Minuta

Consideraciones jurídicas sobre los datos RUN y RUT, asociados con otros datos personales como las calificaciones de los funcionarios públicos y en el contexto de un recurso de amparo al derecho de acceso.

Sumario.

I. Contexto general.

La presente minuta se desarrolla, conceptualmente, en el contexto más amplio 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 *del año 2008*, 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*.

El derecho de acceso que todos los ciudadanos poseen reconocido constitucional y legalmente para conocer los actos, contratos, resoluciones y documentos del Estado, *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 tratándose de sus datos y antecedentes personales y nominativos[1]-[2].

Hay ideas centrales sobre las cuáles reflexionar de cara al necesario equilibrio o conciliación, no en esta minuta y que pueden o no compartirse; a saber: ...la protección de datos personales de los funcionarios públicos y de los ciudadanos debe ser un límite al derecho de acceso a la información, pero considerando caso a caso y la especial naturaleza del dato personal involucrado; ...las leyes de acceso a la información necesariamente deben ser compatibles con las de privacidad y datos personales; ...la protección de datos personales no debe usarse manera general y sistemática para no abrir información del Estado, ya que la restricción al acceso de ciertos y determinados antecedentes referidos 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.

En Chile es 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 los datos personales se incluyen junto a los actos, contratos, resoluciones y documentos que deben ser públicos al estar en poder de los servicios públicos.

En segundo lugar, 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 -incluso con una carga legal expresa de secreto en su artículo 7°- para proteger a los titulares de los datos personales procesados computacionalmente, sean de los ciudadanos, sean de los funcionarios públicos.

Pero a las dos interpretaciones anteriores (si se entiende 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 el artículo 21 N°2 y el 33 letra m) de la ley 20.285, 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.

---

[1] El derecho de acceso a los actos, contratos y documentos en poder del Estado un tema relevante y esencial para las Sociedades del Siglo XXI, pero que no debe ser confundido con la garantía del *"Habeas Data"* y con el principio de la "*Autodeterminación Informativa"* que amparan, desde fines de la década del 70 en el Derecho Comparado, el derecho de cada persona para controlar y decidir exclusivamente sobre el procesamiento de sus datos personales y nominativos, sea por entes estatales o por empresas particulares.

[2] Es *el artículo 12 de la ley 19.628 el que consagra el llamado Derecho de Acceso, Habeas Data o Habeas Scriptum*, una garantía sólo de rango legal y procesal que vino a desarrollar la garantía del respeto y protección de la vida privada que contempla el artículo 19 N°4 de la Constitución Política. Por su intermedio cada titular puede requerir a quien sea "responsable de una base o banco de datos" 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 los sensibles o referidos a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como 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.

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

II. Consideraciones jurídicas sobre los datos RUN y RUT.

1. *Categorías conceptuales esenciales*.

Un *"dato"* es, en el ámbito de la Teoría General de Sistemas, un antecedente que da cuenta de un hecho o de una característica determinada. El conjunto organizado de datos constituye *"información"*. Un dato es *"personal o nominativo*", cuando permite identificar cualquier característica de una persona para relacionarse en sociedad. Y un dato personal o nominativo puede ser de mayor importancia o "*sensibilidad"*, en consideración a su especial naturaleza y como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, los datos biométricos (v.gr. huella digital), las acciones que se poseen, los impuestos pagados, etcétera.

2. *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 -con poco margen de duda- que se alude a una persona determinada, identificada e identificable. Lo mismo vale para el denominado "RUT", que analizamos más abajo.

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 la ley los faculta para hacerlo.

Del mismo modo, 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 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.

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 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 SRC 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.

Un dato a ser tenido presente: las personas jurídicas sólo poseen número de RUT.

3. *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 *es 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.

Téngase presente: del hecho de que sea público no puede concluirse que al estar sistematizado, indexado, cruzado, relacionado o fidelizado en una base de datos de un órgano del Estado, la totalidad de la base de datos de RUT tendría la calidad de *"fuente accesible al público*" o de *"fuente pública de información".*

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.

4. *Ambos son datos personales o nominativos que permiten general información de la misma naturaleza*.

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 física o natural (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?. 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[3].

¿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 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 tributaria en particular -así lo establecen las normas que lo crean- el dígito identificador

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

que los denomina e individualiza, con poco margen de dudas, sería un atributo de su personalidad[4].

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. 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. 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.*

Para terminar: RUN y RUT 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. <u>*Competencias de los servicios públicos en el contexto de la ley 19.628*</u>.

Su señalamiento es especialmente importante para las funciones y resoluciones del Consejo de Transparencia, porque el artículo 33 letra m de la ley 20.285 establece que

[4] Más arriba consignamos que 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", que analizamos más abajo.

este órgano debe velar por el cumplimiento de la ley 19.628 al interior de la Administración del Estado, lo que, por aplicación de un *Decreto Supremo N°100*, se extiende incluso a la definición de las políticas de privacidad de los sitios WEB de los servicios públicos.

