municipales. Se consigna un ejemplo en el inciso segundo, cuando señala que *"los formularios del impuesto territorial pagado"* deberán remitirse por los bancos a la Tesorería para su procesamiento.

[100] Antes de la plataforma y al margen de ella, el SII poseía un convenio con el INP y el Registro Civil; el INP de la época tenía convenio firmado con el Registro Civil; etcétera.

[101] Lo que debe observarse jurídicamente desde ya a este proyecto no son los intercambios de datos con fines de servicio público entre los órganos de la Administración que subyacen en la plataforma, sino que son las gestiones sin respaldo normativo de Derecho Público de la plataforma misma y de los funcionarios quienes la administran y la hacen interoperable. Dicho de

(i) …que normas constitucionales y legales, generales (de la LGBAE, como los artículos 3° y 5°) y particulares como sus propias Leyes Orgánicas, habilitaban a los servicios públicos para colaborar y transferir entre ellos datos personales previamente tratados en el marco de sus competencias exclusivas, actuando dentro de sus competencias, con fines de servicio público y respetando las posibles *"restricciones"* -por ejemplo- en casos de datos sujetos a secreto o reserva;

(ii) …que diversos artículos de la ley 19.628, ya analizada en extenso, validaban expresamente la recopilación, el almacenamiento, el procesamiento y la transferencia o el intercambio de datos personales vía redes, y exigían hacerlo operándose dentro de su competencia exclusiva (artículo 20) y con el resguardo de los derechos de los ciudadanos (artículo 1°); y,

(iii) …que no se necesitaba modificación legal alguna para validar dichos intercambios ni los convenios que los formalizaban, máxime porque el proyecto no descansa conceptualmente sobre la elaboración de una base de datos única o centralizada sino que concibe a la plataforma como una mera pasarela de datos.

Los antecedentes relevados por la consultoría encargada por el Grupo de la Estrategia Digital de la Subsecretaría de Economía, carentes de novedad y enmarcados erradamente bajo el rótulo de *"puesta en marcha de la ley de procedimiento administrativo"* -con la cual no guardan relación jurídica alguna-, no hicieron por ende sino mostrar en forma sistemática los argumentos jurídicos que los propios servicios públicos habían validado y levantado mucho antes, al momento de optar por celebrar entre ellos convenios bilaterales de intercambio de información.

En cuanto a la referencia a la ley 19.880 que señalamos como no relacionada jurídicamente con el proyecto y por ende con la consultoría, conforme a sus disposiciones no existen dudas sobre la posibilidad de operarse en forma electrónica porque en los artículos 18 y 19 se alude expresamente a la posibilidad de realizar dichos procedimientos y mantener los expedientes con los actos administrativos. *Lo que carecía y carece de fundamento era invocar esta ley como fundamento del mero intercambio de datos que caracteriza a la plataforma, toda vez que en la PISEE no se realizan actos administrativos*[102]*, por su intermedio no*

---

otra forma: lo observable jurídicamente es que está operando una plataforma electrónica como la de www.chilecompras.cl, pero sin una ley 19.886 que lo permita legalmente.

[102] Legalmente, los actos son las decisiones escritas que adopta la Administración, decisiones que son formales y que contienen declaraciones de voluntad realizadas en el ejercicio de una potestad pública.

se verifican procedimientos administrativos [103], y en ella no se almacenan expedientes electrónicos con lo actuado procedimentalmente.

En concreto, esta consultoría constató que existían en las normas referidas *principios*, *restricciones* y *condiciones* para la transferencia de datos personales a los cuales debían someterse los servicios públicos que operaran en la Plataforma. (i) Mencionó principios como los de competencia exclusiva, de coordinación, de unidad de acción, de no duplicación, y de actualización de los datos; (ii) se refirió a restricciones evidentes como el actuar dentro de la competencia exclusiva, el usar los datos para los fines tenidos en vista al recopilarse; y respetar normas legales de secreto; y, (iii) consignó condiciones de transferencia también evidentes como que el servicio público requirente tuviera competencia para pedir los datos, que el requirente pidiera datos relativos a trámites de su competencia, que el servicio requerido sólo podía transferir datos recolectados en el ejercicio de sus potestades, y que el servicio solicitante sólo podía usar los datos en la forma que su competencia de Derecho público lo permitiera.

F. Proyección de las normas sobre protección de datos personales de la ley 19.628 al ámbito de la red Internet. El Decreto Supremo N°100 y la regulación de las Políticas de Privacidad de los sitios web de los servicios públicos.

1. La hipótesis de trabajo es la siguiente: *¿procedía implementar y regular especial y expresamente "Políticas de Privacidad" en los servicios públicos o en los órganos del Estado que operen e interactúen con los ciudadanos mediante sitios web?.*

Nos cupo participar en los debates de un Comité Interdisciplinario integrado por profesionales de diversas reparticiones públicas, (i) para definir y estandarizar -obligatoriamente- un Código Deontológico o de prácticas *"del deber ser"* y (ii) para establecer las llamadas *"Políticas de Privacidad"* que deberían contener todos los sitios web del Estado que recopilaran *on line* y procesaran datos personales o nominativos -de aquellos definidos en el artículo 2° de la ley 19.628- mediante los referidos sitios.

Lamentablemente, el desconocimiento de la realidad concreta del procesamiento de datos personales en el Sector Público y un marcado prejuicio acerca de la existencia de supuestas irregularidades y de la conculcación de los derechos de los ciudadanos que accesan los sitios web de los servicios,

[103] Legalmente, los procedimientos son una sucesión de actos trámite vinculados entre sí, emanados de la Administración o de particulares interesados, que tiene por finalidad producir un acto administrativo terminal.

perturbaron el trabajo al punto de olvidarse que el Poder Ejecutivo y los órganos públicos no poseen facultades de Derecho Público para, inicialmente en forma contractual (antes de pensarse en la dictación del Decreto Supremo N°100), acordar con los ciudadanos medidas que mermen sus competencias públicas atribuidas por ley.

Nos sigue pareciendo errada esta opción. Además de lo afirmado en cuanto a que los órganos públicos no *"se auto regulan"* mediante Códigos Deontológicos ni deben declarar cumplir con una o varias normas determinadas para validar su comportamiento en materia de procesamiento de datos personales, ellos deben necesariamente actuar ajustados o conforme a Derecho.

Aún cuando el servicio público no hubiera sido obligado a publicar y mantener en su sitio web políticas de privacidad, ello no hacía inaplicable toda la normativa jurídica que regula el STDP de los órganos de la Administración del Estado -no sólo es la ley 19.628 pero si es esta en especial-, al tratamiento que se hiciera de los datos de los ciudadanos recopilados desde los *log* o registros de los servidores usados para comunicarse mediante la red Internet.

Más aún, el señalamiento o la referencia informativa que en los sitios web se hace a la ley 19.628 de manera general -por ser el contexto legal del tratamiento-, en nuestra opinión era -antes del Decreto Supremo N°100- un señalamiento suficiente, por cuanto los servicios públicos no deben auto regular normas de Derecho Público que les serán siempre aplicables, y menos deben abocarse a elaborar cartillas informativas sobre los contenidos de la ley como una práctica obligatoria[104].

2. En definitiva, en el marco de una norma técnica y reglamentaria para el desarrollo y la operatoria de los sitios web del Estado, esto es, el Decreto Supremo Nº100 publicado el 12 de Agosto del año 2006, se incluyó un artículo 9º que establece que *todos los órganos de la administración del Estado deberán adoptar, mantener y declarar una política de privacidad en su respectivo sitio web.* Ella deberá encontrarse accesible en el sitio y contener una serie de menciones mínimas que se establecen.

No obstante la vigencia de esta norma, el problema que se presenta en relación a ella es que nadie, ningún servicio público, fiscaliza sistemáticamente su cumplimiento[105].

---

[104] En los sitios web de algunos servicios públicos pueden encontrarse referencias que señalan que en sus condiciones de uso no se establecen políticas de privacidad porque ellas se encontraban definidas expresamente por las normas legales y reglamentarias de derecho Público vigentes en Chile, en particular por la ley 19.628; por cierto, en conformidad al Decreto Supremo N°100 esto debiera ya haberse modificado.

[105] Un cuestionario acerca de su aplicación práctica, puede verse en la URL http://www.estrategiadigital.gob.cl/files/Guia_Metodologica_PMG_Gobierno_Electronico_2009.pdf

Una consideración "*meta jurídica*" cabe plantearse: ...con esta norma se establece *"un piso mínimo"* que afecta por igual a todos los servicios públicos del Estado, siendo que ellos desarrollan actividades en Internet de muy diverso volumen o envergadura, con los correspondientes costos de gestión que ello involucra. Dicho de otra forma: en Chile no son más de 10 los entes públicos que se pueden ver drásticamente afectados en su gestión electrónica si, so pretexto de definirse políticas estándares de privacidad, se establecieran a futuro -como ya se propuso- condiciones mucho más gravosas que las definidas por el Decreto en comento[106].

En cuanto a la estructura de los tres Títulos del Decreto, el *Título I* se refiere a su ámbito de aplicación, el *Título II* a las *"tareas para el cumplimiento del nivel 1"* y el *Título III* a las *"tareas para el cumplimiento del nivel 2",* porque se establecieron plazos para dos etapas dentro de las cuales cumplir con las medidas obligatorias y sugeridas.

El objetivo o la obligación general declarada en el artículo 1° inciso segundo, es el de desarrollar los sitios web de manera que se garantice en ellos la disponibilidad y la accesibilidad de la información, *se asegure el debido resguardo de los derechos de los titulares de datos personales,* y se asegure la interoperabilidad de los contenidos, funciones y prestaciones ofrecidas por el servicio público, cualquiera que sean ("*con prescindencia"* dice el Decreto) las plataformas, los programas y los equipos utilizados.

El Nivel 1 o la Primera Etapa, se refirió a la necesidad de desarrollar tareas destinadas a permitir que las personas usuarias de los sitios web accedieran de manera rápida, efectiva y eficiente a los servicios, funciones y prestaciones; la segunda etapa, o el nivel 2, decía relación con desarrollar tareas que permitieran implementar en los sitios web las principales directrices de de las normas internacionales sobre accesibilidad.

Los cinco numerales del *artículo 9º* -incluido en el Título II- aluden a la obligatoriedad de que se contengan las siguientes menciones y/o declaraciones:

> (i) Sobre la individualización del servicio público tratante al que corresponde el sitio web, con precisión de quien lo representa, su domicilio, dirección postal y correo electrónico;

[106] A este respecto, por ejemplo, el informe del Comité mencionado proponía fijar como política de privacidad que *"el órgano del Estado no comunicará ni transferirá datos personales de sus usuarios sin el consentimiento previo y expreso del titular"*. Si esto se aplicara y los servicios públicos tuvieran que pedirle autorización a cada uno de los ciudadanos (incluso, obviamente bajo la modalidad on line), cuando ya la ley y Dictámenes de la Contraloría reconocen que existe autorización para hacerlo legalmente, sería improcedente jurídicamente y una traba a la gestión de los servicios públicos.

(ii) Sobre los fines del tratamiento realizado a los datos personales recopilados desde o en el sitio web (que nunca podrán ser "*no legales*"), indicándose el nombre *"del banco de datos personales",* el fundamento jurídico de su existencia, su finalidad, los tipos de datos almacenados y una descripción de la categoría de personas a que alude, que son por cierto los requisitos definidos por el Decreto Supremo N°779 del año 2000 para el registro informativo del Registro Civil y respecto al cual debe contenerse un enlace o *link*;

(iii) Sobre las condiciones de confidencialidad y garantías existentes en el tratamiento de datos personales adoptadas -lo cual nos reenvía al cumplimiento del Decreto Supremo N°83 del año 2005-, y una referencia al hecho de que los datos serán o no transferidos a terceros o procesados por ellos (lo que se presenta cuando se licita y externaliza esta función), quienes deben ser individualizados en forma suficiente;

(iv) Sobre (i) la declaración expresa de los derechos de acceso o habeas data -y sus derivados- que en conformidad al artículo 12 poseen los ciudadanos en cuanto titulares -y recordemos propietarios- de los datos personales, para resguardarlos, (ii) y sobre los medios que ha dispuesto el servicio público para garantizar el ejercicio de esos derechos; y,

(v) Sobre la indicación de una dirección electrónica de contacto para que el usuario solicite y obtenga electrónicamente y en línea información sobre los datos personales que se mantienen registrados, y pueda ejercer mediante ella los derechos de acceso, modificación, eliminación, cancelación o bloqueo.

Luego de consagrarse la obligación general de que en los sitios web de los servicios públicos *"se adopte, mantenga y declare"* una política de privacidad, se señala que ella debe encontrarse accesible desde su primera página e incluir *"a lo menos"* -como un piso mínimo- las referidas menciones.

Una de las menciones adicionales que el Decreto no contiene, debiera ser si el servicio público utiliza y qué datos registra en base a mecanismos invisibles de gestión *on line*, como es el uso frecuente de sistemas de archivos *"cookies"* o *"rótulos"* que se instalan en el disco duro del computador del usuario que se conecta, sin que él lo sepa, sin que las autorice previamente o sin que pueda bloquearlos en su navegador (porque no sabe que se puede generalmente), en base a los cuales luego se fideliza y optimiza la conexión electrónica con el ciudadano y/o usuario que vuelve a ingresar al sitio web[107].

[107] Se llaman *"cookies de sesión"* cuando el archivo que se genera por el computador que accede al sitio, y son un identificador único que, aunque se diga lo contrario, si identifica personalmente al que sea el propietario del computador. Técnicamente se dice que este archivo expira al momento de cerrarse el navegador, y permite que el sitio web que la instala y la envía sepa -respecto del

No son menciones menores, máxime si existen Directivas Europeas[108] que se han opuesto a su uso, han exigido autorización previa para que se instalen en el computador del usuario y las han calificado de sistemas intrusivos y violatorios de la privacidad, aunque ellas no han contado con mucha adhesión formal de los países miembros y están siendo revisadas a esta fecha[109].

Aparece interesante tener a la vista un sitio concreto que intenta implementar estas condiciones, específicamente el del Blog de la Subsecretaría de Telecomunicaciones ubicado en la URL http://blog.subtel.cl/wp/?page_id=20. Si bien es cierto no cumple con todas las condiciones de la normativa (no se alude específicamente a la posibilidad de ejercer el Habeas Data o no se indica una dirección de contacto), el balance que hacemos desde el punto de vista de la información otorgada a los usuarios del blog y las explicaciones acerca de la finalidad de la recopilación de datos personales de los ciudadanos es positivo. Señala en concreto:

"PROTECCIÓN DE DATOS PERSONALES

Utilización de la información obtenida de los usuarios.

La recogida y tratamiento automatizado de los Datos Personales tiene como finalidad el mantenimiento de la relación establecida con el Blog de la Subtel; la gestión, administración, prestación, ampliación y mejora de los servicios; darse de alta o utilizar la adecuación de dichos servicios a las preferencias y gustos de los Usuarios; el estudio de la utilización de los servicios por parte de los Usuarios; el diseño de nuevos servicios relacionados con dichos servicios; el envío de actualizaciones de los

---

usuario *"rotulado"*-, qué paginas visitan, qué vínculos o enlaces usan, y cuánto dura la visita a cada página, es decir, los llamados *"datos que fluyen con el click"* y que permiten conocer, en definitiva, cuáles son los hábitos, intereses y necesidades de los usuarios.

Existen además las llamadas *"cookies persistentes"*, que a diferencia de las anteriores no expiran cuando se cierra el navegador si no que permanecen en el computador hasta que el usuario las elimina, y crean, asignan o asocian un identificador único al computador. Los administradores de los sitios que las instalan buscan crear una base de datos con las selecciones y preferencias previas del usuario que se conecta, y ofrecen una especie de servicio en que ahorrando tiempo y trabajo se genera un acceso automático a esos sitios. ¿La complicación para el usuario?: que si configura el programa navegador en Internet para que rechace o para que avise cuando de intenta instalar este rotulo persistente, el sitio web luego complica el usar las funcionalidades que ofrece hasta que los archivos son en definitiva instalados.

[108] Téngase presente: "*Una Directiva… es una norma con carácter legal que obliga en cuanto al objetivo perseguido pero no en cuanto a la forma en que este objetivo debe llevarse a cabo, lo que supone que los diferentes países miembros de la U.E podrán llevar a la práctica, a su manera, la obligación común a todos ellos de mejora de la protección de seguridad y privacidad en las telecomunicaciones perseguidos por esta reforma".*

[109] Véase las URL http://www.idg.es/pcworld/Solo-cuatro-paises-de-la-UE-se-adhieren-a-la-direc/doc32865-.htm y http://www.desarrolloweb.com/actualidad/cookies-cambian-reglas-juego-2636.html

servicios; el envío, por medios tradicionales y electrónicos, de información técnica y operativa. La finalidad de la recogida y tratamiento automatizado de los Datos Personales incluye igualmente el envío de formularios de encuestas, que el Usuario no queda obligado a contestar.

Privacidad de los Datos Personales.

La Subtel se preocupa por la protección de datos de carácter personal de sus Usuarios, por lo cual, asegura la confidencialidad de los mismos, y no los transferirá o cederá o de otra manera proveerá, salvo en aquellos casos en que la legislación vigente así lo indique. El uso que el Usuario haga del Blog puede ser almacenado con el objeto de generar una información estadística respecto a la utilización de las secciones, partes y en general, del Contenido de éstos, de manera de determinar los números totales y específicos, por sección, de visitantes, con el objetivo principal de conocer las necesidades e intereses de los Usuarios y otorgar un mejor servicio.

Sobre la seguridad de la información.

La Subtel ha adoptado los niveles de seguridad de protección de los Datos Personales legalmente requeridos, y ha instalado todos los medios y medidas técnicas a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los Datos Personales facilitados por los Usuarios".

3. Previo a las definiciones normativas ya analizadas se realizaron una serie de estudios y reuniones de trabajo. Entre ellos, cabe recoger algunas consideraciones que creemos mantienen vigencia a esta fecha y que explican el tenor de lo establecido en definitiva en el artículo 9° del Decreto Supremo N°100[110], y obedecen a un análisis "*cualitativo"* de la situación a esa fecha -el año 2004- de los sitios web de los órganos de la Administración[111].

Estando a Diciembre del 2009 vigente el artículo 9° del Decreto Supremo 100, sería conveniente volver a realizarlo para comparar el impacto de esta norma. A efectos de nuestro Informe y a falta de información actualizada, sirve de referencia.

Se trabajó en base a un instrumento único de evaluación que establecía una plantilla de diversas condiciones -no copulativas- para verificarse -o no- en los

[110] Estas consideraciones están tomadas de un 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, impulsado por el MINSEGPRES de la época y coordinado por el abogado y profesor Alberto CERDA.

[111] El Capítulo Primero se denomina *"Análisis de la normativa interna aplicable",* pero se limita a transcribir latamente consideraciones doctrinarias acerca de la ley 19.628 y sus contenidos, mismas que después se repiten en la Parte Segunda en forma resumida.

diversos sitios web, con el objetivo esencial de averiguar (i) qué cantidad de sitios recogían en forma visible o mediante la entrega voluntaria de datos por los ciudadanos mediante formularios o aplicaciones especialmente diseñadas al efecto[112] *-no mediante mecanismos técnicos invisibles de registro como las cookies que en forma oculta se instalan en los computadores del usuario on line, porque técnicamente no es fácil testear su uso-*, y (ii) cuántos sitios web cumplían, al hacerlo, con lo dispuesto por la ley 19.628[113].

A esa fecha el 100% de sitios web de los servicios públicos estaba determinado por 266 sitios, y mediante un muestreo probabilístico, aleatorio simple, de selección particular y por azar o que genera muestras se eligieron a 130 páginas de los 21 Ministerios que conforman la Administración del Estado.

A modo de revisión somera de los resultados de la encuesta, cabe consignar: (i) frente a la pregunta de si se recogían visiblemente datos personales el 60 % (78 sitios) respondió que sí; (ii) frente a la pregunta de qué tipos de datos y con qué fines se recogen, se consignaron los de identificación, localización y ocupación y con fines de información o contacto y de registro; (iii) frente a la pregunta de si se informaba la finalidad de la recolección, sólo el 18% (14 sitios) lo hacía; (iv) frente a la pregunta de si se informaba que tratamiento se haría con esos datos recogidos, sólo el 9% lo hacía; (v) frente a la pregunta de si se informaba al usuario acerca de los derechos que poseía como titular -en conformidad al artículo 12 de la ley 19.628, sólo un 5% cumplía parcialmente con la obligación; (vi) consultados acerca de si eventualmente y en forma automatizada se comunicaban o no los datos personales recogidos a terceros una vez que ellos se indexaban, sólo un 21% lo hacía; (vii) frente a la pregunta de si se contemplaba un mecanismo de *"habeas data"* en línea -que no es una obligación legal o carga sino sólo una circunstancia recomendable-, sólo un (1) servicio lo tenía, porque había establecido una específica dirección electrónica de contacto al efecto; (vii) y consultados directamente acerca de si a esa fecha

[112] Los casos más frecuentes de recogida voluntaria de datos en un sitio web se presentan cuando se deja registrada una dirección de correo electrónico para recibir avisos, cuando de contesta una encuesta o cuando se hace una consulta no anónima. Evidentemente, los aportados son legalmente en Chile datos personales o nominativos, y a su respecto es posible exigir que sólo se usen para los fines declarados al recopilarse; esto último, al menos en el sector privado, es lo que generalmente no ocurre, porque la información sobre los usuarios se comercializa, se cruza, se perfila, se cede, se intercambia y se usa para el envío de spam, siempre sin una autorización *"real"* sino formal del usuario que acepta todas las condiciones sin saber en realidad lo que aceptó; y esto último sería ilegal de verificarse con la información de los ciudadanos que se registren en los sitios web de los servicios públicos.

[113] Esta consulta más bien formal se respondió en algunos casos con el señalamiento o la referencia informativa que en el sitio web se hacía a la ley de manera general -por ser el contexto legal del tratamiento-, en nuestra opinión un señalamiento suficiente, por cuanto los servicios públicos no deben auto regular normas de Derecho Público que les serán siempre aplicables, y menos deben, como se pretendía en el grupo de trabajo, elaborar cartillas informativas sobre los contenidos de la ley como una práctica obligatoria de los servicios públicos.

poseía formalmente declaradas y publicadas un texto en forma o similar al de las *"Políticas de Privacidad",* sólo el 15% las poseía.

Por cierto, la parte final del Informe contiene algunas sugerencias, consideraciones u observaciones relacionadas con el uso de mecanismos *"invisibles"* o que implican un tratamiento oculto de recogida de datos, como es el uso muy corriente en todos los sitios web de sistemas de *"cookies".*

Lo que no compartimos en su momento ni ahora, por ilegal e inaplicable, es la intención manifestada de formularse una especie de *"Código Deontológico de Conductas"* que se utilizara bajo el nombre de *"Políticas de Privacidad*", mediante el cual los servicios públicos se auto regularan contractualmente para el desempeño de sus funciones en materia de tratamiento de datos personales a partir de la información recogida en los sitios web institucionales.

G. Regulación jurídica de la seguridad de los STDP en los servicios públicos. Análisis del Decreto Supremo N°83, del 2005, y de las eventuales sanciones penales.

1. De cara a la necesidad de proteger los datos personales de los ciudadanos esto no es teoría. Por ejemplo, recientemente se ha cuestionado públicamente las filtraciones de datos personales desde los sistemas de la JUNAEB[114], lo que incluso generó auditorías de la Contraloría General de la República[115]. Ocurre lo mismo con situaciones anteriores de filtrado de datos personales de 6 millones de ciudadanos[116].

En todo sistema informático, sobre todo si se producen interconexiones a diversos servidores vía redes abiertas como Internet, la seguridad es un problema de gestión, de diligencia y ético que le compete, principalmente, a los administradores del sistema y a los responsables de sus bases de datos.

Si no se actúa diligentemente; si no se resguarda la confidencialidad e integridad de datos y documentos recopilados, procesados, almacenados y transmitidos; si no se vela por autenticar debidamente a los usuarios que acceden al sistema, surgen responsabilidades, tanto para los administradores como para

[114] Véase la URL http://www.colegiotecnologico.cl/noticias/66-tecnologia/1326-directo-de-junaeb-interpuso-querella-por-delitos-informaticos

[115] Véase la URL http://www.contraloria.cl/NewPortal/portal2/ShowProperty/BEA%20Repository/portalCGR/Documentos/Informes_de_Auditoria/DIVISION_AUDITORIA_ADMINISTRATIVA/AREA_EDUCACION_TRABAJO_Y_PREVISION_SOCIAL/2009/AUD09_ETP07_INFORME_FINAL_AUDITOR%C3%8DA_DE_SISTEMAS_JUNTA_NACIONAL_DE_AUXILIO_ESCOLAR_Y_BECAS-DICIEMBRE_2008

[116] http://www.jec.cl/articulos/?p=1963

terceros que eventualmente, en forma indebida y sin autorización, accedan a la data -ahora personal o nominativa pero no sólo la de esta naturaleza- de los sistemas.

Además de poder hacerse efectivas las responsabilidades generales civiles por una actuación negligente que causa perjuicio a los ciudadanos, existen responsabilidades específicas establecidas en Chile, a saber: en materia de resguardo de datos personales o nominativos -ley 19.628-; en materia de autenticación de identidades, integridad de documentos y certificación de firmas digitales o electrónicas -ley 19.799-; en el ámbito la normativa sobre Bases Generales de la Administración del Estado -ley 18.575, artículos 2°, 4° y 42° y el Estatuto Administrativo, conforme a las cuales las faltas administrativas pueden constituir una causal de término de la calidad de funcionario-; y en materia de delitos informáticos, sea que los cometan terceros externos al sistema o personal interno del servicio público administrador -ley 19.223 y modificaciones en curso-.

2. Ya mencionamos -dentro del contexto de la revisión de los contenidos de la ley 19.628- las normas que en la ley 19.628 se refieren a la gestión diligente del funcionario responsable de la base de datos del servicio público.

En efecto, establece el *artículo 11°* que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Y en el Título V, sobre la responsabilidad por las infracciones a la ley, el *artículo 23* dispone que la persona natural o jurídica privada *"o el organismo público"* responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en caso, lo ordenado por el tribunal.

3. *Diligencia, seguridad y responsabilidad son los conceptos claves*.

En un plano de *"lege ferenda",* cabe consignar que a esta fecha el Boletín 6120 ya referido, que modifica el tenor de la ley 19.628, eleva las exigencias y las obligaciones en materia de seguridad de sistemas de bases o bancos de datos personales o nominativos[117] y modifica las normas sobre la responsabilidad derivada en caso de negligencia del responsable de la base de datos personales.

[117] Parece necesario aclarar algunos conceptos que son usados por juristas e ingenieros errada a indistintamente. Téngase presente que *"la privacidad o intimidad"* es un atributo, un derecho de la personalidad y una garantía fundamental consagrada constitucionalmente de las personas, naturales o jurídicas; y que los sistemas informáticos, computacionales o telemáticos -léase redes- no poseen privacidad o intimidad, porque a su respecto sólo cabe exigirse *"confidencialidad o reserva"* de la información, de los datos o de los documentos que en ellos se procesan y

En el artículo 11° se propone agregar nuevos incisos, para establecer (i) que el responsable del tratamiento de datos deberá arbitrar las medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su tratamiento indebido; (ii) que *"reglamentariamente"* -lo cual es muy rígido, atendido lo variable de las normas sobre seguridad de sistemas- serán fijadas las condiciones de seguridad que deben adoptarse por el responsable del tratamiento a efectos de dar cumplimiento a las obligaciones a que se refiere el presente artículo; y, por último, (iii) que *"se considerará indebido"* el registro de datos de carácter personal en ficheros o bancos de datos que no den cumplimiento a las exigencias que determine el reglamento[118].

En cuanto a la responsabilidad y como señala el Mensaje del Boletín 6120, se perfecciona el sistema de responsabilidad civil o se fortalece el derecho del titular a ser reparado por el responsable de la base de datos, de los daños que sufra como consecuencia del incumplimiento de lo previsto en esta ley.

Con este *"Norte"* legislativo, se contempla una regla de presunción de responsabilidad a favor del titular de los datos nominativos en los casos en que se acredite infracción a la ley 19.628, lo que debiera ocasionar que los responsables de las bases tomen -preventiva y efectivamente- todas las medidas necesarias para la seguridad de los datos nominativos. Además, se establece la responsabilidad solidaria del responsable del tratamiento de datos personales y autor del daño -y no del *"encargado",* una nueva figura que se crea-, y con aquellas entidades respecto los cuales sea cesionario porque le han transmitido dichos datos errados, falsos o inexactos[119].

---

almacenan, y estos atributos se logran con la adopción preventiva y reactiva de medidas de seguridad física y lógica de sistemas.

[118] Si se quiere tener una referencia del Derecho Comparado, puede revisarse el artículo 9 de la LORTAD española de 1992, que sólo se concretó mediante el *Real Decreto 994/1999, del 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. En el Título II, el artículo 9 sobre seguridad de los datos dice que (i) el responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. (ii) Agrega o prohíbe que se registren datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. Y, (iii) en forma programática, dispone que reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos.

[119] Por cierto: nada dice el artículo propuesto para el caso en que el responsable de la base de datos del servicio público sea *"cedente"* de la información, lo cual es una omisión que debiera repararse.