(i) *Sólo pueden procesar todo tipo de datos personales de los ciudadanos y de sus funcionarios, como ocurre con los ahora referidos RUN y RUT considerados en forma aislada o relacionados con otros antecedentes*, actuando dentro de su competencia de Derecho Público y para fines de servicio público (artículo 20); tal es el caso, por ejemplo, del servicio de verificación de vigencia de RUT que realiza por Internet el SII para velar por el orden público económico en materia tributaria, para proteger la fe pública y evitar la existencia de facturas falsas.

(ii) Los servicios públicos sólo pueden procesar, tratar, comunicar o publicar los datos RUN y RUT porque una ley los faculta expresamente, o porque, no habiendo autorización legal, previamente obtienen autorización expresa y fundada para ser entregados asociados al nombre del ciudadano -o del funcionario público que trabaja en ellos-, titulares y propietarios[5] de los datos personales o nominativos (artículo 4°);

(iii) 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 (artículo 9°[6]), lo que es un principio esencial en materia de protección de datos personales desde fines de la década de los 70; *así por ejemplo, los hospitales públicos no pueden usar los datos personales de sus pacientes para afiliarlos a un partido político o a un movimiento anti VIH; el MINVU no puede usar los datos de los beneficiarios de subsidios de vivienda para ofrecerles seguros de vida en conjunto con una empresa particular; y el Mideplán no puede usar datos de becarios de la Fundación Chile para en conjunto con una línea aérea ofrecerles pasajes rebajados.*

(iv) El procesamiento de datos personales genera la necesidad de cumplir con la obligación de secreto para los responsables de las bases de datos que expresamente establece la ley (artículo 7°), y que de ser vulnerado por el responsable configura el delito informático del artículo 4° de la ley 19.223; salvo, que la base de datos no sea de acceso restringido, reservado o secreto y pueda por ende legalmente calificarse como *"accesible al público"*; y,

(v) 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 por el sólo hecho de serlo -sin necesidad de acreditar o manifestar interés legítimo pero sin que puedan entrabar la gestión de la Administración del Estado- (artículo 12°[7] y 15°[8]), salvo que provengan de fuentes accesibles al público.

---

[5] 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.

[6] *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.*

[7] *Artículo 12. Toda persona tiene derecho a exigir a quien sea responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.En caso de que los datos personales sean*

(vi) Los *RUT de los funcionarios públicos* que obren 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 puede entenderse como una autorización derivada del haber postulado a ser contratado y que se refiere sólo al 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.

Por cierto que los antecedentes sobre el funcionario, por ejemplos penales o de aquellos que son mencionados en el certificado que al efecto entrega el SRC, pueden ser verificados u obtenidos desde otros servicios públicos o desde otras fuentes de información. De ser así, no podría entenderse que por estar disponibles en la sociedad para su consulta se deriva que un servicio público puede procesarlos, cruzarlos u operar con ellos a su discrecionalidad; obsta a este criterio la institucionalidad jurídica de protección de datos que exige una finalidad de orden y de servicio público para el actuar de los órganos del Estado.

(vii) 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[9] de la ley 19.628)[10].

Como ya anticipamos y como veremos a propósito de los datos personales *"calificaciones de los funcionarios"*, entendemos que al tenor de los artículos 5°, 7°, 21 N°2 y 33 letra m) de la ley 20.285, de la ley 19.628 y del artículo 19 N°4 de la CPE, debe concluirse que *por*

---

erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. 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.

[8] *Artículo 15. 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.*

[9] 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.*

[10] 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.

sobre el derecho de acceso ejercido por un peticionario particular de la ley 20.285 prima el de la protección de los datos personales de los funcionarios, quienes no pierden ni ven esencialmente disminuidos sus derechos fundamentales ni pierden a este respecto un ámbito de esfera privada por el sólo hecho de ser empleados de la Administración del Estado.

6. *Acerca de la importancia del concepto "fuentes accesibles al público" o fuentes públicas de información personal o nominativa, no restringidas ni reservadas a un solicitante*.

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".* Por sus deficiencias, ambiguedades y posibles inconstitucionalidades, existe un proyecto en trámite que apunta a reemplazarlo y asignarle el debido alcance y naturaleza al concepto[11].

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. A modo de ejemplo, las bases de datos personales del SII o del SRC 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 tratándose las rentas de los contribuyentes, salvo, respecto de los antecedentes personales que pueden obtenerse por la vía de los certificados y porque la ley los obliga a entregarlos a los ciudadanos y a los contribuyentes.