4. *Reglas generales de responsabilidad administrativa y deberes de diligencia en materia de seguridad de los STDP, contemplados en la Ley General de Bases de la Administración del Estado.*

La idea esencial es que la gestión de los STDP debe ser diligente y que la negligencia, la culpa o el no cumplimiento de los estándares normativos (ley 19.6268 y Decreto Supremo 83 en especial) debe sancionarse jurídicamente y mediante indemnizaciones si a los ciudadanos se le ocasionan perjuicios.

"...Existe consenso en la doctrina y en la jurisprudencia que cualquier acción u omisión de la autoridad pública que causa un daño a un particular, en que exista relación de causalidad entre uno y otro, genera responsabilidad para el Estado, el que deberá reparar el detrimento causado, de acuerdo a las normas que el ordenamiento jurídico establece al respecto, estatuto propio y distinto al las normas de responsabilidad contenidas en el Código Civil, que rige las relaciones de particulares entre si, o en el Código Penal, que se aplica a las personas ante la comisión de un delito o cuasidelito, cuyas bases son el dolo o culpa del agente activo"[120]*.*

Se deben tener a la vista en el ámbito de esta normativa -la ley 18.575- a los artículos 2°, 4° y 42°, para concluir que el Estado chileno es responsable administrativa -y civilmente en conformidad a las reglas generales- por todo daño que provoque a los ciudadanos titulares de los datos personales, como por ejemplo si al no haberse adoptado mínimas medidas de seguridad se acceden a los servidores de la red Internet de un servicio público y se copian las bases de datos que por ley son secretos o reservados[121].

Podrán presentarse casos de negligencia inexcusable, como si se pudiera ingresar a un sitio web con cualquier clave o no con la generada previamente por el titular, o como si se hubiera mandado a respaldar la información en una empresa externa y en el trayecto o desde esa empresa se filtrara a otras empresas dedicadas al tráfico de bases de datos[122].

---

[120] Véase la URL http://www.institutolibertad.cl/p_251.htm

[121] *"La responsabilidad del Estado nace como un mecanismo para limitar el abuso de éste y de sus órganos, y en Chile se encuentra consagrada en la Constitución Política de la República (CPR), en sus artículos 6º, 7º, 19 Nos 7º, 20º y 24º, 38º inciso 2º y45º, en el artículo 4ºy 42º de la Ley 18.575, LOCBGAE de 1986, en el artículo 142º de la ley 18.695, Orgánica de Municipalidades; artículo 38 de la Ley19.966; y, 174º de la ley 18.290, de Tránsito, entre otras".* Véase la URL http://www.institutolibertad.cl/p_251.htm.

[122] (i) Conocido es el caso de un banco inglés, el HSBC, que el año 2008 tuvo que admitir el extravío de un disco cuando era trasladado de una sucursal a una compañía de seguros; el dispositivo habría tenido información de 370.000 clientes, con antecedentes tales como los nombres, las fechas de nacimiento y detalles -pero no los números- de las cuentas corrientes. (ii) También en Inglaterra, un año antes, *el Servicio de Aduanas* perdió unos disquetes informáticos, que contenían la base de datos de 25 millones de personas, al ser enviados por correo desde unas oficinas en Londres a Newcastle. (iii9 Y nuevamente en Inglaterra, en Mayo del 2009 se supo del

Sin entrar en el tema de si la responsabilidad jurídica que cabe imputarle al Estado en Chile es efectivamente la *"subjetiva, por culpa o por falta de servicio"*[123] o es la "*objetiva*"[124] -que no considera exigir la concurrencia de elementos subjetivos de reprochabilidad en los funcionarios públicos, y que entiende que todo daño que se produzca a un ciudadano que no se encuentre jurídicamente obligado a soportarlo debe ser indemnizado, por el sólo hecho de haberse generado un riesgo o contingencia de daño[125]-, ...es claro que (i) atendida la especialización y lo complejo del ámbito de la seguridad de sistemas, de las bases de datos y de las redes telemáticas y (ii) por lo dispuesto en el artículo 42° de la ley 18.785, habrá que demostrar -por parte del ciudadano afectado, lo que es una carga compleja- que se produjo una violación a un deber mínimo de diligencia en materia de seguridad de sistemas, que en derecho -y conforme a las normas referenciadas- cabe exigirle al servicio público, más que el funcionario público responsable de los sistemas informáticos y, en concreto, del tratamiento de datos personales.

El *artículo 2°* establece la regla general, la del el principio de la actuación administrativa o del ejercicio de las potestades públicas ajustado a la Constitución y a las leyes, dentro de su competencia y sólo de la mano de las atribuciones que expresamente le haya conferido el ordenamiento jurídico a los funcionarios públicos. Y como complemento, de haber abusos o excesos establece que habrá lugar a las acciones y recursos correspondientes.

El *artículo 4°* preceptúa que el Estado será responsable por los daños que causen los órganos de la Administración en el ejercicio de sus funciones, sin

---

extravío de una base de datos de la RAF con antecedentes cuestionables y direcciones de 50.000 militares (tales como problemas bancarios, relaciones extramatrimoniales, adicciones, historiales médicos, etcétera, que podría ser utilizado para chantajes).

123 *"...La responsabilidad por culpa, también llamada subjetiva, es aquella que hace responsable al agente que causa el daño a condición de que éste haya actuado con culpa o dolo. En esta hipótesis, no basta la mera relación de causalidad entre el hecho y el daño producido a consecuencia de aquél, si no que además se requiere que tal hecho sea imputable a una determinada conducta del sujeto que lo ha provocado, realizada con intención inequívoca de causar daño o con negligencia, obligando a probar que los perjuicios tienen como antecedente causal la culpa o dolo del agente activo".*

124 *"...La responsabilidad objetiva tiene como fundamento en que, aquél que crea un riesgo, ejerce una determinada actividad o se sirve de una determinada cosa en provecho propio, debe asumir los efectos de las mismas, sin calificarse la acción del responsable, sólo interesando la relación de causalidad entre el hecho y el daño".*

125 *"En un sistema de responsabilidad objetiva el Estado siempre será responsable de las consecuencias perjudiciales de los actos que ejecuta, aun cuando obre lícitamente y haya tomado todas las precauciones posibles para no causar daño, y lo único que tendrá que demostrar la víctima del hecho, para obtener la reparación, será el daño o perjuicio sufrido, así como la relación de causa entre ese daño y el hecho en cuestión".*

perjuicio de las responsabilidades que pudieren afectar al funcionario que los hubiere ocasionado.

Y el *artículo 42*°, a su turno, señala que los servicios públicos serán responsables del daño que causaren por falta de servicio, agregando que el Estado tendrá el derecho de repetir en contra del funcionario que hubiere incurrido en falta personal. Por cierto: esta norma es la que sustenta en doctrina el afirmar que el Estado Chileno y sus funcionarios son subjetivamente responsables, y que la falta de servicio exige expresamente probar la falta; es decir, no bastaría con la relación de causalidad sino que es necesaria la existencia real de la falta, sea de funcionamiento, de funcionamiento tardío o de deficiente funcionamiento del servicio público, causándose un perjuicio a los usuarios o destinatarios del servicio; y esto, *"....sin que importe individualizar ni perseguir al funcionario cuya acción u omisión personal origina la falta"*, ...porque *"lo que se requiere es invocar y acreditar la existencia de la falta en la actividad del órgano administrativo y que ella es la causa del daño experimentado por la víctima"*[126].

5. Una propuesta personal sobre una política de seguridad en materia de sistemas o de bases de datos personales al interior de los servicios públicos. La importancia de prevenir.

5.1 Lo primero siempre será *"prevenir*", porque el establecimiento o la tipificación legal de conductas que por su gravedad se sancionan con penas privativas de libertad no garantiza ni evita que se cometan delitos. Es necesario ser diligente y responsable adoptándose las medidas de prevención para evitar dichos ataques que, aunque luego castigados, de ser exitosos pueden tener consecuencias económicas importantes[127], pero bajo el supuesto de que la existencia de mecanismos de seguridad computacional debe ser vista por las organizaciones públicas del Estado con la misma naturalidad y alerta con que se instalan extintores contra incendios o personal de vigilancia contra delitos tradicionales.

---

[126] Se sostiene en doctrina: (i) *"...la falta del servicio se atribuye directamente al órgano por su mala organización o funcionamiento defectuoso, por referencia a lo que se está en derecho de exigir de un servicio público moderno, es decir, aquello que debe ser su comportamiento normal"*; (ii) *"...la falta de servicio denota el incumplimiento de un deber de servicio que puede consistir en que no se preste un servicio que la Administración tenía el deber de prestar, o que se preste tardía o defectuosamente de conformidad con el estándar de servicio que el público tiene derecho a esperar".*

[127] Sólo durante una semana de septiembre del año 2002 se constataron más de 2 millones de incidencias de seguridad en redes de información en Europa, convirtiéndose en la principal amenaza para entes públicos y privados como medio y fin para cometer delitos. *"Que se actúe a distancia y sin violencia física no debe llevar a pensar que es un problema lejano ni menor. Son dichas características las que precisamente los hacen más peligrosos y fáciles de cometer. Mentalizarse de que la vulnerabilidad alcanza a todo el que esté conectado a una red -con independencia del tamaño o el sector de actividad- es el primer paso…".*

Si ampliamente se considera que el desarrollo e implementación de sistemas de seguridad específicos, idóneos o apropiados deben contemplar medidas preventivas que abarquen desde las más habituales vulneraciones desde el exterior hasta el tratamiento de los datos por funcionarios técnicamente calificados del servicio público, la cuestión central pasa entonces por determinar que elementos permitirían demostrar debida diligencia, actuación responsable y cuidado al actuarse preventivamente.

Uno esos posibles elementos es la realización de certificaciones de seguridad por empresas auditoras externas[128], procesos evaluativos que son rígidos y de un costo no menor, que se desarrollan en el mediano y largo plazo y que permitirán a los órganos de la Administración reivindicar que se han cumplido determinados y concretos estándares de seguridad.

Una interrogante de trabajo: *¿cuántos servicios públicos habrán presupuestado y realizado estas certificaciones?.*

Estas certificaciones externas apuntan, en general, al cumplimiento del estándar de seguridad informática ISO 17799[129], que a pesar de ser un estándar abierto o genérico -no cerrado ni propietario o de alguien en particular-, se ha impuesto porque permite a las empresas, servicios públicos y bancos contar con un punto de referencia único o una base metodológica de *"las buenas o mejores prácticas*" para acreditar diligencia y responsabilidad en su gestión, la que no descansaría necesariamente en la adopción de tales cuales productos o soluciones tecnológicas[130], al definir parámetros de controles y de seguridad de información.

5.2 Particular preocupación por la seguridad de los STDP debe asumirse en materia de tratamiento o manejo de información en grandes volúmenes, porque será mayor el impacto en los derechos y en la integridad de los ciudadanos en caso de pérdida o mal uso de ellos, en las operaciones o procesos en que la información sea recopilada, procesada, almacenada y cruzada o perfilada desde, o en base a sistemas computacionales. Por cierto, es muy difícil que en forma

---

[128] A modo de ejemplo véanse en Internet las URL http://www.trusecure.com/solutions/index.shtml y http://www.trusecure.com/solutions/products/index.shtml.

[129] La corporación ISO tiene como proceso normal el revisar como máximo cada 5 años sus normas; a consecuencia de ello y como algo natural (recuérdese que la seguridad es dinámica) a fines del segundo semestre del año 2005 se realizó una modificación de la 17799, que quedó numerada como ISO 27001. Más ampliamente, se definió una nueva "familia" o agrupación de estándares de seguridad denominada "grupo 27000".

[130] Sólo teniéndose primero clara una "*Política"* o "*Norte"* de actuación preventiva, deben adquirirse las "*específicas herramientas electrónicas de seguridad"* que, en un ambiente interconectado deben implementase al interior de la organización. Pero estas existen y son conocidas de sobremanera en el mercado. El problema no es propiamente "*tecnológico"* sino más bien "*de gestión".*

manual, mecánica o en soporte papel se manejen grandes volúmenes de data personal, pero las normas si es posible extenderlas a estas hipótesis.

En consecuencia:

(i) no debe mantenerse información confidencial en hojas impresas sin el resguardo correspondiente, ni desplegada en los monitores o pantallas al alejarse o ausentarse los funcionarios de los puestos de trabajo;

(ii) es fundamental proteger adecuadamente cualquier medio (CD, cintas, cartridges, disquetes, listados en papel, etc.) que contenga información, para evitar que pueda ser obtenida por terceros;

(iii) los recintos de custodia deben estar protegidos contra elementos ambientales nocivos, tales como polvo, calor o humedad, y deben contar con mecanismos de alarma de acceso y censores de humo y fuego;

(iv) al trasladarse los equipos portátiles fuera de las dependencias o instalaciones del servicio el portador es responsable de su custodia y del resguardo de la información que contienen, y al ser enviados al servicio técnico, los discos o dispositivos de almacenamiento deben ser removidos y guardados bajo custodia para evitar que terceros puedan acceder a los datos almacenados en ellos;

(v) toda la información que eventualmente se entregue al exterior del servicio público, toda la que se entregue a terceros diversos de los ciudadanos, por cualquier vía, sea en el marco de un convenio de intercambio de información, sea por mandato legal expreso o mediando excepcionalmente un requerimiento judicial, deberá ser previamente autorizada por la Jefatura correspondiente;

(vi) tratándose de las necesarias restricciones especiales para el acceso a información que se obtenga mediante el uso de los sistemas de manejo de grandes volúmenes, los funcionarios responsables deberán ser determinados previa y expresamente por el responsable de la seguridad de los sistemas mediante una resolución formal y específica, y la jefatura respectiva, deberá permanentemente monitorear, auditar y fiscalizar el desempeño de las labores de procesamiento que les sean encomendadas.

6. *El contenido del Decreto 83.*

No obstante la vigencia de esta norma, el problema que se presenta en relación a ella es que nadie, ningún servicio público, fiscaliza sistemáticamente su cumplimiento[131].

[131] Un cuestionario acerca de su aplicación práctica, puede verse en la URL http://www.estrategiadigital.gob.cl/files/Guia_Metodologica_PMG_Gobierno_Electronico_2009.pdf

En concreto, todo servicio público que trate datos personales debe implementar las medidas de seguridad de sistemas que en forma obligatoria establece el Decreto Supremo N°83 del año 2005, definidas en base a estándares internacionales o a las normas ISO sobre el tema.

La base esencial de este trabajo fue una norma publicada el año 2003 por el INN; de hecho, el Decreto 83 se refiere a ella reiterada y expresamente. Ella tradujo, a su vez, para Chile, la Norma ISO 17799 -sobre seguridad de sistemas, servidores y bases de datos-. A pesar de que se trata de un estándar aplicable tanto para el sector público como para el privado, son sólo recomendaciones o sugerencias que no son fiscalizadas en cuanto a su aplicación o implementación concreta. La norma es la NCh2777.of2003, y se denomina como un "*Código de Práctica para la gestión de la seguridad de la información".*

En general, a nivel de guías metodológicas elaboradas por el propio Gobierno o de aspectos a ser fiscalizables a la luz de esta norma -y de otras relacionadas como el Decreto 77-, es de esperar que todo órgano de la Administración vele, en materia de seguridad de datos, documentos, expedientes y comunicaciones electrónicas, al menos: porque se usen mecanismos de autenticación o de control de acceso de los funcionarios para accederse a los sistemas; porque se posean implementadas medidas de seguridad para evitar la intercepción, obtención, alteración o cualquiera forma de acceso no autorizado; porque se incorporen mecanismos periódicos de auditorías de seguridad y de confidencialidad de sistemas y bases de datos; porque se haya designado formalmente a un funcionario responsable en materia de seguridad de sistemas y bases de datos; porque se clasifiquen los documentos electrónicos en cuanto a su prioridad y grado de protección necesarios; y, porque se cuente con políticas de seguridad de acceso, uso, almacenamiento y transferencia de datos y de documentos electrónicos rigurosas y claramente informadas a los funcionarios públicos.

7. De cara al almacenamiento de datos personales en bases o bancos de datos, debe considerarse además si los servicios públicos cumplen diligentemente con las *medidas técnicas que a propósito de los repositorios de información y/o documentos establece el Reglamento de la ley 19.799, DS N°181 del año 2003.*

Cada servicio público debe ajustarse a una serie de normas que regulan, para toda la Administración del Estado, la forma de almacenar en *"repositorios"* electrónicos los documentos y/o expedientes electrónicos que contengan los datos personales de los ciudadanos.

El artículo 42 del Decreto Supremo 181 establece imperativamente que los órganos de la Administración del Estado deberán contar con *“un repositorio o archivo electrónico”* a efectos de su almacenamiento una vez que haya finalizado su tramitación, de conformidad con las normas que regulan a su respectiva oficina

de partes. Y el artículo 43 señala que el repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida, para lo cual la información nominativa deberá ser respaldada en copias de seguridad.

8. *Eventuales sanciones penales ante las violaciones a la seguridad de los sistemas de los servicios públicos*.

Pueden surgir eventuales responsabilidades penales y/o sanciones ante la infracción del deber de diligencia y confidencialidad para los funcionarios que tengan acceso a la información reservada, confidencial y nominativa almacenada en los sistemas informáticos del órgano de la Administración del Estado[132].

La ley chilena vigente desde junio de 1993 es la 19.223, contempla penas que van desde 61 días hasta 10 años.

Considera como delitos informáticos el daño de los soportes físicos, de los fierros o hardware, de las partes o componentes del sistema a pesar de que se trata de un delito común de daños.

Tipifica como delito el ilícito contra cualquier sistema de tratamiento información, pero en abstracto, ampliamente, sin considerar la naturaleza de los datos eventualmente atisbados, copiados, modificados, alterados, dañados o destruidos.

El artículo primero de la ley 19.223 sanciona a quien maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento. La pena establecida es presidio menor en su grado mínimo a medio, esto es, de 61 días y hasta 3 años.

También se sanciona como delito contra un sistema de información si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, y se aplicará la pena señalada en el inciso anterior en su grado máximo, es decir, de 3 años y 1 día a 5 años.

El segundo, a quien con el ánimo de apoderarse, usar o conocer indebidamente la información intercepte, interfiera o acceda a un sistema de

[132] Únicamente porque la tecnología computacional, los archivos y documentos electrónicos, las bases de datos, los discos duros, los correos electrónicos y la red Internet son herramientas esenciales en un servicio público, una conducta ilícita puede realizarse mediante soportes computacionales y violando su confidencialidad o reserva. Y las NTI, TICs o Tecnologías de la Información y las Comunicaciones son una variable cada vez más presente en la comisión de delitos, situación que se agrava ya que por regla general los delitos contemplados en los Códigos Penales tradicionales no comprenden -porque no pueden hacerlo, como el chileno que es de 1875- a los ilícitos realizados mediante un ordenador o computador y contra los programas y los datos o la información de un sistema informático.

tratamiento de información, y será castigado con presidio menor en su grado mínimo a medio o de 61 días y hasta 3 años. Se trata de una hipótesis de acceso no autorizado a información contenida en sistemas de tratamiento de información, dentro de los cuales están los electrónicos o informáticos, o de un caso de "hacking", pero no de un mero acceso y por el sólo hecho de acceder sino con la exigencia de concurrencia de un elemento subjetivo adicional -ánimo de apropiación, uso o conocimiento-.

El tercero, muy similar o relacionado con el artículo 1º, castiga a quien maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, y será castigado con presidio menor en su grado medio o de 541 días a 3 años. A algunos ha llamado la atención la excesiva severidad con que se aborda la destrucción de estos objetos, sin atender mayormente al valor económico o a la cuantía de los mismos.

El cuarto, a quien maliciosamente revele o difunda los datos contenidos en un sistema de información, el que sufrirá la pena de presidio menor en su grado medio -541 días a 3 años-, y si quien incurre en estas conductas es el propio funcionario público responsable del sistema de información la pena se aumenta en un grado –de 3 años y 1 día hasta 5 años-.

H. Regulación jurídica del dato personal "*dirección de correo electrónico*", tanto "*de los ciudadanos"* como *"de los funcionarios públicos".*

1. *Los correos electrónicos pueden ser datos personales*[133]*.*

Si por la definición legal del artículo 2° de la ley 19.628 un dato personal es el relativo a *cualquier información concerniente a personas naturales, identificadas o identificables*, una dirección de correo electrónico poseerá tal calidad en la medida que permita la identificación del ciudadano, del administrado o de un funcionario público. Así ocurre por ejemplo con las direcciones *renato@jijena.cl; info@jijena.cl* o *rjijena@consejodetransparencia.cl*. Y no ocurriría con direcciones del tipo "*supertaldo@gmail.com"* o "*morena@hotmail.com"*. Este acápite del Informe se refiere al primer grupo de antecedentes nominativos.

[133] No es necesario profundizar en la descripción tecnológica o física de lo que son los correos electrónicos. En ese sentido, resulta obvio entender que se trata de sistemas de comunicación electrónica, informática y telemática y de servicios de mensajería de la misma naturaleza, en los que existe una comunicación diferida y no interactiva entre dos sistemas, uno que lo emite o envía y otro que lo recibe, y que mediante los correos pueden enviarse adjuntos textos, imágenes, datos o archivos con mensajes de voz.

Tampoco resulta original afirmar que *"el dato dirección de correo electrónico"* puede dar a conocer nombres y apellidos de una persona, quizás la zona geográfica de residencia u origen *(pero no necesariamente, porque uno puede usar cuentas de extensión ".cl" sin estar en Chile*), o la empresa o servicio público donde trabaja un funcionario determinado.

Lo que si es inexacto es afirmar -como se ha hecho- que un dato *"dirección de e-mail"* puede evidenciar o reflejar aspectos delicados de una persona como su inclinación política, religiosa o sexual, salvo que expresamente quien envía el correo mediante una cuenta de por ejemplo un partido político determinado quisiera ser reconocido o asociado a la militancia de ese partido político, lo cual ya no es una fidelización furtiva o clandestina del dato que realiza sin autorización quien recopila las direcciones de correo.

Una de las últimas modificaciones legales promulgada en Chile ha puesto de relieve la importancia que va adquiriendo progresivamente *el dato personal dirección de correo electrónico de los ciudadanos*, al darle, excepcionalmente, la calidad de domicilio legal complementario en materia de notificaciones administrativas. En efecto, con fecha 5 de Diciembre del año en curso se público en el Diario Oficial la ley 20.406, la que, a propósito del acceso por parte del Servicio de Impuestos Internos a las operaciones bancarias de personas determinadas y reemplazando el artículo 62 del Código Tributario, estableció un procedimiento administrativo para formular los requerimientos de información bancaria sometida a secreto o reserva[134].

2. *Recopilación y uso de las direcciones de correo electrónico de los ciudadanos.*

No existe norma legal alguna que obligue a que los ciudadanos entreguen a los servicios públicos sus direcciones de correo electrónico, por cuanto ellas no son susceptibles, salvo excepciones expresas como la referida ley 20.406, de ser legalmente calificadas como "*domicilio".*

Que así fuera sería complejo, porque no obstante poder ser datos personales, técnicamente las casillas electrónicas son por esencia aleatorias, constantemente modificadas y desactivadas, no permanentes, susceptibles de ser

[134] En el contexto anterior, (i) el numeral 2 señala que el banco que sea requerido puede notificar al titular de la información, alternativamente, o por carta certificada o por correo electrónico, cuando así esté convenido o autorizado expresamente; (ii) el numeral 4 dispone que cuando el titular no responda y el banco deba informar al SII sobre si se ha producido o no la respuesta, será haciendo referencia tanto al domicilio como a la dirección de correo electrónica registrada; y (iii) el nuevo artículo 62 bis establece que cuando sea procedente solicitar autorización judicial y ella deba ser notificada al titular de la información bancaria, ello podrá hacerse por cédula o por avisos, pero adicionalmente y sin afectar la validez de la notificación, el Secretario del Tribunal debe avisar de la notificación también por correo electrónico.

eliminadas unilateralmente por los proveedores de servicios gratuitos y por regla general no son homologables con las direcciones físicas legalmente recogidas.

En consecuencia, si proactivamente la recogida de las direcciones le es solicitada *"de hecho"* mediante el llenado de formularios a los ciudadanos para optimizar, agilizar y fidelizar la prestación de los servicios públicos[135], y el ciudadano sin estar obligado entrega o anota en ese formulario su dirección de email, cabría entender que ha operado la autorización del artículo 4° de la ley 19.628[136].

Aunque en estricto rigor se percibe más bien dada en forma tácita, no cabe duda que el administrado ha consentido voluntariamente en que el órgano administrativo "*trate" -pero debe precisarse el alcance-* y procese sus direcciones de correo electrónico, porque no puede entenderse que la autorización es una especie de *carta blanca* que permite a un servicio público realizar todas las amplias operaciones incluidas en el concepto de "tratamiento" de la ley 19.628, y porque en estricto rigor la autorización debe ser expresa e informada.

Debe partirse del supuesto que los servicios públicos (i) han obtenido lícitamente las direcciones y actuando en el marco de su competencia; (ii) que se trata de datos personales que legalmente no son de naturaleza y no provienen de fuentes públicas; y, (iii) que las posteriores comunicaciones hacia los ciudadanos sólo buscarán cumplir los fines promocionales y asistenciales que son inherentes a los servicios públicos.

Y debe considerarse que concurrirá siempre una "autorización" legal mediata, la del artículo 4° de la ley 19.628 que alude a la autorización o al consentimiento directo del titular del email como mecanismo habilitante, que en estricto rigor sería una habilitación expresa que el legislador reconoce a los servicios públicos que han recibido voluntariamente de los ciudadanos titulares las direcciones de correo electrónico.

Si las leyes facultan a los servicios públicos para procesar datos personales como las direcciones de correo electrónico, para utilizarlas sólo dentro de su competencia y para cumplir sus fines promocionales y asistenciales -todo, por regla general, sin transformarla en un domicilio legalmente constituido-, dichos órganos públicos no pueden renunciar a sus competencias acordando

[135] Lo que se hace en la práctica simplemente es disponer el campo para registrar el dato, de manera opcional y alternativa, y sin discriminar a aquellos ciudadanos que no posean correo electrónico o no quieran señalarlo.

[136] Recuérdese que, en base a los artículos 20, 2° y 4° de la ley 19628, el principio legal que rige es que sólo se pueden tratar (recopilar y ceder en el caso en estudio) datos personales o nominativos como la dirección de correo electrónico, si su titular consiente expresamente y es debidamente informado del propósito del almacenamiento, o (ii) cuando una ley autorice -también expresamente- a hacerlo.

contractualmente (y ofrecer remover sería una convención o acuerdo) con los ciudadanos titulares, que ellos se abstendrán de procesar sus datos personales y removerán o eliminarán sus direcciones de correo electrónico.

¿Podría entenderse que esta autorización de tratamiento se extiende a opciones como la de que entre los servicios públicos se intercambien entre si las direcciones de correo electrónico de los ciudadanos, con la finalidad -por ejemplo- de "promocionar" una nueva modalidad de servicio público, y teniendo presente la obligación de colaborar que establece el artículo 5° de la LGBAE[137]?.

Creemos que no, porque, como consignamos a propósito de los convenios de intercambio de datos personales entre servicios públicos, una operación como "*la entrega masiva, sistematizada y nominada de direcciones de correo electrónico y la elaboración de listados de antecedentes de los ciudadanos*"[138]- no es de competencia exclusiva -al tenor del artículo 20° de la ley 19.628- de ningún servicio público. Menos aún, por cierto, podrían usarse las casillas para fines de marketing político o ponerse las direcciones de correo a disposición de los particulares[139].

El estudio sobre la regulación jurídica debe hacerse (i) evaluándose la procedencia de la entrega -o no- teniendo presente lo que establezcan normas legales generales de Derecho Público y Administrativo[140]; (ii) revisándose lo que dispongan normas especiales como la ley 19.628 sobre tratamiento de datos

[137] Tenemos en mente un fin promocional o de marketing público, que a esta fecha carece de regulaciones legales expresas, a diferencia de lo establecido para el sector comercial en el artículo 28 B de la ley 19.496).

[138] Similar situación se presentaría si lo solicitado fueran, por ejemplo, los números telefónicos de los ciudadanos.

[139] Radicalmente distinto es el caso de datos personales respecto de los cuales, por ejemplo la Tesorería General de la República o el SII, poseen competencias de Derecho Público que le atribuyen la calidad de proveedor de información sistematizada y masiva de esta naturaleza, únicamente con fines de servicio público. Recuérdese que el artículo 20 de la ley 19.628 establece que un servicio público puede tratar datos personales sin consentimiento del titular, *"respecto de las materias de su competencia",* que en este caso se refiere al deber o carga de producir y difundir listados de antecedentes sobre los ciudadanos. Estos datos son, por ejemplo: los roles de avalúo de bienes raíces; los códigos de actividad declarada por los contribuyentes; la fecha de inicio de actividades de los contribuyentes; la fecha de término de giro de los contribuyentes; y el comportamiento tributario irregular de los contribuyentes.

[140] Sería el caso del deber de colaboración general entre servicios públicos contemplado en el artículo 5° de la LGBAE. Ocurre que cuando 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 debiera apoyarse 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

personales[141]; y, (iii) considerándose lo que dispongan las normas orgánicas de un servicio público.

Se debería determinar en concreto:

(i) La naturaleza de los datos *"direcciones de correo electrónico"* solicitados y la legislación que les es aplicable. Por tratarse de datos personales le sería aplicable la ley 19.628, y al no haber existido autorización expresa para el tratamiento, para su eventual cesión a otro servicio público debiera requerirse el consentimiento previo y expreso de los titulares;

(ii) La competencia de los servicios públicos para procesar, almacenar, generar o difundir las direcciones de correo electrónico de los ciudadanos sin autorización expresa de ellos para este objeto sino sólo mediando la previa entrega voluntaria. A esta fecha no existe órgano administrativo alguno que posea competencias de Derecho Público -desde la perspectiva que sólo puede hacerse aquello que la ley establece expresamente- que le atribuyan la calidad de proveedor de información al público ni a los servicios públicos en general, o, concretamente, de administrase un listado de direcciones de correos de los ciudadanos que pueda ser consultado por terceros;

(iii) La posible responsabilidad del servicio público sobre la vigencia, exactitud e idoneidad de las direcciones de correo electrónico, ya que podría ocurrir que los ciudadanos no fuesen contactados o ubicados electrónicamente, y no sería diligente que se les diga posteriormente que se *usó "la dirección que legalmente estaba registrada en tal o cual servicio público"* para responder a sus eventuales alegaciones;

(iv) La naturaleza y finalidad del servicio público que solicita la información, para evitarse que los eventuales envíos no se perciban como correos no deseados, enviados en forma masiva y sin autorización ni menos solicitud previa, lo que a esta fecha en el sector comercial se conoce como *spam*; y,

(v) La posible o eventual existencia de una norma legal expresa que obligue a permitir el acceso a datos personales como las direcciones de correo, que es uno de los supuestos para permitir el tratamiento del artículo 4° de la ley 19.628.

3. *Los servicios públicos, que actuando dentro de su competencia exclusiva -en conformidad al artículo 20° de la ley 19.628- tratan las direcciones de correo electrónico "de los ciudadanos" para el cumplimiento de sus funciones y de sus*

[141] Debe dejarse de lado lo dispuesto por el DS 77 de Diciembre del año 2004, que se refiere funcionalmente a los requisitos y condiciones para implementar una comunicación electrónica entre servicios-ciudadanos, pero que nada dice sobre la procedencia legal de la opción de recopilar y difundir las direcciones electrónicas de los mismos.

fines promocionales y asistenciales, no incurren en conductas de "spam" ni tratan ilegalmente estos especiales datos personales.

3.1 Cabe entenderse por *"spam"* al envío indiscriminado de correos electrónicos no solicitados, "*basura"* o "*chatarra*" y generalmente con promociones comerciales, los que saturan casillas de correos electrónicos. No es necesario contar con una definición detallada o unívoca de esta práctica. Creemos que basta con tener presente un concepto que reúna algunas de las diversas características que se han consensuado y que, de concurrir -no necesariamente todas a la vez-, la transforman en una actividad nociva, perjudicial y eventualmente -de existir regulaciones prohibitivas que por ejemplo la califiquen de delito penal- ilícita.

Lo que no debe hacerse es caer en la simpleza de definírselos como *"todo correo electrónico no deseado, no solicitado o no consentido"* y de creer que así se engloban sus principales características, de partida porque un correo que se envía por ejemplo una única vez no causa perjuicio alguno al destinatario, y porque en definiciones tan simples cabría por ejemplo el caso de que un alumno de derecho o un colega abogado le enviaran un correo a otro abogado para formalizar un contacto, sin que ambos supieran que el destinatario no lo deseaba y no lo consentía, y por cierto sin haberlo solicitado el receptor.

Puede pensarse que siempre estaremos en presencia de un *spam* cuando se trate de correos electrónicos no solicitados por el receptor o destinatario; que sean enviados sin autorización previa y en forma masiva o sin discriminar acerca de la identidad del receptor *("para que llegue a la mayor cantidad posible de receptores"*); que por lo general serán remitidos anónimamente o no identificándose el emisor; y que ofrecen una opción de remoción de la lista de destinatarios que en la práctica después no se verifica, porque sólo se busca confirmar si una casilla está activa.

Se trata de un problema que en sus orígenes utiliza como materia prima -si se nos permite la expresión poco jurídica- el mayor número posible de listas, archivos, ficheros o bases de datos de direcciones de correo electrónico. Esto justifica el considerarlo dentro de los tópicos relacionados con la privacidad o intimidad desde la perspectiva de como se ve violentada de la mano de la conectividad a Internet, y nos lleva a percibir que lo realmente importante, para solucionar el problema de raíz, es evitar el tráfico de bases de datos personales con datos sobre direcciones de correo electrónico.

Las consecuencias nocivas de esta práctica son diversas, y de diferente naturaleza. Concurren perjuicios económicos para los destinatarios; se afecta la conectividad de la redes; perjudican el negocio de los ISP o proveedores de conectividad; suelen ser la consecuencia del tráfico previo y no autorizado de listas de correos electrónicos en un verdadero "mercado negro", lo que ocasiona evasión tributaria; y generalmente se utiliza el dato personal o nominativo "dirección de correo electrónico" sin autorización de su titular.

¿Los servicios públicos en Chile, adquieren listas de correos en el mercado informal o, desde la otra perspectiva, venden y comercializan las bases de datos con las direcciones de correos de los ciudadanos que recopilan en el marco de su función pública?.

Al no poseer competencia para hacerlo y al recaer sobre ellos la obligación general de secreto del artículo 7° de la ley 19.628, este proceder sería ilegal y negligente, sancionable incluso penalmente por el artículo 4° de la ley 19.223 si fuera el funcionario responsable del STDP el que revelase los datos[142].

Ya que en Chile el *spam* es legal en el sector privado, bajo ciertos respectos[143], *¿podría entenderse que esta validación alcanza a generar competencia para que un servicio público promueva abusiva, clandestina y masivamente sus servicios entre los ciudadanos?*.

La respuesta es negativa, toda vez que la validación requiere que estemos en los supuestos de la ley de derechos del consumidor, esto es, que el correo lo envie un comerciante a un consumidor o posible cliente, y que el contenido consista en la oferta comercial de un bien o de la prestación de un servicio

3.2 Los artículos 47 y ss. del Reglamento de la ley de firma electrónica N°19.799, a saber, el DS 181, crearon un Comité Interministerial sobre "*Normas para el Documento Electrónico"* con el objetivo claro y especifico de asesorar al Presidente de la República en la elaboración de *"normas técnicas"* para garantizar la compatibilidad y desarrollo del documento electrónico al interior de la Administración Pública.

En el contexto de un Sub-Comité sobre *"manejo de correo masivo no solicitado"* en los servicios públicos se debatió acerca de dos materias. Por una parte, en cuanto a la adopción de medidas técnicas que permitan filtrar la recepción en los servidores de los órganos estatales de correos masivos, no solicitados, con promociones comerciales y anónimos, denominados *"spam";* y por la otra, *sobre las condiciones para el envío de correos desde los servicios públicos, por parte de sus funcionarios y hacia los ciudadanos*[144]*.*

---

[142] Señala el artículo 4° que **...**el que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio, y que si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

[143] En efecto, la ley 19.496 establece en el artículo 28 B -y es una preciosa declaración de principios que en la práctica no se cumple- que toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario solicite la suspensión de los envíos

[144] Resultó forzado subsumir este tema en el contexto de la ley 19.799 y su Reglamento, toda vez que esta normativa se refiere en general a los documentos electrónicos que sean firmados de la

Fue una percepción empírica o fáctica errada la tenida en vista por el Comité referido, en cuanto, ambiguamente y sin señalarse casos concretos, se consideró que los servicios públicos estarían operando sin fundamento legal, fuera de su competencia, "*de manera peligrosa", "holgadamente",* sin fines de servicio público y de la mano de prácticas de recogida de datos personales ilegales o poco idóneas, procesando abusivamente datos personales -como la dirección de correo electrónico- o sensibles de los ciudadanos, desviando la finalidad de su registro, operando con inseguridad técnica y saturando las casillas de correo de los administrados.

Los servicios públicos no han realizado -ni podrían hacerlo-, prácticas en las que concurran algunas de las posibles notas características más perjudiciales del *spam* en el sector privado[145], esto es: (i) no envían correos electrónicos en forma masiva y reiterativa; (ii) al enviar un correo electrónico no lo hacen de forma anónima sino que se contiene la identidad del emisor y del receptor del mensaje; (iii) no realizan promociones comerciales o publicidad no solicitada; (iv) no actúan fuera de su competencia legal; y, (v) no operan usando direcciones de correo adquiridas ilícitamente en el mercado informal sino sólo las de sus propias bases de datos.

Para el sector público existen diversas normas legales, claras, precisas y suficientes que validan el actuar no abusivo y competente al momento de recogerse direcciones de correo electrónico y enviarse mensajes masivos de la misma naturaleza, estableciéndose en dichas normas las responsabilidades respectivas en caso de negligencia, abusos o perjuicios en contra de los administrados.

Que no se requiera autorización previa, consentimiento, expreso o implícito, se debe a que "la ley" -la ley 19.628 en sus artículos 2º, 4º y 20, un Decreto 77 del

---

misma manera, y específicamente, el Título Quinto del Reglamento, se refiere al uso de firma electrónica por los órganos de la Administración del Estado. *El tema del envío y recepción de correos electrónicos en el Estado, documentos que no son firmados electrónicamente, no cabía ser relacionado con este tema.* El hecho que en el Reglamento se contemple la existencia de un Comité para asesorar en la elaboración de "normas técnicas" para garantizar la compatibilidad y desarrollo del documento electrónico desde una perspectiva estructural, instrumental y técnica, tampoco guardaba relación con los *"spam"* recibidos ni con los eventuales correos electrónicos que en base al dato personal "*dirección de correo electrónico del ciudadano" que* envíe la Administración en consideración a cuestiones de fondo o relacionadas con su procedencia o improcedencia.

[145] Todos los reparos que pudiesen realizarse a las normas legales -en concreto al artículo 5° de la ley N°19.628- para el "Sector Privado", que a esta fecha y por la vía de las excepciones regula legalmente el tratamiento o procesamiento electrónico de los datos personales *"direcciones de correo electrónico"* permitiendo el anonimato y el tráfico de listas y el envío de correos masivos, no solicitados, anónimos y perjudiciales, no son atendibles ni aplicables para lo que ocurre en el ámbito del "Sector Público" ni para la gestión de los órganos de la Administración.

año 2004, diversos instructivos presidenciales de Gobierno Electrónico, las Leyes Orgánicas de cada servicio, normas especiales, y la Ley de Bases Generales de la Administración del Estado- así lo permiten, porque reemplazan a la voluntad, al consentimiento o a la autorización previa de los ciudadanos[146].

Jurídicamente la referencia al actuar de los servicios públicos *"dentro de su competencia"* que contiene el artículo 20° de la ley 19.628 es clara. Dicha competencia va a estar determinada por las diversas leyes que sean aplicables, y si algún ciudadano estima que el servicio público actúa careciendo de competencia al efecto, cuenta con los mecanismos legales idóneos para denunciarlo[147].

Incluso más: los servicios públicos son competentes y no pueden desviar la data nominativa que identifica a los ciudadanos que recogen para cumplir sus obligaciones legales para *"fines diversos" -por ejemplo una campaña política partidista en período de elecciones-,* porque serían responsables legal, constitucional, administrativa y civilmente en conformidad a las leyes generales, de la actuación indebida, del mal uso del dato personal dirección de correo electrónico y de los eventuales perjuicios ocasionados al administrado.

Sugerir y recomendar que los servicios públicos operen con lo que técnicamente se denomina el criterio del *"opt in"* o incurriendo en los costos de solicitar autorización previa al envío a cada uno de los ciudadanos posibles destinatarios, es un despropósito. Por ende: atendidas las facultades legales existentes y si se dan los supuestos de idoneidad que sugerimos, no compartimos una eventual propuesta -que se ha formulado- en orden a que un mensaje debiera ser enviado por los servicios públicos sólo si el receptor ha dado su consentimiento de manera previa y expresa, ni siquiera para establecer que al menos *"la primera comunicación"* exija siempre el consentimiento previo e informado del ciudadano y destinatario.

---

[146] En resumen, el artículo 2° establece que en Chile la regla general son las llamadas "fuentes públicas de información", a saber, las que no sean de acceso restringido o reservado como las cubiertas por el secreto bancario, el secreto tributario, el secreto de filiación política, el secreto sanitario o el secreto estadístico[146]; el artículo 4° consagra un enorme caudal de información que por provenir de fuentes públicas puede tratarse legalmente sin autorización de los titulares individualizados; y el artículo 20° es perentorio para establecer que un servicio público actuando dentro de su competencia no requiere autorización de los ciudadanos para el tratamiento de la información que le toque procesar en el marco de dicha competencia

[147] Los ciudadanos poseen los mecanismos legales para controlar el uso y el eventual abuso respecto de sus datos personales o nominativos. Téngase presente que el derecho de petición está consagrado en la Constitución y en la Ley de Bases de la Administración del Estado; que el artículo 12 de la ley 19.628 consagra el derecho de acceso o "habeas data"; y que cualquier particular puede presentar una denuncia ante los Tribunales o ante la Contraloría General de la República.

Desde otra perspectiva, téngase presente que el Ejecutivo y los servicios públicos no poseen facultades de Derecho Público para adoptar medidas que mermen sus competencias públicas atribuidas por ley. Por lo tanto, *si en materia de tratamiento de datos personales como las direcciones de correo electrónico se quieren establecer cargas nuevas y adicionales a las que a esta fecha han definido las leyes para los servicios públicos*, como sería el caso de acordarse la exigencia de autorización previa "expresa" de los ciudadanos para el envío de un correo electrónico, el tema, necesariamente, debe debatirse en el Parlamento[148].

Por ende, debe rechazarse por ilegal toda recomendación o propuesta regulatoria futura en cuanto a que mediante un Decreto se disponga que al agregarse en un servicio público una dirección de correo electrónico a una lista de distribución de mensajes se haga vía un procedimiento de *opt-in* o de autorización previa del ciudadano destinatario, porque, en definitiva, no cabe acá el ejercicio de la potestad reglamentaria del artículo 32 N°8 de la CPE.

3.3 Se ha publicado en Chile una *Guía Modelo de Protección de Casillas Electrónicas de los servicios públicos,* elaborada en Noviembre del año 2006 bajo el amparo de la previa dictación o por mandato del Decreto Supremo N°93 del 28 de Julio del 2006, que se refiere a la aprobación de una norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados *"recibidos"* en las casillas electrónicas de los órganos de la Administración del Estado y sus funcionarios[149].

No obstante ser su contexto el de las formas técnicas y administrativas de evitar o minimizar "*la recepción"* de correos masivos, no solicitados y con promociones comerciales en los sistemas de los servicios públicos, desde otra perspectiva muy diversa, la Guía contiene un numeral Octavo referido a las *consideraciones que deben tenerse presente en materia de "emisión" o envío de "spam" (es el término usado) desde redes gubernamentales*, de cara a la responsabilidad del funcionario público *"usuario"* y a la del "*administrador de los sistemas".*

---

[148] El artículo 60 N°14 de la CPE de 1980 señala que sólo son materias de ley las que se definan como de iniciativa exclusiva del Presidente, y el artículo 62 N°2 establece que son de iniciativa exclusiva del Presidente las leyes que determinen las funciones y atribuciones de los servicios públicos.

[149] Esta Guía realiza una sistematización acerca de la *"principal"* legislación nacional supuestamente relacionada con "*el sistema de comunicaciones vía correo electrónico*", y que ellas serían: i) la ley 19.223, sobre delitos informáticos; ii) la ley 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma; iii) el Decreto Supremo 181, que reglamenta la ley 19.799; iv) la ley 19.628, sobre protección de datos de carácter personal; v) la ley 17.336 sobre propiedad intelectual; vi) la ley 18.168, General de Telecomunicaciones; vii) la ley 19.927, *"contra la pedofilia*"; y, viii) la ley 20.009 "sobre medios de pagos". No obstante, el documento no explica la forma concreta en que estas normas influirían, directa o indirectamente, en el sistema de comunicaciones electrónicas.

En esencia, subyace la idea y la percepción en los redactores de la Guía -que rechazamos por ilegal y no ajustada a la ley 19.628- que un órgano de la Administración del Estado debería enviar un correo electrónico -lo que técnicamente implica el tratamiento de un dato personal del ciudadano- con autorización previa del receptor (la que legalmente está dada); que el correo debería contener información clara y precisa sobre la fuente de origen del mensaje (lo que siempre ocurre tratándose de servicios públicos, que no operan en forma anónima); y, que se debería ofrecer al ciudadano un mecanismo efectivo para que pueda exigir su exclusión (es el criterio del *opt-out*) de la lista usada para el envío de los mensajes electrónicos.

El *Subcomité de Gestión de Seguridad* que redactó el documento consideró que, *"consciente o inconscientemente*", las redes telemáticas de gobierno y sus usuarios se convertían en emisoras de *spam*, provocando -supuestamente, porque no realizaron levantamiento empírico serio- daños a la imagen de la red gubernamental, problemas de capacidad de respuesta en los servidores de correo institucional, desperdicio de ancho de banda nacional e internacional con flujos de correo basura y molestias a los ciudadanos receptores de los correos. Para este Subcomité, de legalidad cuestionable, resultó *"relevante"* que se tomara conciencia del problema -que en nuestra opinión es inexistente- y que se adoptaran las medidas necesarias para monitorearlo y controlarlo si se llegara a detectar algún "*brote"* de la actividad.

Entre las consideraciones sobre la posible responsabilidad de los funcionarios públicos *"usuarios"* de las cuentas de correo, y aunque simplemente se repiten varios de los contenidos del Decreto Supremo 93, interesa destacar:

(i) la referencia que la Guía hace a que ellos deben respetar la naturaleza confidencial de los datos a los que tengan acceso (*"que puedan caer en su poder"* dice el documento);

(ii) la aclaración de que el sistema de correos del servicio es una herramienta de trabajo que debe ser usada para fines laborales;

(iii) que mediante internet no debe transmitirse información reservada o confidencial;

(iv) que al usuario se le prohíbe enviar cadenas de mensajes, promociones comerciales o mensajes repetitivos; que se prohíbe hacer uso comercial de la dirección de correo *"@serviciopublico.gob.cl"* (el ejemplo es nuestro) y enviar publicidad con esa cuenta; que no se puede usar el email de la institución en foros; y,

(v) que se prohíbe difundir listados de correos electrónicos institucionales para propósitos que no sean de uso institucional.

Entre las consideraciones sobre la posible responsabilidad de los funcionarios públicos *"administradores de los sistemas de correo electrónico",* de manera genérica se señala que ellos deben velar porque las condiciones de seguridad de sus sistemas permitan minimizar las posibilidades de que ocurran emisiones de spam desde la red gubernamental, y de manera específica y esencialmente técnica, se sugiere, por ejemplo, el generar reglas para controlar y monitorear los tráficos de correos salientes, o incluso, al extremo y ya alejándose definitivamente del envío de correos masivos, el establecer políticas para controlar el uso de aplicaciones *"P2P"* que se prestan para actividades ilegales cuando se intercambian creaciones digitales originales violándose las leyes de derecho de autor.

4. Existen *restricciones legales -más precisamente reglamentarias- para el uso de las direcciones de correo electrónico "de los funcionarios públicos",* que por cierto constituyen datos personales porque contienen el nombre, el apellido y la pertenencia a un servicio público determinado de la persona. Nos referimos nuevamente al Decreto Supremo N°93 del año 2006[150].

En este contexto se contempló un artículo 9º que señala que los Órganos del Estado deberán instruir a sus funcionarios acerca del adecuado uso de las casillas institucionales que se les asignen para el cumplimiento de sus funciones.

Agrega la norma que deberá "*propenderse"* a que se usen exclusivamente para fines relacionados con las competencias propias del servicio, y que el uso de dichas casillas para comunicaciones privadas o personales quedará prohibido cuando así "*lo ordene expresamente*" la autoridad o Jefe Superior del servicio -cuestión que es redundante y del todo innecesaria-; porque *a contrario sensu*, si no se prohíbe debe entenderse que se permite. Lo que nos parece errado, es que se señala imperativamente que de existir la prohibición expresa "se autorizará" o deberá autorizarse (siempre) a que los funcionarios habiliten y accedan a casillas personales desde el terminal o equipo computacional que tengan asignado.

5. Por último y siempre en relación a las "*casillas o direcciones de correo institucionales o de los funcionarios"*, cabe revisarse lo establecido por el Decreto Supremo N°77, del 2004, del Ministerio Secretaría General de la Presidencia, que aprueba una norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre éstos y los ciudadanos, permitiendo expresamente -en su artículo 3°- que la transmisión o recepciones de comunicaciones entre órganos de la Administración del Estado o entre éstos y cualquier persona o ciudadano pueda realizarse utilizando técnicas y medios electrónicos, siempre que se cumplan determinados requisitos.

[150] La norma puede verse en la URL http://www.agendadigital.cl/files/decreto_93.pdf

El inicio del año 2005 trajo la entrada en vigencia de una norma Reglamentaria y de alcance general, sobre la eficiencia de las comunicaciones electrónicas entre los órganos de la Administración del Estado y entre éstos y los ciudadanos. Para el desarrollo del gobierno electrónico era importante instrumentalizar una vía para recoger los aportes ciudadanos, y el Decreto Supremo en comento validó el uso del correo electrónico para ejercer el derecho de petición y estableció responsabilidades para los servicios públicos que los reciban. Es un ejemplo concreto de mecanismo idóneo para la interacción *on line* obligatoria entre ciudadanos y servicios públicos.

Los tan sólo 13 artículos del Decreto N°77[151] deben ser observados con cuidado, al margen de consideraciones *"técnicas*" –que nunca son las más relevantes- y dimensionando sus proyecciones.

Con este Decreto Supremo se dio cumplimiento a lo dispuesto previamente en un Decreto Supremo 181 de 2002 del Ministerio de Economía, Fomento y Reconstrucción, que aprueba el reglamento de la ley 19.799 sobre documento electrónico, firma electrónica y la certificación de dicha firma, cuyo artículo 54 dispone la elaboración de la norma técnica que permita que las comunicaciones por medios electrónicos efectuadas entre los órganos de la Administración del Estado y de éstos con los ciudadanos operen de manera efectiva y eficiente.

Está en juego el ejercicio de una garantía fundamental y así se logró que se explicitara en los considerandos del Decreto. Si bien es cierto una ley 19.799 y su Reglamento, sobre documentos electrónicos firmados de la misma manera, dispusieron elaborar una norma técnica que hiciera *"efectivas y eficientes"* las comunicaciones electrónicas al interior del Estado y de cara a la interrelación con los ciudadanos, desde la perspectiva de éstos últimos lo que se ha hecho es instrumentalizar legal y administrativamente -de la mano de una herramienta muy común como es el correo electrónico y la red Internet- el ejercicio del derecho de petición que consagra la Carta Fundamental.

En cuanto a la estructura y contenido esencial del Decreto, llama la atención que omitió definir expresamente lo que debe entenderse por comunicaciones electrónicas, con lo cual, cabe entender que es aplicable incluso a comunicaciones telefónicas vía conexión IP o de la red Internet. Se entiende esta opción si lo que se buscó es dejar la amplitud de la interpretación del concepto *"comunicaciones electrónicas"* a los usuarios e interesados, a los entes administrativos reguladores o a los tribunales, a pesar de que puede entenderse

[151] El Decreto señala expresamente que se aprueba "*la siguiente norma técnica, que permite que las comunicaciones por medios electrónicos efectuadas entre los órganos de la Administración del Estado y entre éstos con personas naturales y jurídicas, legalmente representadas, operen de manera efectiva y eficiente, y que instrumentaliza administrativamente la verificación vía redes electrónicas del ejercicio del derecho de petición consagrado en el número 14 del artículo 19 de la Constitución Política del Estado, siempre y cuando se ejerza en términos respetuosos y convenientes".*

que todos los órganos públicos deberán asumir los costos para almacenar o registrar las comunicaciones telefónicas digitales.

Habríamos preferido –como se propuso- aclarar que por "comunicación electrónica" se entendía a todo contacto e intercambio de información realizado únicamente vía redes digitales, cerradas o abiertas, con exclusión de las comunicaciones telefónicas, que se realizaran mediante plataformas basadas en Tecnologías de Información y Comunicaciones.

Resulta de enorme importancia que en la normativa se explicitara que sus disposiciones permitirán facilitar e instrumentalizar el ejercicio vía redes electrónicas del derecho de petición que la Constitución consagra para los ciudadanos, pero lo anterior será de manera general o supletoria, *"en todos aquellos ámbitos no regulados en otras normas legales, reglamentarias o administrativas específicas".* Esto significa que el Decreto permite, por ejemplo, que todas las normas que a esta fecha regulan la interacción que sostiene el Servicio Nacional de Aduanas con los agentes de aduana y compañías navieras[152].

El *artículo 3°* sujeta la transmisión o recepción de comunicaciones entre órganos de la Administración del Estado o entre éstos y cualquier persona, a que se cumplan los siguientes requisitos: (I) asegurar su disponibilidad y acceso para uso posterior; (ii) compatibilidad de los sistemas utilizados por el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseños de registro establecidos por los órganos de la Administración del Estado; (iii) existencia de medidas de seguridad tendientes a evitar la interceptación, obtención, alteración y otras formas de acceso no autorizado a las comunicaciones electrónicas; y, (iv) *que los órganos de la Administración del Estado designen una o más direcciones electrónicas que serán consideradas aptas para la recepción de dichas comunicaciones, las que deberán encontrarse debidamente puestas a disposición o consultables por cualquier interesado.*

El artículo 4° aclara que en la medida que un servicio público interactúe con personas naturales y jurídicas, a través de un sitio Web de la red Internet, y que exista una página de inicio asociada a una dirección de Internet (URL) específica, para lograr la compatibilidad señalada en la letra b) del artículo anterior, los órganos de la Administración deberán declarar cuales son los formatos y medios compatibles con sus sistemas para efecto de enviarse correos electrónicos y/o autenticarse y acceder al sitio.

[152] Por lo dicho es que el *artículo 1°* preceptúa en su inciso segundo que *"no deberán entenderse modificadas por el presente Decreto las normas administrativas que, dictadas en el marco de competencia de servicios públicos determinados, regulen y/o establezcan condiciones, requisitos y procedimientos específicos para la comunicación electrónica con los ciudadanos que por ley deban cumplir con obligaciones tributarias, aduaneras, previsionales o de otra naturaleza".*

El artículo 5° dispone que la persona natural o jurídica que envíe una comunicación electrónica a un órgano de la Administración del Estado deberá individualizar con precisión la dirección de correo electrónico, o de otro medio autorizado por el órgano de la Administración del Estado, a la cual desea se le avise la disponibilidad de la respuesta, y que no se considerarán aquéllas que no contengan preguntas consistentes y fundadas, que digan relación con materias propias de la competencia de cada servicio público y que, en consecuencia, requieran de un pronunciamiento formal.

I. Sobre la no confidencialidad, "privacidad" e inviolabilidad de las comunicaciones sostenidas por los funcionarios públicos vía correos electrónicos corporativos o institucionales.

1. Se trata esta de una perspectiva de análisis distinta referida al dato personal "*dirección de correo o casilla electrónica"* del funcionario público.

Entendemos a este respecto que el hecho de que la dirección de correo electrónico se trate de un dato personal o nominativo que deba resguardarse y que identifica a la persona en su calidad de funcionario público que labora en un órgano determinado, *no implica que jurídicamente pueda sostenerse que son confidenciales e inviolables las comunicaciones electrónicas que los funcionarios verifiquen mediante cuentas y sistemas de propiedad del servicio público*, las que sólo les han sido facilitadas para el exclusivo desempeño de su función laboral.

En consecuencia, y esto es lo relevante, *la gestión de los funcionarios públicos materializada vía correos electrónicos es susceptible de ser conocida y fiscalizada por los ciudadanos.*

2. Se ha sostenido que a los *e-mails* o correos electrónicos se les puede aplicar siempre la garantía constitucional del artículo 19 Nº5 de la CPE, que asegura a todas las personas la inviolabilidad de la correspondencia y de toda forma de comunicación privada. Las conductas atentatorias contra esta garantía además, según nuestro Código Penal, cometidas dolosamente son constitutivas de delito y castigadas con penas privativas de libertad.

Entonces, para reivindicar la confidencialidad o reserva el argumento central es el de asimilar los *e-mails* al correo tradicional argumentando que la norma no distingue si *"la correspondencia inviolable"* o *"la comunicación privada"* se realiza específicamente de alguna forma o mediante algún soporte determinado. Consecuentemente, se reivindica a su respecto su inviolabilidad, afirmándose que cualquier forma de interferencia de un correo electrónico violaría una garantía constitucional y sería constitutiva de un ilícito penal.

Desde ya una aclaración: se trata de un debate relacionado con la *"confidencialidad"*, "secreto" o "reserva" de correos o documentos electrónicos que podrían ser considerados "comunicaciones privadas" en el contexto de la norma constitucional citada o del Derecho Penal, no de un cuestionamiento sobre la *"privacidad"* de dichos mensajes, porque ellos no son personas que puedan reivindicar en su beneficio la garantía constitucional del artículo 19Nº4 de la Constitución de Chile sino que constituyen elementos de un sistema computacional, digital, electrónico o telemático que *-per se-* carece del derecho de gozar de garantías fundamentales.