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 puede 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 (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 el secreto bancario, el secreto tributario, el secreto estadístico, el secreto profesional y el secreto de filiación política, puede considerarse que todas las restantes fuentes o bases de datos personales serán de acceso público o no restringido o reservado, aplicando el principio de que en Derecho Privado puede hacerse todo aquello que no esté expresamente prohibido.

---

[11] El artículo, una vez modificado en la forma propuesta, 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.

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

Junto con no existir una prohibición expresa de procesar, *"tratar"*[12]*, 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.

Esto está, por ejemplo -y sin realizar un juicio de valor al respecto-: (i) expresamente permitido al SRC, que puede comercializar certificados referidos al estado civil de los ciudadanos como una de sus competencias esenciales de servicio público; (ii) la ley obliga a los municipios a exhibir públicamente el avalúo de los predios y bienes raíces; y, (v) está expresamente permitido que el SII verifique, a requerimiento de un ciudadano, la pertenencia del RUT a un contribuyente que ha emitido una factura, que podría no ser verdadera (falsa) o emitida usando un RUT falso o errado.

III. Aplicación concreta de los criterios anteriores al caso del recurso de amparo interpuesto contra el MINVU y FONASA, en el contexto de la ley 20.285 y para acceder al dato personal *"calificaciones de los funcionarios públicos".*

1. *Planteamiento del tema.*

Este razonamiento jurídico no es de modo alguno fácil. Como señala un documento de la Red Iberoamericana de protección de datos personales del año 2005[13], 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.

Este segundo criterio no sería a nuestro parecer aplicable a Chile, al tenor de los artículos 5°, 7°, 21 N°2 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

[12] La ley define también lo que es el *"tratamiento de datos personales"* en la letra o) del artículo 2°, para afirmar que consiste en *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.*

[13] Véase la URL https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/IV_Encuentro/common/pdfs/MexicoAccesodefinitivo.pdf

esencialmente el ejercicio de su derecho a la privacidad y de su derecho a la protección de sus datos personales (Artículo 19 N°26 de la CPE).

2. *No es esencial al análisis considerar la petición de los números de RUT de los funcionarios públicos, sino que debe tenerse presente que ello se hace en asociación con sus calificaciones administrativas*.

La solicitud de acceso podría hacerse pidiéndose la asociación de las calificaciones a los nombres y apellidos de los funcionarios, pero precisamente, se hace 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. Dicho de otra forma, pueden existir dos personas llamadas "*Rosa Gomez Perez"* pero nunca existirán dos números de RUT similares, con lo cual la base de datos se implementará *"sin ruidos"* o sin que sobren datos y *"sin silencios"* o sin que ellos falten.

Si nos ponemos en la hipótesis de no entregar la información solicitada asociándola a un RUT, 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.

3. *Las bases de datos con las calificaciones de los funcionarios públicos no pueden ser consideradas como accesibles al público, al tenor de la ley 19.628, sino como de acceso reservado.*

Nos remitimos a lo desarrollado en el numeral 6 del acápite anterior.

4. *Razonamiento jurídico para considerar la necesidad de rechazarse el amparo y no acceder a la entrega de la información solicitada.*

a) *Supuesto o hipótesis de análisis*: ...al MINVU y a FONASA se le han solicitado 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 solicitan en forma masiva y nominada o identificada a un funcionario determinado las calificaciones de todo el personal y ex-funcionarios del MINVU y FONASA desde el 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 solicita incluir la tabla de calificaciones y los rangos de inicio y término de cada lista de calificación.

Los mencionados son datos generados por una entidad pública en el ejercicio de sus competencias, que no se solicitan 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 termina el problema de resguardar esfera privada alguna 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.

No se le han solicitado datos relacionados *"con los ciudadanos"* adscritos a su gestión y competencia.

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[14], 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 de moda*- el contenido de sus correos electrónicos funcionariales[15].

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 contratada -planta, a contrata, a honorarios- en sede de transparencia activa, los datos de salud son sensibles y reservados[16], sus declaraciones de impuestos son secretas -como las de todos los contribuyentes-, 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, *este análisis jurídico se inclina por su reserva y la improcedencia de ser revelados en sede de la ley 20.285.*

La conclusión sería diversa, en primer lugar, si nos trasladamos al ámbito de la información meramente estadística o innominada, y nada se pidiera al MINVU y a FONASA atribuido o identificado con un funcionario determinado, sea por su RUT, sea por sus nombres y apellidos. Y la conclusión podría ser diversa, en segundo lugar, 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.

b) Las referencias a cualquiera otra información de los artículos 5 inciso segundo y 10 inciso segundo de la ley 20.285 no puede 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.

---

[14] En Argentina, por ejemplo, en un Municipio debe emplearse al menos a un 4 % de discapacitados.