La posible inviolabilidad de una forma de comunicación como los correos electrónicos no se traduce en una vulneración de la garantía constitucional del artículo 19 Nº5, porque los *e-mails*, técnica y estructuralmente, no son una especie de aquellas comunicaciones privadas susceptibles de ser pinchadas o violadas en su confidencialidad, a que alude la Constitución Política, salvo que ellos se encripten o codifiquen[153]. Se requiere una distinción elemental de cara a la naturaleza física o técnica de lo que es un correo electrónico y, en segundo lugar, en consideración a si concurre o no el elemento "encriptación". Porque sólo de esta forma se le agrega un proceso tecnológico posterior que asegura la confidencialidad o reserva del correo electrónico.

El correo electrónico no es -de manera alguna- un instrumento similar al de un correo normal, y la diferencia no radica sólo en que cada persona posee una casilla postal de carácter electrónica denominada "casilla electrónica.

(i) El correo normal se envía cerrado, y el *e-mail* no; (ii) el correo normal se envía mediante una empresa identificada y determinada, y el correo electrónico cuando es mandado a un destinatario es difícil saber al momento del envío cuál o cuáles son las empresas proveedores de conectividad y los servidores por los que circulará; (iii) el correo normal puede ser "certificado" en cuanto a los hechos que rodearon su envío y no en cuanto a su contenido -porque ellos no se abren- ni a la verdadera identidad de quien lo envía -alguien puede suplantarme en la oficina de correos-; los correos electrónicos cuando se firman electrónicamente es porque previamente se ha "certificado" la identidad de quien lo firma o genera las claves; y, (iv) la integridad del contenido de un correo normal sólo puede violarse o alterarse abriéndose el sobre cerrado, en cambio la integridad de un correo

[153] Si un usuario quisiera agregar confidencialidad o reserva a sus correos, simplemente debe utilizar mecanismos de encriptación o codificación para hacerlo. Es la conducta equivalente a cerrar el sobre que mandamos por la oficina de correos. Sólo en la medida que un tercero distinto al emisor y al receptor de un mensaje -que son los únicos habilitados técnicamente para entender o conocer el contenido del documento codificado- rompa o vulnere la encriptación de un *e-mail* protegido técnicamente, encriptado o codificado, podría hablarse de que se ha vulnerado la garantía constitucional aludida, porque ese correo claramente constituía una correspondencia inviolable y una forma de comunicación privada, reservada o confidencial.

electrónico que se envía abierto y no firmado o encriptado puede modificarse sin necesidad de ninguna operación ilícita de pinchado.

Porque todos los correos pueden ser revisados por el administrador de una red o de un servidor sin necesidad de realizar operación alguna de naturaleza clandestina -como si ocurre en el pinchado de líneas telefónicas-, y porque enviados por Internet están en una red esencialmente "abierta", técnicamente los e-mails son verdaderas tarjetas postales que cualquiera podría tomar y leer.

¿Y acaso podría alegrase vulnerada la inviolabilidad de la correspondencia normal o documental y soportada e papel o de una forma de comunicación privada, cuando la gente del servicio de correos y el cartero toman, miran, observan y leen el contenido de una tarjeta postal soportada en cartulina?.

Es un hecho real que diversas empresas tanto extranjeras como nacionales han despedido empleados por utilizar cuentas de correo electrónico corporativas o asignadas con fines laborales y las redes internas o Intranet y la propia Internet para acceder a o distribuir pornografía o enviar correos ofensivos. Una práctica cada vez más común, por cierto, es el monitoreo o revisión de los sitios de Internet en los cuales ingresan los empleados, esto es, el control de sus hábitos de navegación. Y la problemática se proyecta en igualdad de condiciones a los servicios públicos.

Frente a la pregunta de si es legalmente admisible que un empleador o el Jefe de un servicio público controle el uso del correo electrónico de sus trabajadores o de sus funcionarios el argumento central para responder en forma negativa es el de asimilar los e-mails al correo tradicional y reivindicar a su respecto su inviolabilidad, y afirmar por ende, que cualquier forma de interferencia sería constitutiva de un ilícito penal y atentaría contra el derecho a la intimidad y de inviolabilidad de loa correspondencia del empleado.

Debe tenerse presente que la esfera de intimidad en una empresa o en un servicio público depende del empleador o del Jefe del servicio y no es una garantía absoluta del trabajador que podría, al extremo, llevar a amparar bajo un manto de reserva conductas ilícitas, por lo cual en el caso concreto de una investigación administrativa ningún funcionario podría oponerse a la revisión de sus equipos y casillas de correo electrónico alegando vulneración de su garantía de inviolabilidad de las comunicaciones privadas. Sería ilógico y carente de fundamento jurídico cuestionar la necesidad por parte del servicio de revisar el correo del empleado para poder determinar su naturaleza y la existencia de una ilicitud y decidir la sanción a aplicar.

El elemento o el criterio central debiera ser la consideración del eventual perjuicio producido a la empresa o al servicio público o la magnitud del abuso, dejándose de lado el recurso de que un trabajador o un funcionario público se escude en eventuales atentados a su privacidad o a la inviolabilidad de la

correspondencia. Dicho de otra forma, si no se ha producido un abuso o un gran perjuicio alguno por el envío de uno o más correos electrónicos particulares, no habría razón para sancionar laboralmente al trabajador o administrativamente al funcionario.

A modo de ejemplo: no es lo mismo enviar, usando los sistemas, servidores y casillas de la empresa, cinco correos a familiares que 5000 ofertas de asesoría profesional particular. Vale también un ejemplo en términos de navegación en Internet: si un funcionario público está todo un día bajando cientos de gigabytes con videos pornográficos nadie podría cuestionar el perjuicio y la configuración de una causal de incumplimiento del contrato de trabajo y/o del Estatuto Administrativo.

3. *Casos chilenos de revisión de las casillas de correos electrónicos de los funcionarios de servicios públicos. El caso "MOP".*

En el marco de una investigación judicial, y de la mano de las facultades que le son propias, una ministra de la Corte solicitó acceder a la información contenida en las casillas de correos electrónicos de varios funcionarios del Ministerio de Obras Públicas de Chile MOP. Los afectados por la investigación recurrieron de protección en contra de la Ilustrísima Ministra[154], alegando carencia de fundamentos y la vulneración de la garantía que en el artículo 19 N°5 de la Constitución asegura a todas las personas la inviolabilidad de la correspondencia y de toda forma de comunicación privada. Por cierto, cosa muy distinta es, y parece no entenderse así, la garantía del artículo 19 Nº4, que asegura a todas las personas el respeto y protección de la vida privada, de la pública (la imagen) y de la honra de las personas y sus familias. Nunca estuvo en juego "la intimidad o privacidad" de los funcionarios públicos.

En nuestra opinión no cabía alegar violación de la confidencialidad o reserva de un sistema de comunicación electrónica que es público, por tres factores copulativos: 1) en consideración a la naturaleza de bienes públicos de las casillas fiscales; 2) en atención al contenido público de la labor administrativa propia de que dan cuenta dichos correos; y, 3) atendido que todo correo electrónico que se envíe sin ser encriptado o codificado es *per se* el equivalente a una tarjeta postal y circula abierto por las redes y los servidores de correos que los administran, y cualquier administrador de un servidor de correos puede visualizarlo sin realizar ninguna operación clandestina, de espionaje o de “pinchazo”.

Como hace un tiempo ocurrió con la revisión de las casillas y servidores de correos del Ministerio de Relaciones Exteriores a propósito de la llamada *Red*

[154] Referencia del fallo: CORTE DE APELACIONES DE SANTIAGO - DE LA PUENTE DROGUETT MARIA CONSUELO Y OTROS / MINISTRA EN VISITA EXTRAORDINARIA SRA ANA GLORIA CHEVESICH RUIZ, causa Rol N° 7001/2004

Hamlet, estábamos en un caso de cuentas de correo electrónico corporativas o asignadas con fines laborales que no pueden, administrativa y legalmente, ser utilizadas para enviar correos no funcionariales en el seno de un órgano del Estado. Si se quería enviar correspondencia “privada”, cada uno de los reclamantes debió haber utilizado cuentas contratadas particularmente con algún ISP o proveedor de servicios de conectividad a Internet.

La esfera de la confidencialidad o reserva que se alegaba vulnerada no es una garantía absoluta que pueda llevar a amparar bajo un manto de reserva conductas ilícitas, por lo cual en caso de una investigación judicial ningún funcionario podría oponerse a la revisión de sus equipos y casillas de correo electrónico alegando vulneración de su garantía de inviolabilidad de las comunicaciones privadas.

Además de aceptar que pueden sancionarse por la Ley de Probidad de la Administración del Estado el uso de bienes y equipos fiscales para fines particulares, toda vez que se están mal utilizando recursos asignados para fines públicos, sería un error seguir reivindicando, jurídicamente, que la revisión de los servidores y casillas de correo -que en el marco de una investigación judicial puede detectar una conducta ilícita- configuraría una situación de atentado a la garantía de la inviolabilidad de toda forma de comunicación privada y de la correspondencia, o más ampliamente, un atentado contra la privacidad de los funcionarios cuestionados.

Hay que considerar y entender la realidad fáctica antes de aplicar principios y normas jurídicas. Como se ha dicho, los correos electrónicos enviados y recibidos desde su estación de trabajo son manejados desde otro computador llamado servidor de correos -que es el responsable de administrar los correos en las redes-, y que, en consecuencia, es el servidor de mensajes el que tiene los correos realmente en su memoria y no el computador del usuario.

No se debe olvidar que ese computador es “administrado” por los informáticos responsables del sistema, los que tienen las claves de acceso que les permiten leer, guardar, copiar o borrar los archivos según sean los procedimientos de seguridad de la organización para la cual trabajan. No se trata de manera alguna, por ende y a la luz de lo dispuesto en el artículo 19 Nº 5 de la Constitución, de una forma de *“comunicación privada”* a cuyo respecto pueda exigirse inviolabilidad por parte de un trabajador.

En cuanto al tenor específico del recurso de protección presentado en este caso, a lo informado por la Ministra recurrida y a lo resuelto por la Ilustrísima Corte de Apelaciones de Santiago, recogemos una parte y casi literalmente en los párrafos siguientes la síntesis del fallo. Efectivamente, creemos que resulta de interés conocer y consignar el razonamiento efectuado por la Corte de Apelaciones en la causa De la Puente Droguett, María Consuelo y otros con Ministra Gloria Ana Chevecich.

La sentencia de la Corte de Apelaciones de Santiago se dictó con fecha 6 de diciembre, y se originó por la interposición de un recurso de protección de funcionarios del Ministerio de Obras Públicas en contra de la ministra en visita extraordinaria Gloria Chevesich. Ella había dictado en la causa rol Nº 15.260 XS. Letra D, seguida en el Décimo Séptimo Juzgado del Crimen de Santiago una resolución de fecha 15 de septiembre de 2004, que ordenó la incautación de los correos electrónicos de todos los funcionarios de la Coordinación General de Concesiones del Ministerio de Obras Públicas, enviados y recibidos entre los años 1997 y 2003.

Los argumentos alegados por los recurrentes fueron los siguientes:

(i) La resolución judicial de la ministra Chevesich, que ordenó la incautación de los correos electrónicos de todos los funcionarios de la Coordinación General de Concesiones del Ministerio de Obras Públicas, fue calificada de ilegal porque no cumplió con los requisitos ni fue dictada para los casos previstos en los artículos 176 y 178 del Código de Procedimiento Penal, esto es: ninguno de los recurrentes tenía la calidad de procesado o inculpado en la causa; la resolución que ordenó la diligencia no fue fundada y carecía de la especificidad exigida por la norma ya que no precisaba qué correspondencia era la requerida para su investigación ni quienes eran los sujetos sobre los cuales dicha medida recaía; la resolución fue dictada de manera arbitraria y manifiestamente desproporcionada o injusta, debido a que no fue fundada o no daba cuenta por si sola de los motivos que se tuvieron en vista a la hora de dictarse, y porque mediante ella se pretendía acceder a la correspondencia electrónica de todo el personal de Concesiones, "*incluida la de carácter privado"* (...misma que en nuestra opinión no existía al tratarse de cuentas o casillas laborales y públicas y de verdaderas tarjetas postales electrónicas).

(ii) La resolución judicial constituía una amenaza y una perturbación cierta de las garantías individuales de los números 5º y 4º del artículo 19 de la Constitución Política de la República.

En relación a la garantía de la inviolabilidad de la correspondencia y de toda forma de comunicación privada, expresaron que parte del contenido de los correos electrónicos constituían *"comunicaciones de carácter privado"* (...ya hemos argumentado en contrario más arriba), cuya naturaleza no se desvirtuaba por el dominio del medio a través del cual se transmitía, y que ni la función pública que realizaban ni la propiedad pública de los servidores o equipos necesarios para su transmisión, alteraban el carácter privado del contenido de sus correspondencia o comunicaciones (...lo que en nuestra opinión es totalmente al revés)[155].

[155] Según los recurrentes, y considerando sólo lo que concretamente se consignaba o decía en los mensajes, las cintas contenían tanto correos electrónicos de carácter personal y privado de los funcionarios como los propios del trabajo, formando cada una material y físicamente una unidad

En cuanto al derecho al respeto y protección de la vida privada, que asegura el numero 4º del artículo 19, la resolución judicial que ordenaba la incautación de los correos electrónicos importaba un peligro inminente de verse expuestos a la vulneración de la intimidad (...olvidándose, por cierto, que en el ámbito material la privacidad o intimidad no es un concepto absoluto).

En definitiva, se solicito que para restablecer el imperio del derecho se modificara la resolución judicial y que ella se dictara respecto de los correos de quienes efectivamente revestían la calidad de imputados o procesados en la causa que ella investiga, precisándose la correspondencia requerida, y en subsidio, que se instruyera a la Ministra a fin que se determinaran las personas respecto de las cuales la medida se haría efectiva, individualizando, del mismo modo, los correos requeridos y tomándose los resguardos que al efecto prescriben el artículo 178 y siguientes del Código de Procedimiento Penal.

En cuanto al informe evacuado por la Ministra, él expresó que luego de su designación como Ministra en Visita Extraordinaria dispuso que por separado investigaran los hechos relacionados con la forma en que se procedió en lo relativo al llamado a licitación de obras o servicios por el Ministerio de Obras Públicas, desde 1997 en adelante, requiriendo un listado de todas ellas y precisando si existieron posibles irregularidades en los llamados a licitación, confección de bases, administración y labores cumplidas, como posibles solicitudes de dinero a las empresas a quienes se adjudicaron concesiones, como la justificación contable en cada empresa de estos pagos.

Agregó que en cumplimiento de lo ordenado por la Corte de Apelaciones decretó en el proceso diversas diligencias, y como resultado de una de éstas, la Brigada Investigadora de Delitos Económicos de la Policía de Investigaciones de Chile dio cuenta al tribunal de antecedentes relacionados con un contrato que se celebró en el curso del año 1998, entre la Coordinación General de Concesiones, por intermedio de la Dirección General de Obras Públicas, y una consultora privada, y puso a disposición del tribunal "*hojas impresas de mensajes que se enviaron tres funcionarios de la Coordinación General de Concesiones, vía correo electrónico", utilizando el equipo computacional de dicho organismo,* los que darían cuenta de una suerte de conversaciones entre dichos funcionarios relacionados con el contrato que se iba a adjudicar a la consultora privada, documentos que fueron entregadas a la policía por el autor de uno de esos mensajes[156].

---

indivisible, imposible a simple vista de identificar, lo que impedía al tribunal decretar la incautación de un metraje determinado de cintas.

[156] En el mismo parte policial se hace presente que para el esclarecimiento de los hechos materia de la investigación, era necesario contar con la información computacional que poseía la Unidad de Informática de la Coordinación General de Concesiones, de los archivos magnéticos de respaldo u

Porque durante la revisión de las cintas se procedería de manera que toda aquella que no fuera de interés para el tribunal, léase correos electrónicos de carácter privado, sería eliminada, la práctica de la diligencia constituía suficiente garantía para los funcionarios de la Coordinación General, ya que sólo el tribunal tomaría conocimiento del contenido de las cintas, tanto de los mensajes privados o confidenciales, como de aquellos que, sin tener esa calidad, fueran de interés para la investigación (...es decir, la Ministra estaba aceptando que algunos de los correos enviados mediante cuentas fiscales si serían privados o confidenciales).

¿Cuál fue la Sentencia de la 7ª Séptima Sala de la Corte de Apelaciones de Santiago?.

La Corte, antes de examinar si concurrían los requisitos de fondo que hacen procedente la acción cautelar de protección, desestimó la solicitud de extemporaneidad del recurso planteada por la parte del Fisco de Chile, y analizó luego la concurrencia de los presupuestos de fondo que lo hacían procedente; esto es, si la autoridad judicial cometió un acto ilegal o arbitrario al dictar la resolución que se impugnaba, y si a consecuencia de su actuar los recurrentes sufrieron una privación, perturbación o amenaza de sus garantías constitucionales reconocidas en los números 4 y 5 del artículo 19 de la Carta Fundamental.

Lo primero que debía dilucidarse en opinión del Tribunal de Alzada era si el acto que impugnaba adolecía de ilegalidad o arbitrariedad, lo que se traducía en determinar, a la luz de los antecedentes recogidos en el proceso criminal y de las normas constitucionales y legales, si la Ministra al dictar la resolución actuó o no dentro de la órbita de su competencia y con apego al derecho.

En la parte resolutiva el fallo la Corte de Apelaciones sostuvo que la Ministra en Visita Extraordinaria procedió en el ámbito de su competencia y de manera legal al investigar los ilícitos denunciados, y existiendo mérito suficiente dictó la resolución en la que se dispuso la incautación de los archivos magnéticos de respaldo u otro similar de los correos electrónicos, que los funcionarios de la Coordinación General de Concesiones del Ministerio de Obras Públicas, emitieron entre los años 1997 y 2003, y que no ha incurrido en ilegalidad alguna al dictar la resolución judicial que ha sido motivo del recurso de protección.

---

otro similar de los correos electrónicos de los funcionarios que se desempeñaron entre 1997 y el 2003.

La Ministra Chevesich expresó en su informe que ante las aprensiones de los funcionarios de la Coordinación General de Concesiones, y advirtiendo que el proceso para obtener de las cintas la información necesaria sería complejo y demoroso, designó perito a la Dirección de Investigaciones Científicas y Tecnológicas de la Pontificia Universidad Católica, para asesorar al tribunal en la diligencia de incautación y en el proceso que era necesario llevar a cabo para poder revisar y leer el contenido de las cintas.

La Corte consideró que la actuación de la juez no podía considerarse arbitraria, puesto que la resolución en los términos que fue dictada no obedeció a su mero capricho sino que fue producto de antecedentes reunidos en el marco de una investigación criminal, que la hacían aconsejable para los objetivos del proceso.

Y agregó -lo que es importante destacar ahora y lamentamos porque no se consideró el fondo del tema-, que no se entraba a analizar si el contenido de los correos electrónicos, medio de comunicación de reciente data, se encontraba o no para el constituyente comprendido dentro la documentación privada que resguarda nuestra Carta Fundamental, o si la circunstancia de que se utilizara por funcionarios para fines particulares dicho medio de comunicación usando equipos computacionales pertenecientes al Fisco de Chile, le pueda restar dicho carácter, en razón que ésta es una cuestión que a juicio de los sentenciadores no correspondía dilucidar en esa instancia[157].

Desde una perspectiva no jurídica, la Corte dejó constancia de que era imposible que la Jueza estuviera en condiciones de identificar y clasificar, a priori, cada uno de los documentos contenidos en ellas y estimar que en las cintas ordenadas incautar, junto con la información propia del servicio, cuál correspondería a correos electrónicos de carácter personal y privado de los funcionarios estatales.

Se resolvió que, en cuanto a las garantías fundamentales supuestamente conculcadas por la acción de la magistrado recurrida, concretamente en cuanto a la garantía del número 5º del artículo 19, que dicha actividad se realizó dentro de una investigación criminal, en ejercicio de las facultades otorgadas por la Excma. Corte Suprema y dentro de su competencia, lo cual dejó su acción dentro de la situación excepcional contemplada en la misma disposición constitucional, que señala que hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.

Y aunque en nuestra opinión no cabía referirse a ella, el fallo retoma las mismas razones señaladas en el párrafo precedente para concluir que tampoco se conculcó la garantía contemplada en el número 4º del artículo 19 de la Constitución Política de la República, por cuanto, en la forma de disponer la

[157] En este dictamen, la Corte de Apelaciones evitó pronunciarse sobre la naturaleza pública o privada de los correos electrónicos incautados, lo que era necesario para precisar el alcance de lo que la Constitución denomina *"toda forma de comunicación privada"*. Calificada de pública la correspondencia electrónica la Corte tendría que haber desestimado la acción esgrimiendo que tales documentos no se encontraban amparados por la inviolabilidad del 19 Nº15. En caso contrario la Corte debió haber analizado la orden de incautación de la magistrada Chevesich y las normas procesales que supuestamente respaldaban su decisión a la luz del texto constitucional que solo autoriza la interceptación, apertura o registro de las comunicaciones y documentos privados en los casos y formas determinados por la ley.

incautación y llevarla a cabo, la magistrado participó personalmente en dicha diligencia, adoptando para la revisión de los documentos las medidas conducentes a fin de resguardar su contenido del conocimiento de terceros, disponiendo en esa dirección su correspondiente custodia, el examen personal de su contenido, la segregación de las piezas de carácter privado o confidencial, de aquellos que sí interesan para el éxito de la investigación, ordenando, además, formar cuadernos reservados, resguardando de esta forma, de una manera cierta y efectiva, el respeto y protección de la vida privada, y a la honra de la persona y su familia, que asegura a todos los ciudadanos nuestra Carta Fundamental.

J. Sobre la comercialización y venta de los datos personales de los ciudadanos realizada por los servicios públicos.

1. En sede de la ley 19.628, es su artículo 2° letra o), cuando se define *"tratamiento"* de datos personales, el legislador autoriza a que ellos sean cedidos por el responsable de la base de datos. La ley no distingue, y por ende caben las hipótesis tanto de cesiones gratuitas como onerosas o con fines de lucro, y se ha entendido que toda cesión implica la transferencia a otro de la titularidad sobre un registro, una base o un banco de datos nominativos.

Se trata de una práctica a esta fecha realizada sólo por algunos servicios públicos. Ya mencionamos más arriba que está expresamente permitido para el SERVEL, al que se le permite la comercialización de los padrones electorales y esencialmente el número de RUT; expresamente permitido al SRC, que puede comercializar certificados (documentos que contienen datos personales) referidos al estado civil de los ciudadanos como una de sus competencias esenciales de servicio público; y, "*al parecer permitido"* al Servicio Nacional de Aduanas (no hemos tenido las normas respectivas a la vista), que comercializa datos de las empresas importadoras y exportadoras referidos a las mercancías (valores, orígenes o proveedores, características, etc.) a cuyo respecto ellas son consignatarias.

A nuestro parecer, debiera materializarse esta práctica:

(i) sólo en la medida que el órgano posea facultades normativas expresas para así hacerlo;

ii) debiera hacerse sin finalidades de mero lucro sino que siempre en el marco del cumplimiento de sus fines promocionales y asistenciales de servicio público;

(iii) debiera hacerse considerándose sólo el pago y/o el cobro de los costos en horas/funcionario y materiales en que el servicio público incurra para tratar y generar los antecedentes;

(iv) sería procedente únicamente respecto de datos personales de los administrados que no estén sujetos a una obligación legal específica de secreto o reserva o a la obligación general de secreto del artículo 7° de la ley 19.628; y,

(v) cabría teniéndose presente que no es una competencia propia de los servicios públicos el ser proveedores de datos nominativos para empresas de un mercado particular y comercial, lo que de hacerse, sólo procedería en forma excepcional.

Al margen de estas consideraciones queda el ámbito de la venta o comercialización de información estadística, desagregada, disociada e innominada, que no son datos personales.

Del mismo modo, en el ámbito de las relaciones con los ciudadanos que solicitan controlar y acceder a sus propios antecedentes o datos personales por regla general las eventuales entregas de información debieran ser gratuitas para el titular de los datos. Salvo, que ello implique asumir costos y usar recursos más allá de los previstos o presupuestados, en cuyo caso excepcionalmente podría cobrarse un valor que compense el trabajo a realizarse (horas/funcionario) y los costos directos involucrados.

2. Un anticipo, de cara al intento de armonización de la regulación jurídica del STDP con la ley 20.285.

En el ámbito de las relaciones con los ciudadanos, entendiéndose que el servicio público no posee legalmente la naturaleza de prestador de servicios de información ni de proveedor comercial de la misma, *por regla general* las eventuales entregas de información serán gratuitas o sólo fundadas en la reciprocidad del canje. No obstante, cuando ello implique asumir costos y usar recursos más allá de los previstos o presupuestados, excepcionalmente debiera determinarse un valor que compense el trabajo a realizarse (horas/funcionario) y los costos involucrados.

Este alcance guarda relación y similitud con lo que en materia de fijación de costos establecen los artículos 18° de la ley 20.285 y 20 de su Reglamento. En efecto, estas normas no aluden a la venta de datos personales, sino que, a documentación generada por un servicio público *-y se citaron durante el debate parlamentario como ejemplos al Instituto Nacional de Estadísticas y al Instituto Geográfico Militar-*, y ellas deben complementarse aplicando el principio de la gratuidad, de acuerdo al cual por regla general el acceso a la información de los órganos de la Administración es gratuito, siempre que no irroguen un gasto para el servicio público y pudiendo sólo cobrarse el soporte en que conste la información.

Señala el artículo 18° que sólo se podrá exigir el pago de los costos directos de reproducción y de los demás valores que una ley expresamente

autorice cobrar por la entrega de la información solicitada, y que la obligación del órgano requerido de entregar la información solicitada se suspende en tanto el interesado no cancele dichos costos y valores.

Agrega y detalla el Reglamento en cuanto a que la información se entregará por el medio y en la forma que el requirente haya señalado, salvo que el costo sea excesivo o signifique incurrir en un gasto no previsto y no presupuestado, y estableciendo que, en cuanto a los costos directos de reproducción, debe entenderse que ellos son todos aquellos que sean necesarios para obtener la información administrativa en el soporte que el requirente haya solicitado, sin incluir el valor hora/funcionario para realizar la reproducción.

3. *El caso del SERVEL.*

Hoy se cuestiona en Chile la gestión en materia de tratamiento de datos nominativos de las personas naturales que realiza el Servicio o el Registro Electoral, con referencias al *Big Brother* de Orwell y a una fundada acusación de tráfico de bases de datos, fruto de la desinformación y de una indebida satanización del tema. Este Órgano del Estado, invocando como fundamento diversas normas legales -antiguas y recientes-, desde hace años va más allá de la mera venta de información estadística -que no admite *per se* cuestionamiento- y comercializa el *"padrón alfabético computacional"* con datos nominativos de los electores.

Surgen las siguientes interrogantes: (i) ¿cuáles son las normas legales que el propio servicio dice legitiman su actuar?; (ii) ¿es esta una función de servicio público propia de la competencia del SERVEL?: ...se dice que *"...vender bases de datos a agentes no vinculados con el proceso de elecciones no tiene ninguna relación con la misión del Servicio Electoral, que es llevar un registro de electores confiable al servicio de elecciones limpias e informadas";* (iii) ¿estará cobrando al efecto sólo los costos directos asociados a la generación y procesamiento de la información, que una ley de Administración Financiera permite cobrar?; (iv) ¿la comercialización es una consecuencia necesaria de que su ley orgánica diga que tales registros son públicos (artículo 28) y de que lo faculte para vender bienes muebles (artículo 93)?: se dice que *"...el Servicio Electoral vende el padrón por considerarlo información pública y para que esté al alcance del sistema político, y en particular de los candidatos, bajo el supuesto de que así los electores podrán recibir la información necesaria para tomar una decisión informada"*; (v) ¿las ventas (que no son un canje vía Convenio por otros datos que puedan serle necesarios para cumplir sus fines de servicio público), son de aquellos actos administrativos que conforme a la ley 20.285 deben ser fiscalizados por el recién creado Consejo de Transparencia, de manera de asegurarse que sean probas y transparentes?; (vi) ¿los datos incluidos en el padrón que se venden, nombre, domicilio, RUN, edad, sexo y situación de discapacidad, son datos personales públicos o privados, de *"la esfera social"* o de *"la esfera privada de las personas"*?.

Consultado formalmente, el SERVEL ha señalado por correo electrónico:

"En relación a la materia consultada le informo que, en virtud de lo establecido en el artículo 25 de la Ley N° 18.556, Orgánica Constitucional sobre Sistema de Inscripciones Electorales y Servicio Electoral, los Registros en que se lleva la información que da cuenta de las inscripciones electorales son públicos. Este precepto se encuentra en armonía con lo prescrito en el artículo 8 de la Constitución Política de la República que consagra que son públicos, tanto de los actos y resoluciones de los órganos de la Administración del Estado, como también, de sus fundamentos y los procedimientos que utilicen. Lo anterior determina, conforme a los principios generales de la transparencia y publicidad, la imposibilidad de denegar las solicitudes de acceso a esta información. En ese entendido, al dar lugar a tales requerimientos, el Servicio Electoral sólo cobra el valor de los costos directos asociados a la reproducción de los documentos solicitados o sus copias, lo que, en ningún caso, constituye un principio de enriquecimiento, sino que se encuentra facultado a hacerlo, según lo dispuesto en el DL N° 2136, de 1978, en el artículo 83 de la Ley N° 18.768, que establece Normas Complementarias de Administración Financiera de Incidencia Presupuestaria y de Personal, y en artículo 18 de la Ley N° 20.285, sobre Acceso a la Información Pública. Estos valores fueron fijados mediante Resolución Exenta N° 0862/2002, la que fue modificada a través de la Resolución Exenta N° 1076/2009, siendo esta última publicada en el Diario Oficial, con fecha 01 de septiembre del año en curso".

Una perspectiva de análisis sería considerar que para la ley 19.628 desde 1999 se considera que las bases de datos del SERVEL *"son fuentes públicas de información"* -con la sola exclusión del dato sobre militancia política que es constitucionalmente reservado-, y por ende, sus funcionarios no estarían sujetos a obligación de secreto y el servicio puede *"tratar"*, ceder o transferir los datos sin autorización previa de los titulares incluso para fines diversos a los tenidos en vista al recolectarse -hacer efectivo y legalmente el derecho a voto-. Este criterio puede cambiar si se aclara y precisa lo que debe entenderse por *"fuentes públicas de información"* en el sector público, como lo hemos hecho en este Informe para sostener lo contrario.

Esta normativa, de ser interpretada en el sentido contrario al que hemos formulado en el número 7 del acápite B de esta Parte Primera, blindaría legalmente que el SERVEL opere como proveedor de información (no, como se ha caricaturizado, a la manera de un "*factor de comercio*"), y las explicaciones de esta Política Pública recogida en la Ley 19.628 -que efectivamente transformaron al órgano en "*un actor relevante del mercado de datos personales"*- deben formularlas sus redactores. Su fiscalización es una competencia asignada sólo el año 2005 al recién creado Consejo de Transparencia, en virtud del artículo 33 letra m) de la ley 20.285.

Se dice además que *"...el hecho que un organismo del Estado, sin aprobación previa de los que se inscriben, venda públicamente los datos personales, tales como nombre completo, RUN, dirección, profesión y situación de discapacidad, es sin duda una violación a la privacidad y pone a las personas incluso en riesgo por el uso malicioso que a esa información se le pueda otorgar, mucho más allá del ya molesto uso comercial",* lo que no es correcto, porque, de manera general y especial, diversas leyes ya dieron la autorización en forma previa y prescindiendo de la voluntad de los ciudadanos. Estos datos, por ende, en Chile serían parte de la esfera social o pública de las personas, y lo que debe revisarse es la idoneidad o no de estas diversas normas legales.

Por cierto; no es sólo la ley 19.628 la que permite a los servicios públicos procesar datos personales; son muchas más "*las otras leyes"* especiales a que se refiere el artículo 4° de la norma. Ergo, es errado sostener que si el SERVEL quiere construir bases de datos o generar productos y servicios en base a la información de los registros puede hacerlo sólo mediante una previa autorización expresa, clara y específica de cada uno de los ciudadanos inscritos.

Desde otra perspectiva, no puede entenderse que la obligación de publicidad de los actos, contratos, documentos, resoluciones y procedimientos de la Administración del Estado que exige el artículo 8° de la Constitución de Chile desde el año 2005 deba extenderse a los antecedentes personales, nominativos o íntimos de los ciudadanos que procesa y almacena el SERVEL en sus bases de datos, esencialmente porque la ley 20.285 que desarrolla la norma mayor de la Carta Fundamental establece -en el artículo 21 N°2- como causal expresa de reserva que la publicidad, comunicación o conocimiento de los datos personales o nominativos afecte los derechos de las personas, su seguridad y la esfera de su vida privada.

Dicho de otra forma: ...la comercialización masiva que se realiza del padrón alfabético computacional no es subsumible dentro de los requerimientos de acceso a la información del Estado a que aluden los artículos 5°, 10° y 18 de la ley 20.285. No es esta nueva normativa jurídica una suficiente ni procedente para justificar la venta de datos del SERVEL, porque de serlo, significaría además que serían ilícitas todas las ventas realizadas con anterioridad al año 2005; y cuando esta ley autoriza a cobrar por los costos inherentes a la generación de la información solicitada de acceso ello se refiere sólo a la relacionada con la gestión del Estado y no con los datos personales *"per se"* mantenidos en el registro alfabético computacional.

K. Responsabilidad y competencia de Derecho Público para utilizar datos personales como mecanismos de autenticación para el acceso a los sitios web del Estado. Sobre las claves de acceso o *password* y las llamadas direcciones IP.

1. Este acápite se relaciona directamente con lo dispuesto por el artículo 20 de la ley 19.628, en cuanto a que los servicios públicos sólo pueden procesar datos personales dentro de su competencia.

Ocurre que, aplicándose las mismas medidas o el mismo modelo de seguridad y de autenticación para la identidad de los ciudadanos que se conecten vía Internet utilizado a esta fecha con éxito por la banca, tratándose de los sitios web *"transaccionales"* de los servicios públicos -porque no se necesita autenticar la identidad para visualizar una simple página web informativa[158]- el mecanismo utilizado es el de asociar un dígito verificador que es el número de RUT (un dato personal) a una *password* que genera el ciudadano.

¿Algunos ejemplos de autenticación en base a datos personales de los ciudadanos, donde los usuarios disponen de sistemas de autenticación de un *login* y una *password* (una clave y una contraseña) para acreditarse en línea?: *"...hoy disponen de tal mecanismo el Servicio de Impuestos Internos en relación con los contribuyentes; Chilecompras.cl en relación con los usuarios del sistema de compras públicas en línea; el Servicio Nacional de Capacitación y Empleo, en relación a su conexión con organismos de capacitación; y el Ministerio de Interior, en relación con el registro central de colaboradores del Estado y las Municipalidades".*

Sobre la legalidad de Derecho Público de la implementación de un sistema de autenticación, es el Decreto Supremo N° 77 del 2004, una norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre éstos y los ciudadanos, que establece que con la finalidad de proteger la confidencialidad de la información y cuando corresponda, se podrá adoptar un mecanismo de control de acceso o autenticación a las direcciones electrónicas que contengan las respuestas de la Administración del Estado.

Otra norma es el ya analizado Decreto Supremo N°100, que aprueba una norma técnica para el desarrollo de sitios web de los órganos de la Administración del Estado, y prevé desde el año 2006 -en la letra e) del artículo 9°- la posibilidad de que las personas puedan ejercer sus derechos en cuanto titulares de datos personales en línea, empero, para que el procedimiento pueda realizarse en línea, pone al organismo de la Administración del Estado -previamente o antes de responder las consultas de los ciudadanos- la carga de verificar suficientemente la identidad del solicitante que se conecte al sitio web y utilice la dirección electrónica de contacto que en él se publique. Es decir, se le obliga al servicio a autenticarlo, y la mejor forma de hacerlo es registrándolo previamente.

En principio pues, no es cuestionable jurídicamente la implementación de mecanismos de autenticación, y técnicamente está validado a cabalidad, salvo por

[158] A modo de ejemplo, véase la URL www.jijena.com

el hecho de que, *en primer lugar,* existe la propuesta en el Gobierno de crear, sin un respaldo legal ad hoc sino de facto, un único sistema nacional de autenticación de los ciudadanos, de manera tal que sea uno sólo el servicio público que administre la base de datos personales para la autenticación de los ciudadanos.

En alguna minuta de trabajo de la Secretaría Ejecutiva de la Estrategia Digital que depende de la Subsecretaría de Economía, se ha considerado que la opción conforme a la cual cada servicio público debería disponer de sistemas de autenticación propietarios para su relación con los ciudadanos atentaba contra los principios de eficiencia, eficacia y coordinación que el legislador establece para la Administración del Estado, porque disponer de tantos identificadores como servicios públicos existan entrabaría el funcionamiento de los mismos servicios implicados y desalentaría el uso de medios electrónicos como plataforma de comunicaciones entre los ciudadanos y los distintos órganos de la Administración del Estado, socavando toda pretensión de avanzar en la construcción de Gobierno Electrónico[159].

Y *en segundo lugar*, también es cuestionable jurídicamente que se haya propuesto formalmente que los servicios públicos con menos desarrollo tecnológico puedan externalizar o traspasar a otro servicio público que asuma, bajo su responsabilidad, la gestión del sistema de autenticación propiamente tal y de la base de datos personales necesaria para implementarlo y mantenerlo.

Respecto a lo primero, nada podría cuestionarse si una ley general le asignara la competencia de ser el autenticador *on line* único -por ejemplo- al Servicio de Registro Civil.

---

[159] Jurídicamente, se argumentó en cuanto a que el actuar la Administración del Estado debe atenerse a la observancia de determinados principios, entre los cuales conviene detenerse en los de eficiencia, eficacia y coordinación; que si un determinado órgano de la Administración dispone de un mecanismo tal que su empleo por otra repartición no merma la eficacia y eficiencia en su empleo, no se observa obstáculo en permitir ello, sino que, antes al contrario, ello concreta el mandato legal; que la expresión coordinación -de la LBGAE- apunta a que el accionar de la Administración del Estado debe implicar una disposición metódica de las cosas, lo cual trasunta concertar medios, esfuerzos, etc., para una acción común; y que es una idea persistente del legislador el que la Administración del Estado haga un uso eficiente y eficaz de sus recursos, así como un empleo coordinado de éstos y del ejercicio mismo de sus funciones, a fin de evitar un dispendio de energías en la satisfacción del bien común. La minuta concluye en la necesidad de adoptarse un sistema de autenticación de usuarios en línea, común a los distintos servicios públicos, a efectos de generar condiciones proclives al incremento de iniciativas de Gobierno Electrónico eficaces, eficientes y coordinadas, tanto desde la perspectiva de los organismos públicos como de la propia ciudadanía.

En cuanto a lo segundo, que sería *-por ejemplo*[160]*- el caso de un ciudadano que quisiera entrar a la página web y al sitio transaccional de la Dirección del Trabajo* y al pretender conectarse fuera reenviado telemáticamente al sitio web y a los sistemas del Minsegpres, a espaldas o sin que el ciudadano visualizara que sus antecedentes no están siendo tratados, almacenados y confrontados en la Dirección del Trabajo sino en otro órgano del Estado. Esto es ilegal y contrario a derecho, porque el segundo -el Minsegpres- no posee las competencias de Derecho Público necesarias para asumir la responsabilidad de gestionar los sistemas de autenticación ni las bases de datos personales del segundo -la Dirección del Trabajo-; además de que por mediar un engaño al ciudadano la opción debe ser desechada de plano.

Técnica y jurídicamente, cada empresa o persona que quisiera interactuar con la Dirección del Trabajo generaría una comunicación en línea, de sistemas, que implicaría responsabilidades para el que autentica y para el que se autentica en base a datos personales como el RUT, y esas responsabilidades son las que en derecho debe velarse para que no le sean objetadas -en el ejemplo- al Minsegpres, lo que ocurriría si asumiera externalizadamente funciones para las cuales no tiene competencia legal de Derecho Público y porque deben ser funciones privativas de la Dirección del trabajo.

La función sería, conceptualmente y siempre en nuestro ejemplo, la de validar datos personales, para tratarlos al respaldar identidades y autenticaciones legales en *"la puerta electrónica"* de la Dirección del Trabajo, verificando el carné de identidad, los poderes y los documentos de las personas o empresas que entraran al sitio web (...es decir, tratamiento o gestión de datos personales).

Cualquier análisis jurídico o Informe deberá hacerse cargo de la siguiente *hipótesis*: ...encontrar fundamentos legales para blindar o justificar en derecho el que el Minsegpres (u otro servicio, por cierto) asumiera externalizadamente y con sus equipos y sistemas propios, la responsabilidad jurídica y la prestación del servicio de autenticación de los ciudadanos usuarios del sitio web de la Dirección del Trabajo, con el consiguiente trabajo de tratamiento de datos personales de los usuarios y/o ciudadanos.

En caso contrario, porque en materia de Derecho Público sólo puede hacerse aquello que está expresamente permitido y porque las competencias de Derecho Público no son ni amplias ni permisivas, lo obrado adolecería de nulidad absoluta, por violar normas constitucionales y legales que determinan la competencia legal para el actuar del Minsegpres.

[160] Se trata de un ejemplo con ciertos visos de realidad, toda vez que en su momento la Dirección del Trabajo si trató de obtener que otro servicio público le prestara el servicio de autenticación de usuarios/ciudadanos, proyecto que no sabemos si se ha materializado a la fecha de este informe.

En nuestra opinión, el mayor obstáculo jurídico es el de intentar salvar la ilegalidad que conllevaría violar lo que preceptúa el artículo 20 de la ley 19.628, a saber, que el servicio externalizado tratara datos personales cuyo procesamiento es de competencia exclusiva y privativa -en el ejemplo- de la Dirección del Trabajo. Esta normativa no permite que sea un servicio público ajeno a la relación de Derecho Público entre los ciudadanos y la Dirección del Trabajo, el que opere respaldando identidades y gestiones legales en un ámbito que no es legalmente de su competencia; o dicho coloquialmente, no habilita para que el esté sistemática y habitualmente (7x24) en "*la puerta electrónica"* de la Dirección del Trabajo.

En efecto, al decir de un Informe interno de los asesores del Grupo Estrategia Digital, *"...el solo empleo de dispositivos de autenticación de usuarios supone algún tratamiento de datos personales de los mismos, cuando menos en lo concerniente a ingresos y egresos del sistema, esto es, datos de acceso, operación que queda afecta a las disposiciones de la Ley Nº 19.628 sobre Protección de la Vida Privada. Tal ley, faculta a los organismos públicos para tal proceder, en tanto se realice en el marco de sus propias competencias y con sujeción a las disposiciones de la misma".*

Porque, efectivamente y a mayor abundamiento, *"...el tratamiento de los datos personales que pueda implicar la implementación de la iniciativa deberá atenerse a las disposiciones de la Ley 19.628, tanto en cuanto a las obligaciones a que se encuentra afecto el organismo responsable del tratamiento de datos, como en cuanto a los derechos que corresponden al titular de los datos personales concernido"* o autenticado.

No es válido tampoco aludir al principio de la colaboración entre servicios públicos a que alude la Ley de Bases Generales de la Administración del Estado. No basta -como se ha hecho en algún momento- hacer referencia sólo al artículo 3° que habla de la coordinación entre servicios públicos[161], y omitir referirse al artículo 5° que expresamente alude a que los órganos del Estado deberán cumplir sus cometidos *"coordinadamente buscando la unidad de acción"*, porque esta normativa y el principio de colaboración no justifica el incurrir en ilegalidades de Derecho Público.

Dicho de otra forma y siempre en base al ejemplo de la Dirección del Trabajo, sería contrario a derecho el que un servicio público asuma los cometidos "de la Dirección del Trabajo" al margen de sus funciones de Derecho Público,

[161] Dispone el artículo 3º que la Administración del Estado está al servicio de la persona humana; su finalidad es promover el bien común atendiendo las necesidades públicas en forma continua y permanente y fomentando el desarrollo del país a través del ejercicio de las atribuciones que le confiere la Constitución y la ley, y de la aprobación, ejecución y control de políticas, planes, programas y acciones de alcance nacional, regional y comunal.

incurriendo en los costos y asumiendo -con las responsabilidades respectivas- un verdadero outsourcing tecnológico de la gestión de otro servicio público[162].

Desde otra perspectiva, nadie discute que la Dirección del Trabajo puede automatizar sus procesos de comunicaciones electrónicas y de autenticación[163]. Es una obviedad. Puede hacerlo la Dirección del Trabajo y cualquier otro servicio público en Chile, en virtud de varias normas legales y reglamentarias, generales y particulares, tales como el artículo 3° de la ley 19.799, su reglamento o Decreto Supremo 181, la ley 19.880, la ley 19.886, el Decreto Supremo 77, los Decretos Supremos 81 y 83, el Decreto Supremo N°100, etcétera.

Poco aporta además afirmar que si hay autenticación en línea legalmente ello podría ser subsumido para el concepto de firma electrónica de la ley 19.799, el que es tan amplio que alude a *"cualquier mecanismo que permita identificar formalmente al autor de una firma,*" que puede aplicarse, aún cuando al autenticarse no exista propiamente firma[164]. Porque para la ley chilena el simple hecho de autenticarse legalmente es firma.

2. *Claves de acceso, RUT y direcciones IP: una necesaria distinción para llegar a la confidencialidad de los datos personales de conectividad a la red.*

Una variante de enorme aplicación práctica, sobre todo en caso de comisión de delitos informáticos de acceso no autorizado a un servidor de un servicio público -lo que está sancionado por el artículo 2° de la ley 19.223 y técnicamente se denomina "*hackeo"*- es la relacionada con la responsabilidad y la naturaleza tanto (i) de las claves secretas o *password* que generan los usuarios para asociarlas a su RUT e identificarse o autenticarse al acceder al sitio web,

---

[162] Por eso es, por ejemplo, que en Chile la Tesorería General de la República desarrolló su propio sistema validador *on line* de identidades al momento del pago de impuestos, aunque los contribuyentes sean los mismos que operan con el Servicio de Impuestos Internos.

[163] Como se ha dicho, *"....de acuerdo a lo sostenido sistemáticamente por la Contraloría General de la República, se encuentra permitido el uso de tecnologías de información por los organismos públicos, a efectos de apoyar la labor administrativa. Esta postura encuentra su fundamento en los principios de eficiencia y eficacia en el actuar de los organismos públicos, consagrados en la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado. Con todo, el órgano contralor sostiene que tal uso es procedente siempre que se reúnan tres condiciones, a saber: (i) que se dé cumplimiento a las disposiciones que regulen el procedimiento de que se trate y en la medida que estas normas específicas no obsten a dicha posibilidad; (ii) que el servicio que pretende hacer uso de ellas cuente con la factibilidad técnica para implementarlas; y, (iii) que se adopten las medidas de resguardo necesarias para asegurar la veracidad e inviolabilidad de la información".*

[164] Porque es correcto entender que *"...un sistema de autenticación de usuarios permite identificar a una persona en un determinado entorno, en este caso, en las acciones que despliega en un sitio web, de modo que es posible identificar siquiera formalmente al autor de un determinado documento. Desde tal perspectiva, el sistema de autenticación hace las veces de dispositivo de firma electrónica".*

como (ii) de las llamadas "direcciones IP", que son el número identificativo que un ISP o proveedor de conectividad asigna a un usuario de la red Internet para navegar en ella y que permite identificar al computador desde el cual se llama para conectarse a un servidor determinado, en este caso de un servicio público.

Téngase presente: (i) las claves secretas las generan los ciudadanos que acceden al servidor del servicio público; (ii) la responsabilidad por la "*confidencialidad"* (no "*privacidad*") de ellas por regla general será del usuario que las genera; (iii) sólo surgiría responsabilidad para el órgano público si dichas claves se obtuvieran mediante el acceso no autorizado al sistema del servicio que las almacena para luego ser confrontadas; (iv) sea cual sea el número o la dirección IP desde que se conecte un ciudadano, se trata de datos personales de conectividad que identifican al usuario y que son asignados por el ISP en el marco de una relación de confidencialidad, reserva o secreto, y que al ser registrados automáticamente por el servidor del órgano de la Administración "llamado" digitalmente, quedan cubiertos durante su "*tratamiento"* por la obligación de secreto del artículo 7° de la ley 19.628.

2.1 *Respecto a las direcciones IP.*

Ellas, asociadas al RUT de una persona, en síntesis permiten identificar al sistema desde el cual un usuario de la red Internet accede al sitio web. Constituyen en conformidad al artículo 2° de la ley 19.628 datos personales que identifican a un usuario[165], le son asignadas por su respectivo proveedor de conectividad o ISP, y para el servicio público en cuyo sistema se registran automáticamente -porque es información que el programa navegador de la red le envía al sitio web visitado o accesado[166] constituyen legalmente -de cara a su tratamiento y eventual comunicación a terceros- datos sujetos a secreto o reserva, en conformidad al artículo 7° de la ley 19.628.

Esta norma establece que los funcionarios de los servicios públicos que trabajan en el *"tratamiento"* de datos personales están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público -y los servidores de la red Internet no poseen tal calidad-, como asimismo sobre los demás datos y antecedentes relacionados con la base de datos.

---

[165] La norma citada los define como los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

[166] Técnicamente, dependiendo de la configuración que viene por defecto o de la que defina el usuario, lo que el programa navegador envía al servidor es la dirección IP del proveedor de conectividad que se le asigna al usuario que se conecta, el nombre del sistema operativo que se está utilizando, y el nombre y la versión del programa navegador. Los sitios web que reciben estos datos declaran que sólo los utilizan para fines estadísticos, pero será una cuestión de hecho el precisar caso a caso si así ocurre con los sitios de los servicios públicos.

La misma norma citada, pero en sus artículos 2° letras c) y o), aclaran que el tratamiento que debe ser para el servicio público secreto comprende la imposibilidad de verificarse una comunicación o transmisión de datos a terceros, al definir esta operación como dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

La calidad de dato de conexión o de conectividad reservado de las direcciones IP es compartida y legalmente está así normado para las empresas ISP o proveedoras de conectividad, que por regulaciones de la Ley General de Telecomunicaciones e instrucciones de la Subsecretaría de Telecomunicaciones no son accesibles al público o a cualquier persona y están sujetas a una obligación de "reserva" para dichas empresas. Estas empresas asignan un rango a cada uno de sus clientes, y sólo revelan el antecedente de la dirección de internet desde la cual alguno se conecta previa orden o resolución de un tribunal o, en concreto, del Ministerio Público.

Es el *artículo 6° del Decreto Supremo 142 del año 2005*, sobre interceptación y grabación de comunicaciones telefónicas y otras formas de telecomunicación, el que establece que los proveedores de acceso a Internet deberán mantener, *"en carácter reservado"* y a disposición del Ministerio Público o de toda otra institución que por ley esté facultada para requerirlo, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a 6 meses, de los números IP de las conexiones que realicen sus abonados.

Estas direcciones IP -por ende- no pertenecen al servicio público que es llamado o conectado en línea desde ellas, no son generadas por el órgano público ni con presupuesto público, y no son el parámetro que identifica a los ciudadanos cuando acceden autenticádamente al sitio, porque esta funcionalidad es posterior e independiente, y se entrega a las ya mencionadas claves de acceso asociadas a un RUT.

2.2 *Respecto a las claves de acceso.*

Toda página web de un servicio público debiera informar a los ciudadanos usuarios que, para la operatoria del mecanismo de autenticación que consista en la combinación del RUT con una clave, su generación y confidencialidad es de exclusiva responsabilidad del ciudadano.

Del mismo modo, si efectivamente un tercero usa su clave secreta en forma indebida y ello configura el delito de acceso no autorizado al computador del usuario del artículo 2° de la ley 19.223, es una situación de hecho a cuyo respecto el servicio público al cual posteriormente accedió quien no tenía derecho de usar la clave, no posee competencias legales para investigar, calificar ni denunciar judicialmente, porque no será un sujetos pasivo o víctima directas de delito

informático alguno, ya que no sería desde sus servidores donde se habrían obtenido en forma dolosa sus claves de acceso.

Un servicio público, en el caso anterior, o más propiamente respecto de sus sistemas de la red Internet, no incurre en responsabilidad alguna ni puede impedir eventuales accesos indebidos por parte de terceros no autorizados al efecto por un contribuyente, si es que dicho acceso se ha registrado formalmente en forma debida y mediante la clave de usuario registrada previamente por el contribuyente en la base de datos del órgano del Estado.

El órgano público además, no administra, actualiza o modifica dichas claves de acceso, y sólo está obligado a asegurar su confidencialidad en la medida que estén almacenadas en sus bases de datos, en especial por las exigencias del Decreto Supremo 83 del año 2005. Es por eso que la definición de seguridad publicada en cualquier página debiera señalar que la responsabilidad derivada de la falta de cuidado, de la indebida reserva, del mal uso o del uso por terceros autorizados o no por el usuario, ocasionándose o no perjuicios directos o indirectos o de cualquier especie, es exclusivamente del titular de dicha clave.

L. Prevenciones sobre la legalidad del proyecto Plataforma Integrada de Servicios Electrónicos del Estado (PISEE).

1. En el ámbito del denominado Gobierno Electrónico, en Chile se está desarrollando una plataforma integrada de servicios ciudadanos o un sistema nacional de información ciudadana. Y el mismo gobierno lo ha calificado como un *"proyecto prioritario"*[167], lo que hace necesaria su revisión legal.

Si el Estado debe permitir el acceso a los datos y documentos que le afectan o le interesan a los ciudadanos o administrados, razones de *"economía de gestión"* abonan que se le pueda ofrecer una opción que les permita en un sólo ámbito conectarse con todos los servicios públicos a la vez, para evitar acudir a cada servicio por separado. Previo a este objetivo, el primer paso es integrar a los diversos servicios públicos, lo que no resulta fácil por el diverso grado de desarrollo tecnológico de cada uno.

Se ha dicho que la interoperabilidad existe cuando mediante sistemas heterogéneos pueden intercambiarse procesos o datos, permitiéndose significativas ganancias en términos de *eficacia* y de *eficiencia, y que en* el

[167] Véase lo afirmado en las URL http://www.edicionesespeciales.elmercurio.com/destacadas/detalle/index.asp?idnoticia=20090814152008&idcuerpo= y http://www.edicionesespeciales.elmercurio.com/destacadas/detalle/index.asp?idnoticia=20090814151771&idcuerpo=

contexto del avance del gobierno electrónico, la interoperabilidad es hoy en día un objetivo deseado y buscado en todas las Administraciones Publicas. Con una plataforma integrada de servicios ya no se hablará sólo de la noción de *'conectividad'.* El elemento clave se denomina *'Interoperatividad'* o *"Interoperabilidad*", es decir, asegurar que al asumirse en la Administración del Estado la satisfacción de las necesidades de los ciudadanos, los sistemas, los procedimientos y la cultura se administren maximizándose las oportunidades para el intercambio y la reutilización de la información.

A modo de ejemplo concreto, citamos: *"….una persona que va al Instituto de Previsión Social (IPS) a solicitar una Pensión Básica Solidaria, tendría que al menos llevar su certificado de nacimiento y el de cada hijo, más un certificado de la AFP y acreditar su residencia. Gracias a la plataforma, sólo tiene que llevar su cédula de identidad y solicitar el beneficio; ….lo importante es que a las personas no se les pida recopilar información que ya está en poder del Estado, por ejemplo, certificados de nacimiento, giro de empresas, estado civil o hijos".*

Y como la generalidad de la información intercambiada a través de la plataforma es calificable como datos personales o nominativos, se justifica y se requiere levantar las observaciones existentes a esta fecha en cuanto a su falta de respaldo jurídica, las que de no ser subsanadas a la brevedad aconsejan se suspenda su operatoria.

2. Para plantear el reparo jurídico, repetimos lo anticipado a propósito del acápite sobre los convenios de intercambio de información nominativa entre servicios públicos.

Dijimos que legalmente la verificación de los convenios bilaterales de intercambio de información no merece reparo alguno, y que no se discutía la validez de una práctica que incluso desde hace años había sido validada por la Contraloría General de la República.

Afirmamos que los antecedentes relevados por la consultoría encargada por el Grupo de la Estrategia Digital de la Subsecretaría de Economía, enmarcados erradamente bajo el rótulo de *"puesta en marcha de la ley de procedimiento administrativo"* -con la cual no guardan relación jurídica-, no hicieron sino mostrar en forma sistemática los argumentos que los propios servicios públicos ya habían validado y levantado mucho antes, al momento de optar por celebrar entre ellos convenios bilaterales de intercambio de información. Por cierto, estos convenios pueden operar al margen o con prescindencia del uso de una pasarela que intermedie entre ellos.

En *cuanto a la referencia a la ley 19.880 que señalamos como no relacionada jurídicamente con el proyecto y por ende con la consultoría,* conforme a sus disposiciones no existen dudas sobre la posibilidad de operarse en forma electrónica en un ámbito específico, porque en los artículos 18 y 19 se alude

expresamente a la posibilidad de realizar procedimientos administrativos y mantener los expedientes con los actos administrativos en soporte electrónico o digital autenticado. Pero lo que carecía y carece de fundamento era invocar esta ley 19.880 como fundamento del mero intercambio de datos que caracteriza a la plataforma, *toda vez que en la PISEE no se realizan actos administrativos*[168]*, por su intermedio no se verifican procedimientos administrativos* [169]*, y en ella no se almacenan expedientes electrónicos con lo actuado procedimentalmente.*

Lo que debía y debe observarse jurídicamente no son los intercambios de datos con fines de servicio público entre los órganos de la Administración que a esta fecha se realizan mediante la pasarela o el canal llamado *"PISEE",* sino que lo reparado son las gestiones de Derecho Público sin respaldo normativo de la plataforma misma y las competencias y responsabilidades no establecidas en Derecho Público de los funcionarios y de las empresas externas que la administran. Dicho de otra forma: está operando en Chile una plataforma electrónica como la de www.chilecompras.cl que facilita el intercambio de datos personales entre servicios públicos, pero sin una ley 19.886 ni otra norma legal que lo permita legalmente, sin que se cumpla el Decreto 83 en materia de seguridad de sistemas, y sin que los que gestionan reconozcan ser objeto de las exigencias de Derecho Público que le caben a los funcionarios públicos.

3. Es errada la cita de normas legales realizada por los asesores del Ministerio de Economía al intentar validar la gestión de esta instancia. Aluden a la ley 19.880 sobre procedimientos administrativos; a la ley 19.799 sobre firmas y documentos electrónicos, y a la ley 19.628 sobre protección de datos personales.

No aplica la ley 19.880 porque la PISEE no realiza procedimientos administrativos registrados en expedientes electrónicos, que es lo que validan los artículos 18 y 19 de la ley; no aplica la ley 19.799, porque no se usan sistemas criptográficos de "*PKI*"[170] para la firma electrónica de documentos de la misma naturaleza; y no aplica la ley 19.628 en su artículos 4° y 20°, porque no existe servicio público alguno al cual se le haya asignado por ley la competencia exclusiva de Derecho Público para gestionar la plataforma y que califique como responsable de los sistemas mediante los cuales se transmiten telemáticamente datos personales.

Los mismos asesores olvidaron intentar buscar fundamento en un Decreto Supremo N°81 del año 2004, que aprobó una norma técnica para lograr que los

[168] Legalmente, los actos son las decisiones escritas que adopta la Administración , decisiones que son formales y que contienen declaraciones de voluntad realizadas en el ejercicio de una potestad pública.

[169] Legalmente, los procedimientos son una sucesión de actos trámite vinculados entre sí, emanados de la Administración o de particulares interesados, que tiene por finalidad producir un acto administrativo terminal.

[170] Es la sigla en inglés que alude al uso de claves y firmas digitales en un Infraestructura de Llaves Públicas y Privadas o de criptografía asimétrica.

documentos electrónicos del Estado sean interoperables en base a un mismo formato o esquemas de estructura; de haberlo hecho, tampoco habría sido una opción idónea porque acá lo regulado sólo es *"el contenido documental"* electrónico y no *"el canal electrónico"* para intercambiarse dichos documentos.

Lo que esta iniciativa de gestión y tratamiento electrónico de datos personales requiere, para no ser ilegal, es una norma como la ley 19.886 y su Reglamento, que validaron el sistema electrónico de *www.chilecompras.cl*.

4. El único soporte documental de validez en que descansa es un *Convenio Marco de diversos servicios públicos para participar en un plan piloto de implementación*, documento jurídico que por su naturaleza no es fuente de Derecho Público.

Sin entrar a su análisis detallado, cabe mencionar que se concibe a la Plataforma como un medio de traspaso de información, como un conector único y transparente para los servicios públicos, que asegura que la información se transmita encriptada, que permite que la información sobre los ciudadanos que poseen los servicios públicos esté disponible en otros órganos de la Administración, y que redirige la comunicación entre el servicio que se conecta o se sube a ella aportando o requiriendo datos, con el servicio a su vez solicitante o requerido -respectivamente- de datos personales.

Lo anteriormente referido en forma sumaria implica la realización de actividades de gestión y prestación de servicios públicos referidos al tratamiento de datos personales, que será de competencia exclusiva de esta plataforma en conformidad al artículo 20° de la ley 19.628, y que no se condice con otras afirmaciones del mismo Convenio tendientes a eximir de responsabilidad por la gestión, al aclarar que la PISEE no es una persona jurídica de Derecho Público, cuando, para operar responsablemente, debe serlo, bajo subordinación expresa de algún Ministerio. Más aún: no existe fundamento legal de Derecho Público para que, así como la plataforma de www.chilecompras.cl dependa jerárquicamente del Ministerio de Hacienda, la PISEE a esta fecha dependa de la Subsecretaría de Economía.

5. Los desarrolladores de la PISEE en la Subsecretaría de Economía declaran por la prensa haber contratado servicios legales para "*solucionar"* los aspectos legales de la PISEE. En Internet puede consultarse un resumen ejecutivo que se califica como la consultoría que entrega el respaldo legal para el funcionamiento del proyecto PISEE[171].

[171] Véase, en la URL http://www.estrategiadigital.gob.cl/files/Guia_Metodologica_PMG_Gobierno_Electronico_2009.pdf, lss páginas 97 y ss.

Lo único que a esta fecha se ha realizado es la validación de la posibilidad de que bilateralmente los servicios públicos del plan piloto puedan intercambiar datos personales entre si, pero estos estudios, de manera alguna y como expusimos en el acápite E de este Informe, validan la gestión de la plataforma y son un aporte novedoso. Tampoco era necesaria una segunda consultoría ya contratada, para concluir en que la única opción posible para validar la gestión de la PISEE es la de promulgarse una ley específica que regule la interoperabilidad proyectada en y para esta plataforma.

6. Otro aspecto reparable desde el punto de vista jurídico y de las responsabilidades, es que *la PISEE no cumple con las normas de seguridad del Decreto 83.* En consecuencia, (i) no existe un funcionario público responsable de la transferencia telemática de datos personales que por su intermedio se realiza; (ii) por definición conceptual la plataforma se considera una pasarela que no se responsabiliza por la intermediación; y, (iii) la gestión se ha externalizado en dos empresas tecnológicas particulares, a las cuales no se les fiscaliza y, hasta donde sabemos, salvo error u omisión, no se les ha obligado a suscribir contratos de confidencialidad y/o reserva ni de imposibilidad de cesión a terceros de cara al procesamiento de los datos personales de los ciudadanos.

7. En términos de los principios y el articulado de la ley 19.628, el proyecto PISEE (porque sólo eso es) está vulnerando el llamado *"principio de cesión"* o para nosotros de la transferencia telemática que realicen los servicios públicos.

En síntesis, si bien de acuerdo a este principio los datos personales que existan en una base pueden darse a conocer, y si bien se define comunicación o transmisión de datos personales como el dar a conocer de cualquier forma los datos nominativos a personas distintas del titular, sean determinadas o indeterminadas, se exige que el o los responsables del registro o banco de datos personales de los servicios públicos que participan en la plataforma cautelen los derechos de los titulares y que la transmisión guarde relación con las tareas y finalidades de los organismos participantes, como además, que se fiscalice que el servicio público receptor sólo pueda utilizar los datos personales para los fines que motivaron la transmisión.

Estas funciones, obligatorias en virtud de la ley 19.628, no son desarrolladas por la Subsecretaría de Economía, porque no posee las competencias de Derecho Público al efecto y porque la Plataforma se define "acomodaticiamente" -lo que es una negligencia administrativa desde el punto de vista de la seguridad de sistemas- como una mera instancia de intermediación.

PARTE SEGUNDA

REGULACION DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES (STDP) DE LOS SERVICIOS PÚBLICOS Y UN INTENTO DE ARMONIZACION CON LA LEY 20.285.

A. Normas constitucionales, políticas legislativas y conflictos jurídicos diversos. Distinciones esenciales acerca del contexto de las leyes 19.628 y 20.285.

1. En *Agosto del año 2008* se promulgó en Chile la ley 20.285 sobre transparencia de la función pública y acceso a la información de los órganos de la Administración del Estado[172], la que, junto con crear un nuevo órgano llamado *"Consejo para la Transparencia",* fue el resultado de una previa reforma constitucional. En *Abril del 2009* se dictó su Reglamento complementario, el Decreto Supremo N°13, sobre acceso a la información pública.

La modificación a la Constitución Política de 1980 el año 2005[173] contempló la incorporación de un nuevo artículo 8°[174], en cuya virtud y dentro del Capítulo acerca 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" (i) los actos y las resoluciones de los órganos del Estado, (ii) sus fundamentos y (iii) 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).

---

[172] Véase la URL 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/

[173] La modificación se hizo en la misma época en que, por su parte, la Contraloría General de la República ya había consignado la existencia de app. 100 resoluciones que establecían secreto o reserva de actos administrativos.

[174] 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 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"*[175], consagrado previamente -en 1999- en la Ley General de Bases de la Administración del Estado[176]. Y vino a aclarar que sólo el Parlamento y no los propios entes u órganos públicos -como ocurría en el pasado- será el llamado a establecer "*excepciones a la publicidad"* -es decir hipótesis de reserva o secreto- cuando ella afecte (i) *el cumplimiento de las funciones públicas, (ii) los derechos de las personas, (iii) la seguridad de la nación o (iv) el interés nacional.*

Dentro de la causal *"los derechos de las personas"* caben los reconocidos por el artículo 19 N°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 más no exclusivamente- electrónico, informático o telemático.

Por eso es dable sostener desde ya, sin entrar aún al análisis del articulado de la ley 20.285 -en general- y de su artículo 21 N°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 lo que se refiere como un *"...abrir los espacios públicos al escrutinio ciudadano";* o, como consigna SOTO, si *"la letra y el espíritu de la ley están construidos 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.

2. Desde la perspectiva de las garantías constitucionales en juego, cabe visualizar la necesidad de armonizar tres de ellas: la del 19 N°4, la del 19 N°12 y la del artículo 8°. Recuérdese lo afirmado al inicio de la Parte Primera de este Informe, cuando aludimos a la necesidad de lograr un equilibrio y establecer límites entre el derecho a la intimidad que consagra el artículo 19 N°4 de la

[175] Lo de *"piedra angular"* sería incluso validado por un fallo del Tribunal Constitucional, que ratificaría luego la existencia en Chile de *"un derecho constitucional de acceso a la información pública".*

[176] 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.

Constitución y los derechos de acceso a la información consagrados en los artículos 19 N°12 y 8° de la Constitución de 1980.

Ergo, la interrogante a dilucidar o la hipótesis de trabajo y estudio puede ser 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 -lo reiteramos- 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.

3. Hemos visto además que en Chile es al artículo 12° de la ley 19.628 el que consagra el llamado *Derecho de Acceso, Habeas Data o Habeas Scriptum,* un derecho -en nuestro país- 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 N°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 de cumplimiento al principio de probidad del artículo 8° de la Constitución.

4. *"Acceso para la transparencia" de la información administrativa versus "acceso para la autodeterminación" de la información nominativa.*

La distinción anterior 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 -*"tratados"* dice la ley 19.628- 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.

5. Citados a exponer 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[177].

A saber: que el derecho de acceso que todos los ciudadanos poseen reconocido constitucional y legalmente para conocer los actos, contratos y documentos de los órganos de la Administración del Estado (y que es el *expertice* principal del Consejo de 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.

[177] El contenido de la exposición puede verse en la URL http://www.derecho.ucv.cl/jijenacam.pdf

Dicho de otra forma: ...porque asegurar la *"transparencia activa"* que exige la ley 20.285 en sede de protección de datos personales no existe; al contrario, acá, para garantizar el respeto del artículo 19 N°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 19 N°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*[178], porque este 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, propone:

> *"Artículo único: Modificase el artículo 19 N° 4 de la Constitución Política de la República, 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."*

B. Contenidos esenciales de la ley 20.285 y su Reglamento.

1. La norma legal consta de siete Títulos. El Primero contiene disposiciones generales; el Segundo, alude a la publicidad de la información de los órganos de la Administración del Estado; el Tercero a la denominada transparencia activa; el Título Cuarto, al derecho de acceso a la información de los órganos de la Administración del Estado o a la transparencia pasiva; el Título Quinto, al Consejo

[178] Véase la URL http://www.habeasdataorg.cl/2008/06/05/%c2%bfhacia-la-constitucionalizacion-del-habeas-data-en-chile/

"para la Transparencia"; el Sexto establece infracciones y sanciones; y el Séptimo, contiene diversas disposiciones transitorias.

La síntesis de sus contenidos está dada en el artículo 1°, según el cual la ley regula (i) *el principio de transparencia de la función pública,* (ii) *el derecho de acceso a la información de los órganos de la Administración del Estado*, (iii) *los procedimientos para el ejercicio del derecho y para su amparo,* y (iv) *las excepciones a la publicidad de la información o las causales de reserva o secreto.*

Como ya anticipamos, se le ha denominado (en el número 4 del artículo 1°), por sus contenidos, la "*Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado* -en adelante ley de acceso y transparencia-, 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, como ya vimos y a pesar de confusiones terminológicas detectadas recientemente en los Tribunales-, y (iii) *la perspectiva orgánica o la creación del Consejo de Transparencia*.

2. *El Principio de la Transparencia de la función pública.*

Está fundamentado y formulado en los artículos 3° y 4°. Según el primero la función pública *"se ejerce con transparencia"*, de modo que permita y promueva el conocimiento *de los procedimientos*, *de los contenidos* y *de las decisiones* que se adopten en ejercicio de ella. Según el segundo, todas *"las autoridades"* -con prescindencia de la denominación con que las designen legalmente-, y todos *"los funcionarios de la Administración del Estado"*, deberán dar estricto cumplimiento al principio de transparencia de la función pública.

¿En qué consiste?: según el inciso segundo del artículo 4°, *"...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 al efecto establezca la ley".*

3. *Las definiciones conceptuales del artículo 5°.*

Uno de los sólo dos artículos que componen el ***Título II*** de la ley, sobre la *Publicidad de la Información de los Órganos de la Administración del Estado*, es clave para luego entender el alcance de la información que en definitiva debe concluirse acerca de su necesidad -por un mandato legal obligatorio- de publicarse y transparentarse. Desde ya, digamos que se volverá sobre la idea de que ese alcance ni subsume ni comprende a los datos personales o nominativos, y que de

entenderse lo contrario, se estarían violando normas constitucionales y legales expresas.

A partir de citar el principio de transparencia de la función pública, dispone perentoriamente la norma que (i) *los actos y resoluciones de los órganos de la Administración del Estado*, (ii) *sus fundamentos*, (iii) *los documentos que les sirvan de sustento o complemento directo y esencial*, y (iv) *los procedimientos que se utilicen para su dictación*, *"son públicos"*, salvo las excepciones que establece esta ley en el artículo 21 y las previstas en otras leyes de quórum calificado. Previamente, el artículo 4° anterior da elementos claros para entender qué se está exigiendo, y señala que el principio de la transparencia consiste en respetar y cautelar la publicidad de *"los actos"*, de *"las resoluciones"*, de *"los procedimientos"* y de los *"documentos"* de la Administración, incluyendo *"los fundamentos"* de todos.

Se agrega en el inciso segundo el artículo 5°, que *"es pública"* la información elaborada con presupuesto público *"...y toda otra información que obre en poder de los órganos de la Administración"*, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, a menos que esté sujeta a las excepciones señaladas[179].

Estimamos que esta referencia a "*toda otra información"* debe entenderse en el sentido del inciso primero, es decir, que se trate de antecedentes que den cuenta de la gestión de los servicios públicos y no de datos personales. Si la ley 20.285 ha demostrado un gran celo y cuidado de los datos personales en los artículos 7° letra e), 21 N°2 y 5° y 33 letra m), de haberse querido incluir en esta enumeración genérica a los antecedentes nominativos de los ciudadanos se habría hecho expresamente. Por cierto, el punto de este posible alcance del inciso 2° del artículo 5° nunca fue debatido durante la tramitación parlamentaria de la ley, y por ende debe ser analizado con extrema rigurosidad.

Volveremos en extenso sobre estas expresiones, para descartar subsumir en ellas a los datos personales o nominativos de los ciudadanos y/o de los propios funcionarios públicos.

4. *Las hipótesis de "transparencia activa" y las de "transparencia pasiva".*

Se ha conceptualizado a la ***"Transparencia Activa"*** del artículo 7° (ya en el ***Título III***) de la ley 20.285 como un deber positivo que recae sobre los órganos de la Administración, para otorgar regularmente o en forma permanente, actualizada

[179] La Moción Parlamentaria que originó la ley aludía al derecho al libre acceso a las fuentes públicas de información, entendido como la posibilidad real de la ciudadanía para tomar conocimiento de los actos de la Administración y de la documentación que sustenta tales actos.

y sistematizada publicidad *on line* -mediante sus sitios web de la red Internet- a un conjunto de información administrativa considerada por la ley 20.285 como de mayor relevancia, ya que además de *"respetarse y garantizarse"* el derecho fundamental del acceso a la información y de transparencia él también debe *"promoverse*".

Desde otra perspectiva, ya no sólo de la de una carga legal para los servicios públicos sino la de la consagración de un derecho específico para los ciudadanos, se considera que la ***"Transparencia Pasiva"*** es el deber que recae sobre los servicios públicos para entregar la información que posean o que generen fruto de sus funciones y actividades, cuando ello les sea solicitado por los administrados en conformidad al procedimiento contemplado en los artículos 12° y ss. de la ley de transparencia y acceso a la información[180].

Salvo, por cierto, que concurra alguna de las causales de secreto o reserva que -en conformidad al artículo 21- habilitan para denegar parcial o totalmente el acceso a la información. Dentro de estas causales, veremos en particular la de los números 2°[181] y 5°[182], que se relacionan con los derechos personales de los administrados que eventualmente puedan verse afectados.

5. Es en el ***Título IV*** donde se regula el *"Derecho de Acceso a la Información de los Órganos de la Administración del Estado"*, y el artículo 10°, al inicio, establece como principio fundamental 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 la propia ley 20.285.

Agrega -como ya vimos- que el acceso a la información comprende el derecho de acceder (i) *"a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos",* así como -en segundo lugar- (ii) *"a toda información elaborada con presupuesto público",* cualquiera sea el formato o soporte en que se contenga y salvo las excepciones legales.

Y lo establecido en el artículo 10° es concordante o se funda en la letra b) del artículo 11, que consagra el *"Principio de la libertad de información"*, de

---

[180] Con esta norma se inicia la regulación un procedimiento administrativo especial de acceso a la información. Ante la negativa, los artículos 24 y ss contemplan el reclamo de amparo ante el Consejo de Transparencia.

[181] Alude a *cuando la 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.*

[182] Se refiere a 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 8º de la Constitución Política, esto es, 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*".

acuerdo al cual por regla general toda persona goza del derecho a *"acceder a la información que obre en poder de los órganos de la Administración del Estado".*

C. Hipótesis de trabajo y/o planteamiento general acerca de la armonización jurídica. 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.

1. 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 CPE 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 N°4 de la CPE y por la ley 19.628 de 1999.

Porque el derecho de acceso que todos los ciudadanos poseen reconocido constitucional 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 cuáles se hace necesario reflexionar y, en la medida de lo posible, consensuar un criterio, de cara al necesario equilibrio o conciliación, tales como:

(i) ...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;

(ii) ...las leyes de acceso a la información necesariamente deben ser compatibles con las de privacidad y datos personales; y,

(iii)...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 referidos 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 cuál sea la especial naturaleza del dato personal pedido de acceso.

2. 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[183].

La misma idea o la misma formulación está dada a nivel del principios 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 en sede de la ley 20.285 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, teniendo como fundamento o por este sólo hecho de tratarse de datos personales excluidos de las causales de solicitud, y antes de entrar al análisis de fondo en cuanto a la procedencia de la causal de reserva del artículo 21 N°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) se concluye que el Constituyente el legislador de la ley 20.285 fueron sensibles -desde el punto de vista de la Política Pública regulada- 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 para comprender o subsumir dentro de la información que debe transparentarse, entregarse sin motivo o causa o publicarse a los datos 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"*.

3. Es clave pues, lo reiteramos, el 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 la normativa sobre derecho de acceso -o no- por sobre la confidencialidad y restricciones que establece la ley 19.628 para proteger a los titulares de los datos personales procesados computacionalmente

[183] 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.

-incluso con una carga legal expresa de secreto en su artículo 7°-, sean dichos datos de los ciudadanos, sean de los propios funcionarios públicos[184].

4. 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 N°2, el 21 N°5, el 33 letra m) de la ley 20.285, el artículo 8° de la Constitución, el artículo 19 N°4 de la Carta Fundamental y la ley 19.628, normas 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 de 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°[185], 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 -por regla general- respecto de los datos personales o nominativos de los administrados que sean tratados por los servicios públicos[186], porque ellos, también 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.

5. Por todo lo dicho *-en el acápite de la letra A más arriba y en este acápite C-*, 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

[184] Téngase presente que, en relación a los funcionarios públicos, en sede de 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 ya ha resuelto entregar sus calificaciones.

[185] 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 al efecto establezca la ley*.

[186] 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 (v.gr. Registro Civil, TGR, Aduana, SII, etcétera).

intimidad- …existiría jurídicamente *"coincidencia eventual"* con las causales de acceso del artículo 10° de la ley 20.285[187]-[188]. 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 sede del Instituto de la Protección de Datos Personales 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 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 donde coincidir *"jurídicamente"*, y esa atribuida *"generalidad"* no puede -con fundamento jurídico claro, apoyándose en al 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 sede de la ley de acceso y transparencia.

También resulta cuestionable, jurídicamente hablando, sostener -como se hace en la misma propuesta en comento- que lo que encarga el Ordenamiento Jurídico -*es decir 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 -clasificando- 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",* con miras al control social del accionar público[189].

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

---

[187] Véase la propuesta en la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

[188] 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".*

[189] Cuándo una información sería de naturaleza *"pública"* y cuando *"privada"* es algo que los abogados que formulan la propuesta no aclaran en forma debida y que se hace necesario.

personales[190], 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.* Los cambios, para el futuro, en este sentido, son los que contiene el Boletín 6120 tantas veces mencionado.

La concreta posibilidad legal 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 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 (v.gr. 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 muy especial 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

[190] 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.

selección[191]. En este particular y excepcional caso[192], al solicitante y recurrente de amparo no podría aplicársele la causal de reserva o secreto del artículo 21 N°2 porque precisamente se trataba de sus antecedentes, y el Consejo determinó la procedencia de la entrega de la información[193].

¿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 N°2[194] y denegado el acceso a la información?.

6. 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 -cuestión analizada en la *Parte Primera* de este Informe-, 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°.

7. Todo lo anterior debe ser considerado antes y en paralelo o durante el cumplimiento de la obligación que recae sobre el Consejo de 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"*[195], esto es, en esencia, el realizar un balance de la mano del 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

---

[191] Véase la Decisión de Amparo N°A29-09 en la URL 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

[192] Caso en el cual, además, téngase muy presente que 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.

[193] Haciendo aplicación de la normativa relativa a la protección de datos, el Consejo determinó que es claro el artículo 2° ñ) de la Ley N°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.

[194] 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.

[195] Véase la URL 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.

retenerla; o dicho de otra forma, se trata de *"determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría ocasionarse al ser ella revelada".*

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 una persona natural como a una jurídica y aún cuando la ley 19.628 no ampara a las fictas sino sólo a las físicas[196], lo que obliga -al órgano requerido primero y sobre todo al Consejo de Transparencia después- a decidir si prevalece la protección de la esfera privada -la causal del artículo 21 N°2 en concreto- o el interés público en dar a conocer la información solicitada[197].

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[198], o si derechamente se piden tales datos en forma directa (…v.gr. 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[199], los correos electrónicos de los ciudadanos, la

---

[196] Esto, lo sostenemos porque la causal del artículo 21 N°2 no debería entenderse restringida sólo a la esfera privada de las personas naturales.

[197] Y por cierto, como veremos dos acápites más abajo, la misma herramienta deberá usarse si efectuada la evaluación se percibe que existen derechos de terceros que puedan verse afectados, porque, como se ha consignado, *"...la Ley de Transparencia establece la obligación del órgano requerido de notificar al tercero, el que puede oponerse a la entrega de la información en forma escrita y con expresión de causa, y la posibilidad de invocar la causal de reserva del numeral 2 del artículo 21 de la Ley N°20.285. Luego, si el solicitante no estuviere de acuerdo, deducirá el reclamo correspondiente, y será, en definitiva, el Consejo para la Transparencia quien tendrá que decidir si prima el interés público en conocer la información o el interés personal que implicaría denegarla".*

[198] 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 N°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.

[199] Respecto a los datos sobre bienes raíces debe resguardarse la confidencialidad: 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.

nómina de enfermos 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 el Instituto de 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 N°2 de la ley 20.285.

D. 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.

1. 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°[200], deberán mantener a disposición permanente del público, a través de sus sitios web electrónicos de la red Internet[201], 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 *on line* serán la planta del personal y el personal a contrata y a honorarios, con las correspondientes remuneraciones.

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.

[200] 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 1º 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 1º precedente".*

[201] 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.

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 que se transcribe, al decir que *"no se incluirán en estos antecedentes los datos sensibles, esto es, los 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 los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"*.

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 incluyó casi al final de la tramitación legislativa, en una Comisión Mixta de Enero del año 2008 y a instancias de los Honorables Senadores *Larraín* y 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 a ley 19.628 para excluir a sus datos sensibles de dicha publicidad.

El Reglamento de la ley, 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.

2. (i) La regla general en sede de 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 del artículo 7° y no estar disponibles en fuentes públicas y, los referidos a los beneficiarios, por ser además datos sensibles.

(ii) 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 de acceso y transparencia.

3. 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 N°2 y N°5 y 33 letra m), estas referencias en sede de 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 a 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 contra excepción, sus datos sensibles de aquellos a que alude la ley 19.628.

4. 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.

E. Invocación de *"los derechos contemplados en la ley 19.628"*, en especial del derecho de controlar y autodeterminar el tratamiento de sus datos personales, como *"causa suficiente"* para que un tercero notificado en virtud del artículo 20 de la ley 20.285 se oponga a la solicitud de acceso a la información.

1. Como ya consignamos, el Título IV se refiere al *"Derecho de Acceso a la Información de los Órganos de la Administración del Estado"*, y el artículo 10°, al inicio del Título, establece como principio fundamental 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 la propia ley 20.285.

Agrega o precisa que *el acceso a la información comprende por regla general el derecho de acceder* (i) a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como (ii) *a toda información elaborada con presupuesto público*, cualquiera sea el formato o soporte en que se contenga. Las excepciones, como veremos más abajo, están con templadas en el artículo 21.

Ante la obligación expresa para los servicios públicos de entregar o proporcionar la información que se les solicite, la concurrencia (i) "*de la oposición de un tercero regulada en el artículo 20"* o (ii) "*de alguna de las causales de secreto o reserva que establece la ley"* son las únicas hipótesis en que podría presentarse una negativa a la solicitud de acceso, que siempre será fundada[202].

El artículo 20° se pone en el supuesto de que la solicitud de acceso presentada ante el servicio público aluda o se refiera a *"documentos o antecedentes que contengan información que pueda afectar los derechos de terceros".*

SOTO VELASCO estima que esta posibilidad de oposición de un tercero es una herramienta de gran relevancia y un aspecto esencial del sistema que garantiza su legitimidad, para que no se pierda su razón de origen -el control del Estado por los ciudadanos- y se transforme en un mecanismo de acceder a información privada que es administrada por los servicios públicos[203], misma a la que además visualiza como parte o dentro de *"una amplia esfera de privacidad de las personas*".

Se trata de una posibilidad o de una eventualidad de perjuicio, lo que requiere de una estimación o calificación del órgano público acerca de que "*potencialmente"* la entrega afecte a los terceros, y por lo mismo, no se requiere certeza al decidir si comunicarles y/o notificarles de las solicitudes. Quizás a esto se ha referido el profesor SOTO VELASCO cuando menciona la necesidad de advertir un relativo desamparo en el que quedan los funcionarios públicos que reciben y resuelven las solicitudes de acceso, los que deciden en sólo dos días hábiles, *en primer lugar*, si una petición alude a documentos o antecedentes que contengan información que pueda afectar *"los derechos de terceros",* y *en segundo lugar*, quiénes son específicamente los terceros que deben ser notificados[204].

Entre esos antecedentes con información factible de afectar los derechos de terceros pueden haber datos personales de aquellos que ampara y regula la ley 19.628 de 1999, o los mismos pueden estar consignados en los documentos

---

[202] El artículo 16 señala que *"...deberá ser fundada, especificando la causal legal invocada y las razones que en cada caso motiven su decisión*"

[203] Él alude a información *"que está en su poder",* pero tal referencia quizás induce al error de creer que a los órganos de la Administración la data nominativa les pertenece.

[204] Por su especial naturaleza, quizás no se presenten conflictos cuando lo solicitado se refiera a datos personales sensibles o personalísimos o aquellos sujetos a una obligación legal expresa de secreto; el funcionario público claramente deberá notificar a los titulares, por ejemplo si al Ministerio de Salud se le piden los antecedentes sobre enfermos con el virus VIH. En otros casos, efectivamente la opción -a que alude SOTO VELASCO- de notificar a muchos posibles afectados para que al menos uno se oponga y la decisión se traslade al Consejo de Transparencia aparece como muy factible.

que se soliciten. Y ese o esos terceros quizás querrán evitar la publicidad o el conocimiento de los antecedentes nominativos que a ellos aluden e identifican, ejerciendo su derecho de oposición, siempre *"con expresión de causa"* -señala imperativamente la ley 20.285- (...lo que por cierto lo diferencia de los requisitos establecidos para el derecho de acceso del artículo 10°).

O incluso más, bastará que el tercero sólo quiera *"conocer y acceder"* -un derecho específico- al tratamiento, cesión o comunicación de sus antecedentes que en principio se está pidiendo que realice un servicio público en sede de la ley 20.285, para simplemente exigir la "*eliminación"* (porque son datos errados, almacenados sin fundamento legal o caducos) o el *"bloqueo"* de ellos *-todos derechos específicos que concede la ley 19.628-*, los que luego de eliminados o bloqueados no podrían ser entregados en virtud de la solicitud de acceso del artículo 10° de la ley 20.285.

¿Cuál sería el posible conflicto a nivel de principios y regulación que se presenta?: ...que, a diferencia de lo que le exige para oponerse al tercero el inciso segundo del artículo 20° de la ley de acceso y transparencia, el artículo 12 de la ley 19.628 en el caso del bloqueo de datos entregados o proporcionados voluntariamente no exige expresión de causa, y esto debe ser cumplido por el responsable de la base de datos del servicio público y debe ser hecho cumplir por el Consejo de Transparencia.

La norma en comento dispone que la autoridad, jefatura o jefe superior del órgano o servicio de la Administración del Estado, dentro del breve plazo de dos días hábiles que se cuenta desde la recepción de la solicitud que cumpla con los requisitos legales, deberá… *-está imperativamente dicho porque no es una simple opción, y de no hacerse se incurre en las responsabilidades del Titulo VI de la ley 20.285, en las de la ley 19.628 y en las de la Ley General de Bases de la Administración del Estado que opera supletoriamente-* …comunicar el hecho mediante carta certificada a la o las personas a que se refiera o afecte la información, recordarles la facultad que les asiste para oponerse a la entrega de los documentos solicitados, adjuntando copia del requerimiento respectivo que se le ha presentado.

Agrega la ley (i) que los terceros afectados podrán ejercer su derecho de oposición dentro del plazo de tres días hábiles contado desde la fecha de notificación; (ii) *que la oposición deberá presentarse por escrito y que como anticipamos "requerirá expresión de causa"*; (iii) que deducida la oposición en tiempo y forma el órgano requerido quedará impedido de proporcionar la documentación o antecedentes solicitados, salvo resolución en contrario del Consejo, dictada conforme al procedimiento de amparo del derecho de acceso que se establece en los artículos 24 y ss.; y, (iv) que en caso de no deducirse la oposición *"se entenderá*" *-es una consecuencia o efecto jurídico que establece la ley en caso de inactividad o silencio del titular de los datos-* que el tercero afectado accede a la publicidad de dicha información.

2. Esos *derechos de terceros contemplados en la ley 19.628, ampliamente considerados*, son los mismos que luego menciona, como causal de reserva el artículo 21 N°2 de la ley 20.285 cuando se refiere a que a consecuencia de una petición de acceso puedan afectarse derechos de las personas, *"particularmente tratándose de su salud o de la esfera de su vida privada o derechos de carácter comercial o económico".*

SOTO VELASCO estima, nuevamente, que el derecho a oponerse a la publicidad de antecedentes que puedan afectarlos no debe entenderse referido sólo a su vida privada, sino que además, por ejemplo, puede verificarse en su capacidad de manejar información estratégica para competir en un mercado determinado[205].

Pero si las mencionadas son causales de reserva para el servicio público requerido, jurídicamente no vemos obstáculos a que se estimen como causa suficiente para que en forma anticipada y/o complementaria el tercero también se oponga a la solicitud de acceso invocando esta misma causal, máxime cuando puede haber sido presentada por un peticionario sin invocarse interés legítimo, motivo ni causa alguna, porque así lo permiten las disposiciones y los principios de ley de transparencia y acceso.

Esos *derechos de terceros contemplados en la ley 19.628* constituyen causas especificas expresables por el tercero al oponerse, tales como: (i) el que se estén solicitando antecedentes personales o nominativos, de aquellos que la ley 19.628 sujeta a la obligación general de secreto o de reserva para el servicio público en el artículo 7°, (ii) el que no están disponibles en fuentes de acceso público, (iii) el que una ley especial establece expresamente su calidad de antecedentes nominativos secretos (como es el caso del artículo 35 del Código Tributario), o (iv) porque son particular y especialmente reservados como los datos sensibles o personalísimos.

Por cierto: para aplicar el Instituto de la ley 19.628 en relación a este derecho de oposición de los terceros no nos podemos apoyar, de modo alguno, en

[205] Agrega o aconseja el Profesor SOTO que debiera revisarse la Jurisprudencia de los tribunales ordinarios relacionada con la vida privada; ello es inoficioso, toda vez que los recursos de protección presentados y fallados han tenido como objetivo actos arbitrarios o ilegales relacionados o con la vulneración del honor o de la honra, o con el derecho a la propia imagen, que son bienes jurídicos distintos a la vida privada, a la privacidad o intimidad, tanto en cuanto datos personales tratados computacionalmente. El caso más frecuente, el de hacer aparecer por error a un titular en el sistema comercial como sujeto de protestos o mora, es de fácil solución una vez que se acredita el error y el perjuicio para el sujeto publicado. Lamentablemente, y salvo error u omisión, a esta fecha no existe jurisprudencia como el resultado del mero ejercicio del derecho de acceso o Habeas Data, mecanismo procesal que ni siquiera se ha utilizado para corregir la publicación errada de datos patrimoniales negativos porque se ha preferido la herramienta del Recurso de Protección.

lo que se ha referido como *"…el acervo jurídico existente a la fecha en los operadores producto de la aplicación de la ley 19,628".* Como analizamos en extenso en la Parte Primera, la ley sigue siendo una norma no conocida -casi *"lírica"* dijo un abogado alguna vez-; sigue sin haber sido proyectada al mundo de la red Internet; son muy pocos los recursos procesales de Habeas Data interpuestos; es casi un mito la supuesta ilegalidad -denunciada a la prensa- de los actos del Estado respecto a las bases de datos nominativos que requiere y administra sólo con fines de servicio público y actuando dentro de sus competencias; y es poco el aporte de trabajos de investigación que amalgaman doctrina antigua española y textos legales europeos, sin aplicar el material a realidades concretas especialmente del sector privado, que si afectan la privacidad y que nada tienen que ver con la honra, el honor o el derecho a la imagen de las personas.

3. A nuestro parecer, el tercero puede incluso oponerse en base a una causal genérica y amplia, esto es, el *"ejercer el derecho esencial de controlar y autodeterminar el tratamiento y/o cesión o comunicación que se quiere hacer de sus propios antecedentes o datos personales",* mismo que, reconocido en los artículos 4° y 12° de la ley 19.628, es un derecho irrenunciable que se traduce en que si él no autoriza la entrega de los datos expresa, formal y fundadamente, y ellos además no son subsumibles bajo una *"esfera social o pública"* de los ciudadanos, el servicio público debe abstenerse de entregarlos. Porque -*debe siempre tenerse presente*- al servicio público los datos de los ciudadanos no le pertenecen y sólo es un mero poseedor de ellos, con una competencia para "*tratarlos"* que no siempre habrá sido asignada -necesariamente- con la amplitud que pudiera colegirse de la lectura del artículo 2° letra o)[206].

Y a su turno, conociendo el Consejo de Transparencia del recurso de amparo del derecho de acceso (artículo 24), tampoco podría entenderse -interpretándose en forma no restrictiva y sumado a los argumentos ya referidos en los acápites A y C- que *"la norma del artículo 5° o la del artículo 10° de la ley 20.285"* constituyen *"tácitamente"* una autorización legal conferida a los servicios públicos para tratar, ceder, comunicar o publicar los datos nominativos con prescindencia de la voluntad de su titular, a que también alude la regla general del artículo 4° de la ley 19.628[207].

[206] Recuérdese que la norma señala que es tratamiento de datos, 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.

[207] Conforme lo dispone el artículo y la totalidad de la ley 19.628, las habilitaciones legales para el tratamiento de datos personales sin el consentimiento ni la autorización de su titular deben ser expresas y no tácitas.

4. Recuérdese que, *en sentido estricto,* de cara a los específicos derechos que consagra la ley 19.628 para que los ciudadanos titulares de los datos personales registrados en bases y bancos de datos de los servicios públicos puedan controlar y autodeterminar el tratamiento de sus antecedentes, con ocasión de esta oposición del artículo 20 el responsable del STDP del servicio público podría ser objeto por parte del tercero y titular de los antecedentes de un derecho de información y acceso, de un derecho de rectificación o modificación, de un derecho de cancelación o eliminación, de un derecho de bloqueo y de un derecho de indemnización.

5. Un caso concreto que ya se ha presentado -no en sede del acceso de la ley 20.285 por cierto- puede servir al análisis y sería el siguiente. El de una empresa del sistema de información comercial que existe en Chile, interesada en acceder en forma asociada a los datos de los propietarios de los bienes raíces en Chile, es decir, a que se le entreguen en forma sistematizada y asociada todos los Roles de Avalúo con todos los respectivos RUT de las personas naturales que figuren como sus propietarios en el STDP de un órgano de la Administración.

En definitiva, y en sede de protección de datos personales, lo que se está pidiendo en el ejemplo es conocer, sólo con fines de lucro, la situación patrimonial o los datos personales patrimoniales de los ciudadanos, que son antecedentes en Chile amparados por la ley 19.628, no disponibles en fuentes de acceso público, sujetas a la obligación general de secreto del artículo 7° de la ley 19.628, tratados por los servicios públicos competentes sólo con la finalidad de velar por la aplicación y pago del impuesto territorial, y sin que ley alguna obligue a algún servicio público a entregar o proveer esos antecedentes nominativos en forma sistematizada[208]. Antecedentes que por cierto, asociados, permitirán conocer la capacidad patrimonial en materia de bienes raíces de una persona y en definitiva violar la esfera de su vida privada a que alude el artículo 21 N°2 como causal de reserva o secreto.

Ergo, cada uno de los propietarios y titulares de sus datos personales identificativos y patrimoniales poseerá un *"motivo"* o una *"causa suficiente"* para oponerse a la solicitud de acceso que haga la empresa distribuidora de información, sólo con fines comerciales, y en este supuesto, es que consideramos que el Consejo de Transparencia si debería calificar si es legítimo, motivado y poseedor de causa -o no- el interés de la solicitud[209], porque la petición de acceso se relaciona directamente con las garantías de la ley 19.628 que el Consejo está llamado a velar para que se apliquen en los servicios públicos, dejándose de lado el principio de la no discriminación del artículo 11.

[208] Por cierto, los datos de los roles de avalúo están disponibles en cada una de las municipalidades por separado, pero ellos no se asocian a los RUT de los propietarios, porque asociados, pasan a ser un dato personal nuevo, y no se encuentran disponibles en forma sistematizada.
[209] Siempre se verificará acá la necesidad de realizar un test de transparencia.

6. El Consejo de Transparencia en uno de sus Decisiones de Amparo que se analizan en el último acápite de esta Segunda Parte -como hemos mencionado a pie de página- ha debido considerar los alcances del ejercicio de este derecho.

El caso fue el de un recurso interpuesto en 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 N°A35-09).

Respecto de los dos postulantes que no se opusieron a la entrega de su identidad ni informaron el traslado que les fue conferido en conformidad al artículo 20 de la ley 20.285, el Consejo estimó, "*en principio",* que podría aplicarse el artículo 7° de la ley 19.628 y declarar que sus identidades eran reservadas.

Pero *"en definitiva",* teniendo a la vista el inciso final del artículo 20 de la ley de acceso y transparencia, que 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 ella accede a la publicidad de la información, el Consejo consideró que esta norma era la que debía preferirse y aplicarse en este caso, (i) por su especialidad y (ii) por el interés público existente en conocer el funcionamiento de este servicio público, ya que no se trataba de la identidad de cualquier postulante sino, específicamente, de la de aquéllos que fueron propuestos para ser elegidos por el Comité de Selección de directivos.

7. Para terminar y antes de pasar al acápite siguiente, y recogiendo afirmaciones del citado profesor SOTO VELASCO, es plausible -y esperable- que el funcionario público que debe resolver la solicitud de acceso pueda negarla si a su parecer y después de un análisis de fondo acerca de los bienes jurídicos involucrados, así se estima procedente porque se estarían afectando los derechos de las personas, al margen o con independencia de que esta oposición de un tercero no se haya verificado.

Es decir, la negativa al acceso solicitado sería procedente aún cuando deba entenderse legalmente que el tercero afectado que nada dijo accedió a la publicidad de la información, en conformidad al inciso final del artículo 20. El problema es que, en el hecho, esta opción de rechazo no fundada en alguna de las causales legales que contempla la ley 20.285 implicará probablemente un análisis de mérito, es decir, tener en vista (i) quién pide los antecedentes que pueden afectar los derechos de las personas y (ii) para qué o con qué fines se está pidiendo, opciones que -como señala SOTO VELASCO- no son admisibles en el marco de la ley de acceso y transparencia.

Al margen de que se permita o no invocar en forma autónoma y sin el parecer de los terceros una causal consistente en la afectación de los derechos de las personas y su necesaria protección -v.gr. y de la mano de la jurisprudencia comparada, se mencionan cuando se trate de antecedentes *"comercialmente sensibles"*[210], de archivos médicos (que en Chile son secretos porque así lo establece el artículo 127 del Código Sanitario), o de archivos personales que al publicarse ocasionarían una invasión a la privacidad-, …las herramientas específicas que la ley 20.285 concede al servicio público para actuar de esta forma y velar por la protección de los derechos de las personas son las causales genéricas de secreto o reserva del artículo 21.

F. 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.

1. 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, aún 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[211], 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. Porqué unas

[210] Es interesante la cita de jurisprudencia de EE.UU. que realiza el profesor SOTO VELASCO, en la que se llegó a determinar que debía calificarse como confidencial a cualquier información financiera o comercial cuya entrega pudiera *"probablemente"* afectar la capacidad del Estado para obtener información necesaria en el futuro, o que pudiera causar un *"daño substancial"* a la posición competitiva de la persona que entrega la información o que envía los documentos a un servicio público.

[211] SOTO VELASCO menciona como ejemplo una causal que se debatió y se rechazó en el Parlamento, que aludía a *"el acuerdo entre instituciones de Chile y otro país".*

especificaciones y no otras?; SOTO VELASCO 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 futura del Consejo de Transparencia pasará por dar una adecuada interpretación a estas causales ante su necesidad de acotarlas, y nos sumamos a ella[212].

Lo hacemos -*el sumarnos a entender lo esencial del rol interpretativo y de delimitación de las causales que le cabe al Consejo*- desde esta perspectiva: ...la de entender que limitar o restringir los alcances de la transparencia y el acceso cuando 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).

2. *Causales de los números 1, 3 y 4 (referencia).*

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 excepcionarse de la entrega de los documentos o antecedentes en tres casos:

(i) …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;

(ii) …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[213]; y,

(iii) …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- 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 como se verificaría la distracción indebida y de alto costo operativo, antes de

[212] (SOTO VELASCO) 2009

[213] 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.

optarse por no amparar el derecho a la información y acogerse la causal invocada[214].

El número 3 alude al supuesto que *"la publicidad, comunicación o conocimiento"* afecten la seguridad de la Nación, *"particularmente"* -y 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 menciona, por ejemplo, que también se afectaría el interés nacional si con la petición estuviera comprometida "*la política exterior del país"*.

3. *Causales de los números 2 y 5.*

3.1 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 (i) su seguridad, de (ii) su salud, de (iii) *la esfera de su vida privada* o de (iv) 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.

(i) 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

[214] 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.

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.

(ii) Y a otras disposiciones constitucionales, legales y reglamentarias, partiendo por el artículo 19 N°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 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*[215]; 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 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.

[215] 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.

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 de Transparencia, en especial, reconociendo en uno de sus fallos de Amparo *-en concreto el N°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 N°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 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 juego[216] 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 deslegitimizar el sistema, porque de divulgarse sin restricciones la información sobre la vida privada de los ciudadanos se perdería *"su razón de origen"* -que el ciudadano pueda controlar al Estado- y pasaría a ser -el sistema- y pasar a ser una válvula de acceso a la información privada de los ciudadanos.

3.2 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 8º 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*

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

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 N°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.

G. Acerca del rol -preliminarmente asignado- por el artículo 33 letra m) de la ley 20.285 al Consejo de Transparencia.

1. Ocurrió, inicialmente, que en la ley 20.285 se contempló una nueva función para el llamado Consejo de Transparencia, ajena a la obligación de tutelar y velar por el acceso a los actos, contratos, resoluciones y documentos de los órganos del Estado y relacionada con el Habeas Data o Derecho de Acceso a los datos personales de los chilenos que regula el artículo 12 de la ley 19.628.

Señaló el artículo 33 letra m de la ley 20.285 que el Consejo tendría, entre sus funciones y atribuciones, la de *"velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal por parte de los órganos de la Administración del Estado".* Durante la tramitación parlamentaria se había propuesto que la facultad fuera la de velar por la debida reserva *"de los datos e informaciones que conforme a la Constitución y a la ley tengan carácter secreto o reservado",* y el cambio terminológico no es menor si no que trasunta una intencionalidad y una política legislativa de ir en concreto -salvada sea la expresión coloquial- *"a por la protección de los datos personales".*

Es decir, se trató de un señalamiento genérico que asigna algún grado no precisado en el mismo artículo de competencia fiscalizadora al Consejo por sobre los funcionarios "*responsables"* -y a futuro además sobre los funcionarios *"encargados"* según el Boletín 6120- de registros, bases y bancos de datos de órganos públicos (...recuérdese que el conjunto de *"bases", "ficheros"* o *"registros"* es un *"banco"* de datos), y quedaba pendiente -por cierto-, en esa pasada parlamentaria, el tema de la regulación de los responsables de bases de datos privadas o particulares.

En el hecho y en Derecho, el Consejo de Transparencia se ha constituido con esta facultad genérica y amplia en una entidad pública y autónoma que debe fiscalizar el respeto de todas las normas técnicas y jurídicas relacionadas con la gestión diligente de los sistemas de tratamiento de datos personales o nominativos en el sector público o al interior de la Administración del Estado, a cuyo análisis hemos dedicado la extensa *Primera Parte* de este Informe. Sólo cumpliendo con

esta potestad proyectada a los ámbitos relacionados, se verificará que los servicios públicos cumplan adecuadamente con la ley 19.628.

Sería una grave *capitis diminutio* que se entendiera su competencia sólo referida al concreto articulado de la ley 19.628

Esta facultad asignada en el artículo 33 letra m) debe percibirse concordante además, con otras obligaciones que -*a propósito del Derecho de Acceso a la Información del Estado y para lograr un equilibrio entre éste y la protección de la privacidad de los ciudadanos*- recaen sobre el Consejo.

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.

Lo anterior, lo establecido en el artículo 33 letra m), reiteramos, es una competencia limitada. Esta facultad se contempló o se agregó en forma paralela o al margen de la previa institucionalidad del acceso a la información de la gestión de la Administración Estatal cuya probidad se busca controlar, pero 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 a creer que el Consejo posee competencia procesal y administrativa para conocer de reclamos en que se invoque su no aplicación o respeto por los servicios públicos.

Sería el caso -*de falta de competencia*-, por ejemplo, cuando un responsable de la base de datos de un servicio público negara el acceso a un titular que lo ha requerido en conformidad al artículo 12 de la ley 19.628, y en vez de accionar ante la negativa o la no respuesta en sede judicial en conformidad al artículo 16 de la misma norma -descartándose el recurso ante los tribunales- y sin tratarse del conocimiento de actos, contratos, documentos o resoluciones de un servicio público, se interpusiera un recurso de amparo al derecho de acceso en conformidad a los artículos 10° y 24 de la ley 20.285.

2. Pero se acordó en el Parlamento retomar el tema de esta nueva competencia del Consejo de Transparencia en otro proyecto de ley.

Consta en las actas de la Sesión en la Sala del Senado del 14 de Enero del año 2008 y en el marco de la Comisión Mixta, que el Diputado Señor *Cardemil* da cuenta de que se tuvo la ocasión de analizar la experiencia de países como Gran Bretaña, donde existía un Consejo que manejaba *"en una sola mano"* toda la

información pública relacionada con datos de carácter personal. El parlamentario aclaró que el Consejo de ese país tenía las facultades de velar por las normas de transparencia activa y pasiva, pero además *"velaba por la protección"* -porque su competencia es garantista y no publicista- de los datos personales de los ciudadanos que procesaran -únicamente- los servicios públicos. Terminó por comentar que habría sido ideal que tal opción se hubiera logrado introducir en el sistema chileno, *"pero no se pudo"*, y por ende se conversó con el Ministro -del MINSEGPRES- para que a futuro se enviara un proyecto de ley complementario.

Ergo, con el Boletín 6120 del año 2008 -ya analizado en extenso en la Primera Parte de este Informe[217]-, se estaba cumpliendo con el acuerdo entre el Ejecutivo y el Congreso de avanzar y profundizar la regulación para el resguardo del tratamiento de los datos personales, ya no sólo respecto de los STDP del sector público sino además en el sector privado.

En derecho, a esta fecha se tramita el proyecto de ley contenido en el Boletín 6120 que extiende dicha competencia a los sistemas de tratamiento del sector privado, y que le otorga formalmente el rol de la Autoridad, Agencia o Consejo de Protección de datos personales en Chile, con las competencias nuevas que un órgano de esta naturaleza requiere

En concreto, sobre este punto el Mensaje del Proyecto declaró:

> *"Considerando la necesidad de dar respuesta a las exigencias de protección del derecho a la autodeterminación informativa, sumado a la conciencia de que el establecimiento de una autoridad de control es fundamental para el real cumplimiento de la ley, se planteó la necesidad de incorporar facultades en esta dirección dentro de las competencias del Consejo para la Transparencia, durante la discusión parlamentaria de la ley N° 20.285. Sin embargo, sólo se incorporó la facultad de "Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado". Se tuvo conciencia de que ello sería insuficiente para el resguardo del tratamiento de los datos personales y los derechos de los titulares. Pero se concordó en avanzar y profundizar la actual regulación".*

De aprobarse el proyecto como está tendremos en realidad una nueva entidad, una de protección, control y resguardo de datos personales ante el requerimiento de sus titulares que quieren controlar y autodeterminar sus antecedentes nominativos (similar a la APD de España o al CNIL de Francia), y no equivaldrá a la competencia que en virtud de la ley 20.285 se le asignó al Consejo para asegurar la transparencia y publicidad de los actos, contratos, documentos y antecedentes de la gestión de la Administración del Estado.

[217] Véase el apartado final de la letra B de la Parte Primera.

Puestos en este escenario, debiéramos dejar de hablar y de escribir acerca de la *"desnaturalización del Consejo de Transparencia"*[218]

Téngase presente, sin teorizar. Devenido en Autoridad de protección de datos el Consejo deberá hacerse cargo, por ejemplo, (i) de los problemas de la red *Swift* -que también opera sin control en Chile y transfiere internacionalmente datos de los chilenos-, (ii) de los abusos de la empresa *Choicepoint*, (iii) de los excesos conocidos por el negocio entre una empresa funeraria y algunas Isapre, y (iv) de eventualmente ver que la nueva entidad garante y fiscalizadora del tratamiento de datos personales o nominativos de los chilenos tenga la capacidad jurídica que en España ha llevado a que la Agencia de Protección de Datos sancione a empresas como Telefónica o Terra por no resguardar la confidencialidad de los datos de sus clientes[219].

3. ¿Qué es lo que podría o no hacer a esta fecha el Consejo, atendido el señalamiento del artículo 33 letra m) de que debe velar por la aplicación o *"el adecuado cumplimiento*" de la ley 19.628?:

(i) ¿Mantener un Registro Único Nacional de Bases de Datos?; creemos que no.

(ii) ¿Fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estimara pertinente?; creemos que si.

(iii) ¿Inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley?; creemos que si.

(iv) ¿Requerir la inscripción de los bancos de datos que no estén registrados en el Registro Único Nacional?; creemos que no, porque en la propia normativa de protección de datos al Registro Civil no se le dio competencia para hacerlo.

(v) *¿Dictar instrucciones de carácter general o particular respecto de las condiciones de legitimidad de un tratamiento de datos personales?; creemos que si, pero sería una función meramente informativa y que no podría sancionarse si no se cumpliera con lo instruido.*

(vi) ¿Conocer de las reclamaciones de particulares relacionadas con el ejercicio del Habeas Data y de los derechos que le confiere la ley 19.628?;

[218] Véase la URL http://www.latercera.com/contenido/895_146299_9.shtml

[219] Véase las URL http://www.guiaservicios.com/serv_noticia_detalle.php?pk_noticia=10 y http://www.diariojuridico.com/noticias/la-apd-multa-con-mas-de-840-mil-euros-a-telefonica-por-el-tratamiento-indebido-de-datos-personales.html

creemos que no, porque el artículo 10° de la ley 20.285 no subsume en sus supuestos a los datos personales o nominativos, y porque la ley 19.628 obliga a recurrir a los tribunales de justicia en caso de una negativa o una respuesta disconforme del responsable de la base de datos del servicio público.

(vii) ¿Ejercer potestades sancionadoras contra los responsables de los bancos de datos de los órganos de la Administración que infrinjan la normativa sobre protección de datos?; definitivamente no.

(viii) ¿Requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro?; definitivamente no.

Todo lo mencionado anteriormente serán, sin posibilidad de discusión, las nuevas competencias del Consejo si se aprueban las modificaciones a esta fecha en trámite parlamentario.

4. No compartimos a priori -y a esta fecha- afirmaciones del tipo que de concentrarse ambas funciones —la de *"promover el acceso y transparencia*" y la de *"velar por la protección de datos de carácter personal"*— en el Consejo, la labor de ponderación sería efectuada de una manera más eficiente y con criterios armónicos y uniformes. No porque a esta fecha y ante solicitudes de acceso el Consejo haya ponderado y resuelto aplicando un test de transparencia algunos casos por la aplicación de la ley 19.628, se asegura adecuada ponderación.

Recuérdese además que esto es una aspiración que procedería sólo tratándose de Habeas Data presentados contra los servicios públicos, porque nada se debe conciliar y nada puede decir a esta fecha el Consejo de Transparencia -derivado de su *expertice* y competencias- cuando se aluda a la problemática del tratamiento de datos personales en el sector privado, esto es, en la banca, el retail, las compañías de seguros, las AFP, las ISAPRE, etcétera. Y es acá, no en el sector público, donde se juega prioritariamente el rol de un nuevo ente garante de la protección de datos personales en Chile.

H. 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 sede de la ley 20.285, con los supuestos y principios esenciales de la ley 19.628.

1. *Hipótesis de trabajo.*

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 de 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 N°2 y N°5 pero, muy especialmente, el Consejo de 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 propio 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.

2. *En principio, ...las normas legales pertinentes son claras y los Dictámenes de Amparo del Consejo de 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 sede 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, frente a las preguntas acerca de *qué se pide*, *quién lo pide* y *para qué se pide*, en sede 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",* 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 N°A8-09* de Junio del año 2009 pronunciada en virtud de una supuesta decisión de denegación de acceso de Chilecompras, 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 *-...mismas que, en cuanto a su contenido y por mandato de transparencia activa, si 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.chilecompras.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[220].

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 *site 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 in formación de los artículos 12 y ss.

(ii) El pronunciamiento anterior fue ratificado en Julio del 2009 en la *Decisión de Amparo N°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 N°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 restricciones a su empleo que no estén establecidas expresamente por una ley, y,

[220] 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 links sin autorización a sitios comerciales o de ofertas de consultoría.

(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 un mero fin de lucro, y no fiscalizar la probidad de las actuaciones del Servicio de Impuestos Internos. *¿Cabe entender que los servicios públicos deben 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.

3. *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 sede 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 sede de transparencia y acceso de la ley 20.285, que si lo solicitado 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 de 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 *N°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.

4. Sirve como ejemplo nuevamente el caso referido más arriba. Ante una solicitud de acceder en forma asociada a los datos personales RUT + 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 que se hace, sólo 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), por parte de una empresa distribuidora de información. 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.

5. En la Parte Primera del presente Informe consignamos algunos de los principios esenciales de la ley 19.628, los que no están señalados expresamente como los del artículo 11 de la ley 20.285. Pero, por cierto, son los mismos de la legislación española y de las Directivas de la Unión Europea, toda vez que la ley chilena de 1999 tomó -supuestamente- como modelo a la LORTAD española de 1992 y a la ley de Francia de 1978.

Sostuvimos que no era libre la gestión administrativa que realizan los servicios públicos mediante STDP -porque debía ajustarse a derecho-, y que además de las normas expresas referidas, subyacían en la ley 19.628 diversos *"principios esenciales"* que inspiraban la regulación, recogidos de la legislación y la doctrina extranjera y que configuraban un verdadero *"Código Deontológico"* para los funcionarios públicos responsables del tratamiento de los datos nominativos de los ciudadanos. Ellos son, conforme la última síntesis oficial que realiza el Boletín 6120 tantas veces referido, el principio (i) *del consentimiento del titular*, el (ii) *de los datos personales especialmente protegidos*, el (iii) *de la calidad de los datos*, el (iv) *de seguridad y de responsabilidad*, el (v) *de secreto* y el (vi) *de la cesión o transferencia telemática de datos personales.*

Confrontados estos principios con los de la ley 20.285, claramente surge una diferencia radical entre el secreto, la reserva y la confidencialidad general de la ley 19.628 con la publicidad, apertura y transparencia de la ley 20.285, que

presume que toda la información en poder de los órganos del Estado es pública. Los "Nortes" orientadores, las reglas generales y por ende las Políticas subyacentes son diversas.

(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[221].

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 al 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

[221] 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 entrabar la gestión de la Administración del Estado.

del Estado deben proporcionar información en los términos más amplios posibles, excluyendo sólo aquello que esté sujeto a las excepciones constitucionales o legales.

6. Un ejemplo concreto puede servir para relevar como 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 sede 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 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 RUN de ellos cuando este 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.

I. Comentarios a algunos criterios jurisprudenciales del Consejo de Transparencia, sostenidos en los Dictámenes de Amparo en materia de tratamiento y protección de datos personales[222].

1. De manera general, la *experiencia y los criterios contenidos en algunos de los Dictámenes de Amparo que ha emitido el Consejo de Transparencia* permiten establecer algunas clasificaciones y/o distinciones. Algunas de las opciones se comparten en este Informe y otras -como el caso del *Dictamen de Amparo N°A10-09,* sobre el acceso a las calificaciones por su desempeño de los funcionarios públicos, las informamos en su momento para ser resueltas en forma contraria a la decisión que -en definitiva- adoptó el Consejo.

En efecto, el Consejo:

(i) Ha considerado que algunos datos personales de los funcionarios públicos, como sus calificaciones, deben ser entregados en sede del acceso a la información administrativa;

(ii) Ha resuelto además que antecedentes como los números de RUT de los ciudadanos y de los funcionarios deben ser mantenidos en reserva al momento de entregar otros antecedentes -en coincidencia con la norma que en sede de transparencia activa obliga a informar los datos personales sobre remuneraciones de los funcionarios asociados a sus nombres y apellidos-;

(iii) Ha resuelto que los datos personales de aquellos ciudadanos que estén optando a cargos de funcionarios públicos deben ser transparentados cuando los mismos postulantes, titulares y propietarios, los soliciten;

(iv) Ha resuelto que respecto de los ciudadanos algunos datos personales deben ser tachados al entregarse la información solicitada; y,

[222] Comentarios y análisis de los propios abogados del Consejo de Transparencia, en los que se pone el énfasis en la forma en que el Consejo ha resuelto los *test de transparencia* y efectivamente ha equilibrado la protección de datos personales con el acceso a la información, pueden verse en la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

(v) Ha considerado que los datos personales y en especial los sensibles o personalísimos de los ciudadanos deben ser reservados y no accesibles por cualquier persona, que no posean en definitiva y de hecho -es nuestra opinión- interés legítimo, causa o motivo pero en sede de la ley 19.628.

2. *Algunos datos personales "de los funcionarios públicos", como sus calificaciones funcionarias, deben ser entregados en sede de Derecho de Acceso (DA N°A10-09 y N°A126-09).*

2.1 *Supuesto o hipótesis de análisis.*

Al MINVU y a FONASA se les pidieron en sede de la ley 20.285 datos personales o nominativos de los funcionarios públicos que trabajan en los servicios, relacionados con sus calificaciones de desempeño profesional.

Concretamente, se solicitaron en forma masiva y nominada, no disociada, identificada y referida a un funcionario determinado las calificaciones de todo el personal y ex-funcionarios del MINVU y FONASA desde el año 2003 al 2008, en formato Excel, conteniendo en cada columna el RUT, tipo de contrato, el estamento, sexo, puntaje, lista de calificación, y el año. Además, se solicitó incluir la tabla de calificaciones y los rangos de inicio y término de cada lista de calificación.

2.2 De manera general, respecto a un funcionario público puede interesar conocer antecedentes, por ejemplo, sobre sus remuneraciones, la modalidad de contratación, sus licencias, enfermedades o su estado de salud, el hecho de ser o no discapacitado para determinar si se cumple con algún porcentaje mínimo obligatorio que la ley exija estén contratados en un servicio público, sus calificaciones, sus declaraciones de impuestos, su situación patrimonial y sus declaraciones de patrimonio, sus antecedentes penales, si cumple con los requisitos de ingreso a la Administración Pública, sus cualificaciones profesionales o curriculum vitae, sus fotos, sus nombres, el número de su teléfono celular y el nivel de gastos reflejados en la cuenta, sus relaciones familiares o la nómina de sus parientes que trabajan en el mismo servicio público, o incluso -es un tema del cual nos hicimos cargo en la parte primera- el contenido de sus correos electrónicos funcionariales.

La situación de algunos de estos datos personales ya está resuelta expresamente por normas de Derecho Público que presumen intereses legítimos en los solicitantes o el interés público involucrado. Por ejemplo, se publican remuneraciones y la modalidad en que está contratado el funcionario -planta, a contrata, a honorarios- en sede de transparencia activa; los datos de salud son

sensibles y reservados[223]; sus declaraciones de impuestos son secretas -como las de todos los contribuyentes-; sólo algunas declaraciones de patrimonio son públicas y obligatorias de realizarse; y, debe acreditarse públicamente el cumplir con los requisitos de ingreso que establece el Estatuto Administrativo.

Si no hay norma expresa sobre "*las calificaciones"*, y si son datos personales no disponibles en fuentes públicas, nuestro análisis jurídico se inclinó por su reserva y la improcedencia de ser revelados masivamente en sede de la ley 20.285. La conclusión sería diversa, si con la divulgación del dato personal *"calificación del funcionario"* se permitiera conocer el desempeño -correcto o no- de las tareas y responsabilidades asignadas únicamente a un funcionario y en un caso concreto o determinado, a cuyo respecto se acreditara un interés legítimo del solicitante -cosa que por cierto la ley de acceso y transparencia no exige-.

2.3 Los planteamientos que formulamos, para sostener la postura de la negativa en la entrega de las calificaciones de los funcionarios, fueron los siguientes:

a) Reconocimos que el razonamiento jurídico no era de modo alguno fácil, porque, como señala un documento de la Red Iberoamericana de protección de datos personales del año 2005[224], junto a un supuesto consenso generalizado en apoyo a la protección de los datos personales de los empleados públicos en la medida que ello no impida sus rendiciones de cuentas administrativas, hay quienes consideran que un funcionario público debe renunciar a su derecho a la privacidad en *pro* de la transparencia aún cuando no se trate de datos personales inherentes al cargo que desempeña.

b) Entendimos que un funcionario público en Chile sólo excepcionalmente y por ley renuncia a su derecho a la privacidad en *pro* de la transparencia, al tenor de los artículos 5°, 7°, 10°, 21 N°2 y N°5 y 33 letra m) de la ley 20.285, de la ley 19.628 y del artículo 19 N°4 de la CPE. Un funcionario público chileno, por el hecho de desempeñarse en la Administración Pública no puede entenderse que pierde o que ve esencialmente disminuidos sus derechos fundamentales, y toda restricción o limitación legal deberá cuidar de no entrabar esencialmente el ejercicio de su derecho a la privacidad y de su derecho a la protección de sus datos personales.

---

[223] Recuérdese que el a*rtículo 10 de la ley 19.628 señala que no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos de salud necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.*

[224] Véase la URL https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/IV_Encuentro/common/pdfs/MexicoAccesodefinitivo.pdf

c) No nos pareció esencial al análisis considerar la petición de los números de RUT de los funcionarios públicos, sino que debía tenerse presente que ello se hacía en asociación con sus calificaciones administrativas. La solicitud de acceso también podría hacerse pidiéndose la asociación de las calificaciones a los nombres y apellidos de los funcionarios, pero precisamente, se hacía en relación al elemento indexador RUT porque es mucho más preciso y exacto, y porque luego puede ser asociado, fidelizado, relacionado y procesado computacionalmente con otros antecedentes disponibles en otras bases de datos[225]-[226].

d) Tuvimos presente que los mencionados eran datos generados por una entidad pública en el ejercicio de sus competencias, que no se solicitaban en forma innominada o estadística. Si así hubiera sido, o se resolviera que procede su entrega de manera que no sea factible identificar al funcionario calificado, se terminaba el problema de resguardar esfera privada alguna -en los términos del artículo 21 N°2- de un funcionario público. Si se hubiera solicitado la información anterior no asociada con el RUT o con los nombres y apellidos de los funcionarios, no habría problema alguno en transparentar -por ejemplo- que "x cantidad" de funcionarios fue calificada en Lista 1, otro tanto en Lista 2, y sólo "x" en Lista 3.

e) Que las referencias a *cualquiera otra información* de los artículos 5 inciso segundo y 10 inciso segundo de la ley 20.285 no podía ser extensiva a los datos personales o nominativos, ni de los ciudadanos ni de los funcionarios públicos, en caso de una solicitud en sede de transparencia pasiva. De acogerse una interpretación en sentido contrario, se violarían la ley 19.628 y el artículo 19 N°4 de la CPE.

f) Que las referencias en sede de transparencia activa y sin que medie una petición previa y expresa de acceso, transparencia o publicidad a las remuneraciones o sueldos *"de los funcionarios"* y a las nóminas *"de los ciudadanos beneficiarios de programas sociales"* -que son datos personales según la ley 19.628- debían ser consideradas excepcionales y de aplicación restrictiva.

g) Que el interés del legislador de la ley 20.285 por proteger los datos personales y la privacidad, en la búsqueda del equilibrio necesario, quedaba *"aún*

[225] Por cierto, si nos ponemos en la hipótesis de no entregar la información solicitada asociándola a un RUT o a un nombre propio, nos desplazaríamos al ámbito de la información estadística. Y acá, al ser data personal pero innominada o desagregada, no tiene aplicación alguna la institucionalidad jurídica de la protección de datos personales o de la ley 19.628.

[226] Lo relevante para la resolución del Consejo de Transparencia debía ser la consideración del dato personal o nominativo *"calificación de un funcionario público"*, y si se decidía acceder al reclamo de amparo y entregar en forma sistematizada las calificaciones de muchos funcionarios recibidas en un lapso determinado, esa información nominativa o personal debió ser entregada asociándola a un número de RUN o de RUT, porque así lo exige un Decreto Número 18 del año 1973.

más claro" en conformidad al inciso que en la letra i) del artículo 7° precisaba que a propósito de la publicación de los beneficiarios sociales no se incluirán los datos sensibles, esto es, los 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 los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) Que la causal de rechazo del artículo 21 número 2, al establecer las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, aludía a derechos de las personas como su seguridad, su salud o la esfera de su vida privada, y por ende debía ser considerada como la regla general desde la perspectiva o tratándose de la eventual comunicación, publicación o conocimiento por terceros de datos personales o nominativos, resultando aplicable tanto *"a los ciudadanos"* como *"a los funcionarios públicos identificados en cuanto a su calificación administrativa",* porque la ley no distinguía.

i) Que debía entenderse que, si bien por regla general en materia del acceso de la ley 20.285 el Consejo no había exigido expresión de causa o motivo para los peticionarios, *si debía concurrir un interés legítimo y público acreditado y demostrado para una petición administrativa general y no referida a un caso concreto en que se cuestionara el desempeño de un funcionario determinado* (porque el recurrente de amparo no lo había invocado así), cuando se refería a datos personales de los funcionarios y considerando supletoriamente las exigencias los artículos 1° inciso 1ro, 18° inciso 1ro y 21 N°1 de la ley 19.880 -sobre Bases de Procedimientos Administrativos-, para integrar las disposiciones de la ley 20.285.

j) Que no afectaba a las conclusiones anteriores el que según el Estatuto Administrativo las calificaciones son información elaborada con presupuesto público, que se trata de una materia propia de la competencia de todo servicio público, y que existe la obligación de cumplir con la calificación. Esto abona el principio general del artículo 20 de la ley 19.628, que establece que un servicio puede procesar o tratar datos de las personas cuando caiga bajo su competencia privativa de Derecho Público -misma que ahora determina el Estatuto Administrativo- y conforme a las funciones que esa competencia implique, pero no se podía concluir que la existencia de esta carga u obligación habilitaba para que posteriormente el servicio pueda comunicar los resultados a terceros carentes de interés legítimo, que las actas de calificación estarían en bases de datos públicas, que las calificaciones no son parte de la esfera privada de un funcionario, y que los artículo 5° y 10° de la ley 20.285 así lo permitirían expresamente.

k) Que en términos del artículo 8° de la CPE, procedía la reserva o secreto porque la publicidad del detalle de las calificaciones afectaría los derechos de los funcionarios públicos establecidos en el artículo 19 N°4 de la Constitución y en la

ley 19.628 y su entrega, sin exigencia previa ni acreditación de un legítimo interés, sería un abuso del derecho que posee el peticionario y recurrente de amparo en conformidad a la ley 20.285, solicitud que -a nuestro entender- no apuntaría al objetivo constitucional de permitirse la transparencia en el uso de recursos públicos y de evitarse la falta de probidad en la Administración del Estado.

l) Que para determinar el eventual beneficio público de transparentar las calificaciones de los funcionarios y de llevarlas desde la esfera privada a la esfera social o pública, debía explorarse el resultado de realizar un *"test o prueba de interés público"*. Esto es, el analizar si por la importancia del problema o de la información solicitada debía prevalecer el interés público por sobre los intereses individuales de los funcionarios calificados, o dicho de otra forma, si la apertura de la información sobre su desempeño era un bien superior al perjuicio que se ocasionaría por mermar su esfera privada o su derecho a la privacidad. Pero este procedimiento, según al parecer establecen las normas comparadas de derecho de acceso -que no hemos tenido a la vista-, debería realizarse no de oficio sino a petición la parte interesada y recurrente de amparo, lo que no se había verificado.

m) Un punto de contacto esencial: …que al resolver una reclamación o solicitud de amparo de los artículos 8 (Transparencia Activa) o 24 (Transparencia Pasiva) de la ley 20.285, el Consejo debía tener presente que al mismo tiempo debía velar porque los servicios públicos cumplieran con o aplicaran la normativa de la ley 19.628, porque así lo establece expresamente el artículo 33 letra m. Ergo, al tenor de la ley 19.628, debía considerarse:

(i) que las bases de datos personales del MINVU y de FONASA no eran fuentes de acceso público o accesibles al público (artículo 2°) sino que eran de acceso restringido o reservado a los solicitantes, salvo, por cierto, que la petición se haga por el propio titular, únicamente respecto de sus propios antecedentes, y ejerciendo el derecho de acceso o habeas data del artículo 12°.

(ii) que los órganos implementan y administran las bases de datos y procesan (o tratan) los datos personales *"de los funcionarios"* y *"de los ciudadanos"* porque leyes especiales como la 19.628 y sus leyes orgánicas los facultan -artículo 4°-, sin que deban pedirle autorización previa, expresa y por escrito ni a los ciudadanos ni a los funcionarios;

(iii) que al hacerlo, como responsables de bases de datos no accesibles al público, regía para ellos la obligación de secreto del artículo 7°;

(iv) que los órganos MINVU y FONASA debían usar esos datos sólo para los fines para los cuales fueron recolectados -artículo 9°-;

(v) que los órganos MINVU y FONASA no podían transmitir en forma electrónica los datos personales sobre calificaciones de los funcionarios existentes en sus bases, porque ello no guardaba relación con sus fines y tareas de servicio

público y porque no tenían expresamente asignada la competencia de Derecho Público para hacerlo -artículo 5°-;

(vi) que los órganos MINVU y FONASA debían procesar o tratar los datos personales sólo respecto de materias de su competencia -artículo 20°-, y no existen normas de Derecho Público que les asignen competencia para ser proveedores de la información referida a sus funcionarios (salvo que se haga en forma innominada o estadística) o que, incluso, les permitan vender sus bases de datos;

(vii) que la ley 20.285 no primaba por especialidad, como para entender que ella los obliga a entregar datos personales de funcionarios o de ciudadanos identificados nominativamente a terceros diversos de los funcionarios o de los ciudadanos, sin que primero obtengan la autorización expresa, por escrito, fundada e informadamente que exige el artículo 4° de la ley 19.628;

(viii) que con un criterio interpretativo que no proteja "las características morales" involucradas dentro de los factores de calificación de los funcionarios (v.gr. interés por el trabajo realizado, liderazgo, capacidad para trabajar en equipo), podrían terminar entregándose las calificaciones y también los informes psicológicos a un peticionario que ni siquiera acredita un interés legítimo para solicitar esta información, con lo cual, se les podría estigmatizar ante terceros e influenciar o generarse eventualmente malas o erradas convicciones en los posible futuros empleadores del funcionario, discriminándose en su derecho de acceso al trabajo; y,

(ix) que de no respetarse las normas anteriores, los órganos incurrirían en responsabilidades de Derecho Público en conformidad a los artículos 11 y 23, y eventualmente procedería la indemnización de perjuicios.

2.4 Empero, en definitiva el Consejo resolvió la entrega de las calificaciones y acoger parcialmente el amparo interpuesto. Se basó para ello en que no se había cuestionado que las calificaciones si eran información pública, y que lo objetado era la entrega porque la data no estaba disponible como se pedía (en una hoja de cálculo con varias columnas); que tanto el proceso de calificaciones como el escalafón que se forma y se envía a la Contraloría General contenía toda la información solicitada, aunque en un formato diverso al solicitado y sin incluir a los funcionarios a contrata; que la entrega de la información no distraería indebidamente a los funcionarios; y, muy especialmente, porque no había duda del interés público que tienen las calificaciones funcionarias como mecanismo de rendición de cuentas no sólo ante las jefaturas sino también ante la sociedad.

El Consejo resolvió (Considerando Doce) que a pesar del interés público que tenía la entrega de las calificaciones funcionarias, algunos argumentos debían formularse en consideración a la ley 19.628 y matizarse tratándose del número de

"RUT" de los funcionarios y ex funcionarios públicos, requerido por el solicitante, el que no debía entregarse. Tuvo presente la naturaleza de dato personal de las calificaciones, que por el artículo 4° y el 20° el MINVU y FONASA podían procesar, y la obligación de secreto del artículo 7°.

Se percibió que si una persona había estado interesada en acceder a ser funcionario público y que a ese efecto -por exigirlo el artículo 13 del Estatuto Administrativo- la entrega de sus antecedentes personales debía hacerse porque estaba obligado, en el sentido que lo permite el artículo 4° de la ley 19.628, el Consejo estimó que el dato RUT no se había obtenido directamente de un registro público y por ende legalmente se mantenía en los sistemas del MINVU y de FONASA sólo para su tratamiento administrativo al interior del servicio público respectivo y no para su cesión a terceros.

3. *Los números de RUT "de los funcionarios públicos" deben ser mantenidos en reserva al momento de entregar otros antecedentes relacionados (DA N°A10-09 y N°A126-09),* en coincidencia con la norma que en sede de transparencia activa obliga a informar los datos personales sobre remuneraciones de los funcionarios asociados sólo a sus nombres y apellidos.

Las consideraciones en sede de la ley 19.628 tenidas en vista fueron: que el RUT era un código numérico creado con el fin de identificar a los contribuyentes del país; que se trataba de un dato de carácter personal en conformidad a la ley 19.628, cuyo tratamiento sólo puede efectuarse cuando dicha ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello; que quienes trabajen en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público; que el tratamiento de datos personales por parte de un organismo público sólo podía efectuarse respecto de las materias de su competencia....; y que el RUT no estaba disponible en fuentes de acceso público.

En todo caso y cuanto al dato de los RUT de los funcionarios públicos del MINVU y de FONASA calificados, creemos que el Consejo no reparó en los siguientes aspectos:

a) Que los RUT de los funcionarios públicos que obran en poder de los respectivos servicios donde se desempeñan se obtiene de manera directa, no sólo por la mera voluntad o consentimiento del empleado público que postula al cargo -lo que podría entenderse como una autorización tácita derivada del haber postulado a ser contratado y que se refiere sólo a la posibilidad de que se registren los antecedentes nominativos-, sino además por una exigencia legal del Estatuto Administrativo que obliga a su entrega y registro al momento de ser contratados. Así considerado, cabe concluir que los órganos de la Administración no acceden a los RUT y a los restantes antecedentes identificativos desde fuentes

de datos personales accesibles al público, en el sentido de aquellas a que alude el artículo 2° de la ley 19.628; y,

b) Que por el hecho de ser contratados los funcionarios y estar disponibles sus RUT (y otros datos personales) en los sistemas o bases de datos del servicio, ellos no se transforman en parte de fuentes de datos personales de acceso público ni pasan a ser de propiedad del órgano, quien sólo es un mero poseedor. Ergo, si su comunicación o cesión a terceros particulares que lo requieran no ha sido expresamente permitida o establecida como de su competencia por normas del Derecho Público Constitucional o Administrativo, y se aparta de los fines que motivaron su recogida, recopilación y registro, se requeriría autorización expresa del funcionario para comunicar o ceder el RUT asociado a su calidad de funcionario (esto, aplicando la regla general de los artículos 4° y 20[227] de la ley 19.628)[228].

4. *Respecto "de los ciudadanos" algunos datos personales como los números de RUN o de RUT también deben ser tachados al momento de entregarse la información solicitada (Decisión de Amparo N°A33-09).*

El amparo fue interpuesto por una persona para solicitar copia de la red familiar del causante de una herencia que se había denunciado como vacante, en contra de la Subsecretaria de Bienes Nacionales.

El Consejo, tras analizar un Oficio del Servicio de Registro Civil que informó *"la red familiar de ese causante",* constató que el documento contenía datos personales de los integrantes de dicha red, concretamente sus (I) *números de RUN,* (ii) su *domicilio* y (iii) los *datos de algunas inscripciones de matrimonio y de nacimiento*.

En base a las normas de la ley 19.28, que el Consejo debe hacer aplicar en conformidad al artículo 33 letra m) y que regula los antecedentes nominativos tratados computacionalmente que pueden formar parte de la esfera privada de una persona (lo que además configura o materializa la causal de reserva del 21 N°2 de la ley de acceso y transparencia), determinó que el RUN y el domicilio de los terceros que constaban en la red familiar en poder de la Subsecretaría de Bienes Nacionales no provenían ni habían sido recolectados de las *"fuentes accesibles al público"* a que alude el artículo 2° de la ley de protección de datos. Como a ellos

[227] El artículo 20 dispone que *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.*

[228] Cuestión diversa será cuando el requerimiento de los RUT lo realice otro servicio público, ante lo cual y en conformidad al artículo 5° de la LBGAE debe considerarse la viabilidad de colaborar con él y entregar los RUT, o cuando se entregue en virtud de un convenio de intercambio que persiga fines de servicio público o de mejor funcionamiento de la Administración del Estado.

sólo puede accederse con la autorización de su titular o cuando la ley lo permite -y no existe ley expresa que obligue a dar a conocer ni el RUN ni el domicilio de una persona-, en definitiva se dispuso el acceso a la información solicitada pero *"tachándose u ocultándose"* estos dos datos.

5. *Los datos personales "de aquellos ciudadanos que estén optando a cargos de funcionarios públicos" deben ser transparentados (Decisiones de Amparo N°A29-09 y A35-09).*

5.1 Como ya anticipamos, en la *Decisión de Amparo N°A29-09* el Consejo ha considerado tener competencia para conocer del reclamo respecto de los datos personales de un solicitante, *con la muy especial 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, los que habían sido parte de los fundamentos tenidos en vista en un proceso administrativo de postulación a un cargo en un servicio público y para la dictación del acto administrativo final de selección.

Citamos: *"…el solicitante requería los resultados de su evaluación personal en el proceso de selección implementado para proveer el cargo de Jefe de Cobranzas y Quiebras de la Tesorería General de la República. La Dirección Nacional del Servicio Civil (DNSC) invocó la causal constitucional de afectación de los derechos de las personas, prevista también en el artículo 21 N°2 de la Ley de Transparencia, argumentando que el titular de los informes psicolaborales no sería el postulante a que se refieren, sino la autoridad que solicitó la asesoría profesional para efectuar dicha evaluación*".

En la Decisión en comento el Consejo estableció que aunque el informe fue encargado por la Dirección el titular de los datos allí contenidos era la persona a que se refieren dichos datos, en este caso, el postulante requirente, e hizo aplicación expresa de la norma que conforme al artículo 33 letra m) está llamada a velar porque se aplique, por cierto al conocer de las materias propias de su competencia. Así, aplicándose el artículo 2° letra ñ) de la ley 19.628, que entiende por titular de los datos a la persona natural -identificada e identificable- a la que se refieren los datos nominativos, resolvió que el solicitante y requirente de amparo tenía derecho a conocer su evaluación personal, con excepción o excluyéndose las referencias a terceros o a los otros postulantes.

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. En este particular y excepcional caso, donde no se estaba invocando 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, al solicitante y recurrente de amparo -titular de los datos

que eran parte de su "*esfera privada"*- no podría aplicársele la causal de reserva o secreto del artículo 21 N°2, y el Consejo determinó la procedencia de la entrega de la información.

En nuestra opinión, si la ley 20.285 hubiese sido usada por el titular de los datos personales sólo para acceder a información personal que obraba en poder del organismo público, sería una opción jurídicamente cuestionable, y tanto el órgano requerido como el Consejo de Transparencia deberían haberlo puesto de relevancia y haberse abstraído de conocer el asunto. En la especie, se pidieron los fundamentos del acto administrativo que cerró un proceso de selección de personal y no directamente los datos personales del postulante.

Haciendo aplicación de la normativa relativa a la protección de datos, el Consejo determinó que es claro el artículo 2° ñ) de la ley N°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.

¿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 N°2[229] *y denegado el acceso a la información?.*

5.2 *Amparo al derecho de acceso a la información interpuesto en 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 N°A35-09).*

Respecto de los dos postulantes que no se opusieron a la entrega de su identidad ni informaron el traslado que les fue conferido en conformidad al artículo 20 de la ley 20.285, el Consejo estimó, "*en principio",* que podría aplicarse el artículo 7° de la ley 19.628 y declarar que sus identidades eran reservadas.

Pero, teniendo a la vista el inciso final del artículo 20 de la ley de acceso y transparencia, que 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 ella accede a la publicidad de la información, esta norma era la que debía preferirse y aplicarse en este caso, (i) por su especialidad y (ii) por el interés público existente en conocer el funcionamiento de este servicio público, ya que no se trataba de la

[229] 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.

identidad de cualquier postulante sino, específicamente, de la de aquéllos que fueron propuestos para ser elegidos por el Comité de Selección de directivos.

En su fallo el Consejo, *"…agrega que la conclusión anterior cambiaría tratándose del silencio de postulantes que no fueron incluidos en dicha nómina de candidatos, porque en este supuesto el Consejo estima que aplicando un test de daño o interés público prevalecería la reserva del dato personal sobre su publicidad, porque la difusión de tales identidades contribuiría escasamente a conocer el fundamento de la decisión adoptada. En esa hipótesis, el Consejo, en caso de silencio, estima que debiera preferirse el artículo 7° de la ley 19.628 por sobre el inciso final del artículo 20 de la ley de acceso y transparencia"*[230].

6. *Negativa de entregarse datos personales "de los ciudadanos" porque la publicidad, comunicación o conocimiento datos personales puede afectar derechos de terceros, trabajadores denunciantes o de los que han prestado declaración ante la Inspección del Trabajo* (*Decisión de Amparo N°A53-09).*

En este caso el solicitante presentó amparo al derecho de acceso a la información por haberle sido denegado el acceso a la copia de los expedientes relativos a las multas cursadas en su contra, por la Dirección del Trabajo.

El Consejo estimó que la confidencialidad en este procedimiento de fiscalización sólo regía durante su tramitación, pero consideró que *"cierta parte de la información contenida en los expedientes solicitados por el reclamante*" podrían contener datos personales de terceros, que deberían ser protegidos de acuerdo a los artículos 2°, 4°, 7°, 10° y 20° de la ley 19.628.

Si bien es cierto se consideró que no se podía desconocer la naturaleza especial de las denuncias realizadas por los trabajadores ante la Dirección del Trabajo, existía el riesgo derivado de que tanto su divulgación como la de la identidad de los denunciantes o la de los trabajadores que habían declarado en un proceso de fiscalización en contra del empleador, afectara su estabilidad en el empleo o los hiciera víctimas de represalias, sobre todo si se mantenían laboralmente vinculados con el empleador denunciado.

"Por consiguiente, dispuso que, respecto de aquellos datos personales señalados, cabe entender que la publicidad, comunicación o conocimiento de dicha información puede afectar derechos de terceros —en el caso en análisis de los trabajadores denunciantes o de los que han prestado declaración—, en

[230] Tomado de la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

particular tratándose de la esfera de su vida privada y sus derechos de carácter económico emanados de la relación laboral, configurándose de esta forma y respecto de aquellos datos la causal del artículo 21, numeral 2 de la ley de acceso y transparencia, causal que se encuentra reforzada por la especial función que el artículo 33, letra m), de la Ley de Transparencia, encomienda al Consejo, en orden a velar por el adecuado cumplimiento de la ley 19.628 por parte de los órganos de la Administración del Estado"[231]*.* Efectivamente, como ya analizamos en el Acápite F de esta Segunda Parte, el artículo 33 letra m) "refuerza" o hace aún más importante la causal del 21 N°2.

[231] Tomado de la URL http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

REFERENCIAS BIBLIOGRÁFICAS

AUTORES - DOCUMENTOS

JIJENA LEIVA, Renato, Chile, *La Protección Penal de la Intimidad y el Delito Informático*, Editorial Jurídica de Chile, 1992.

JIJENA LEIVA, Renato, *"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 N°19.628 sobre protección de datos de carácter personal, Cuadernos de Extensión Jurídica 5, Facultad de Derecho Universidad de Los Andes, año 2001.

MENDOZA ZUÑIGA, Ramiro, *"Régimen de los bancos de datos de organismos públicos. Una aproximación del Derecho Administrativo a la ley sobre protección de la vida privada";* en Estudios sobre la Ley N°19.628 sobre protección de datos de carácter personal, Cuadernos de Extensión Jurídica 5, Facultad de Derecho Universidad de Los Andes, año 2001.

MINSEGPRES, CERDA Alberto y otros; 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*.

PUCCINELLI, Oscar, *El Habeas Data en Indoiberoamérica*; Editorial Temis, Colombia, 1999.

SOTO VELASCO, Sebastián; *"Ley de Transparencia: desafíos en su aplicación*"; en Revista Temas de la Agenda Pública, Año 4, N°30, de septiembre del 2009.

VAN WEZZEL, Alex, "*Privacidad y publicidad de las deudas tributarias",* en Informativo Jurídico de la Editorial Jurídica de Chile, N°40; de Junio del 2007.

PRINCIPALES URLS CONSULTADAS

http://www.habeasdataorg.cl

http://www.soteder.blogspot.com

http://www.estrategiadigital.gob.cl/files/Guia_Metodologica_PMG_Gobierno_Electronico_2009.pdf

http://www.redipd.org/reuniones/encuentros/IV/index-ides-idphp.php y http://www.redipd.org/reuniones/encuentros/IV/common/mexico_acceso_definitivo.

pdf , donde se encuentra disponible 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.

http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html

Santiago, Diciembre del 2009.