[15] Este es un tema que debiera ser objeto de otro análisis, y que ya hemos estudiado informalmente para el Ministerio Público a propósito del acceso a los servidores de correos del Ministerio del Interior.

[16] 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.*

c) Las referencias en sede de transparencia activa y sin que medie una petición previa y expresa (artículo 7° de la ley 20.285) 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- deben ser consideradas excepcionales y de aplicación restrictiva.

El interés del legislador de la ley 20.285 por proteger los datos personales y la privacidad, en la búsqueda del equilibrio necesario, queda aún más claro en conformidad al inciso que en la letra i) del artículo 7° precisa 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.

d) 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 alude a derechos de las personas como su seguridad, su salud o la esfera de su vida privada, y por ende *debe ser considerada como la regla general tratándose de la eventual comunicación, publicación o conocimiento por terceros de datos personales*. Y resulta aplicable tanto *"a los ciudadanos*" como *"a los funcionarios públicos identificados en cuanto a su calificación administrativa",* porque la ley no distingue.

e) *Punto de contacto esencial*: …al resolver una reclamación o solicitud de amparo de los artículos 8 (TA) o 24 (TP) de la ley 20.285, el Consejo debe tener presente que al mismo tiempo debe velar porque los servicios públicos cumplan con o apliquen la ley 19.628, porque así lo establece expresamente el artículo 33 letra m.

Y, por ende, al tenor del contexto de la ley 19.628, debe considerarse[17]:

(i) Las bases de datos personales del MINVU y de FONASA no son fuentes de acceso público o accesibles al público (artículo 2°) sino que son 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) los órganos las 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) al hacerlo, como responsables de bases de datos no accesibles al público, rige para ellos la obligación de secreto del artículo 7°;

(iv) los órganos MINVU y FONASA deben usar esos datos sólo para los fines para los cuales fueron recolectados -artículo 9°-;

(v) los órganos MINVU y FONASA no pueden transmitir en forma electrónica los datos personales sobre calificaciones de los funcionarios existentes en sus bases, porque ello

[17] Véase lo argumentado en el numeral 5° del acápite anterior.

no guarda relación con sus fines y tareas de servicio público y porque no tienen expresamente asignada la competencia de Derecho Pübblico para hacerlo -artículo 5°-;

(vi) los órganos MINVU y FONASA deben 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, como si existen, como ya mencionamos, para el SERVEL y respecto de los datos de los ciudadanos;

(vii) la ley 20.285 no prima 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[18];

(viii) 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) 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.

5. <u>*Consideraciones finales.*</u>

a) Cabe concluir que las bases de datos del MINVU y de FONASA no son fuentes públicas de información nominativa o datos personales, y que existe por ende obligación de secreto en conformidad al artículo 7° de la ley 19.628;

b) Debe considerarse que la publicidad de las remuneraciones en el artículo 7° de la ley 20.285 es excepcional;

c) Debe tenerse presente que de permitirse el acceso a las calificaciones funcionarias se estaría desconociendo una ley que prima por especialidad y que el Consejo debe hacer cumplir y respectar por los servicios públicos en conformidad al artículo 33 letra m de la ley 20.285;

d) Debe tenerse presente que en la ley 19.628 el único legitimado activo para ejercer el habeas data del artículo 12 y acceder a los datos personales o nominativos *"calificaciones*

[18] Señala el Artículo 4° que *el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito.*

de los funcionarios" es el propio titular de los datos (que es el individualizado o identificado);

e) Debe considerarse que al no existir norma legal expresa que permita la publicidad sería improcedente en derecho que el Consejo excluyera los datos sobre calificaciones de la esfera privada de un funcionario y obligara al MINVU y a FONASA a entregar, comunicar, publicar o dar a conocer a terceros extraños al titular el detalle de las calificaciones y no el simple hecho objetivo de -por ejemplo- *"haberse aprobado el proceso calificatorio en una fecha determinada"* o "*no haberse presentado a rendir los exámenes"*[19];

f) Debe entenderse que, si bien por regla general en materia del acceso de la ley 20.285 a esta fecha el Consejo no ha exigido interés legítimo para los peticionarios, si debe concurrir un interés legítimo y público acreditado y demostrado para una petición administrativa general y no referida a un caso concreto en que se cuestione el desempeño de un funcionario determinado (porque el recurrente de amparo no lo ha invocado así), cuando se refiere a datos personales de los funcionarios y considerando supletoriamente los artículos 1° inc. 1ro, 18° inc. 1ro y 21 N° 1 de la ley 19.880 para integrar las disposiciones de la ley 19.628.

g) No afecta 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-, pero no se puede concluir que la existencia de esta carga u obligación habilita 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 permiten expresamente.

Renato Jijena Leiva
Abogado
Profesor de Derecho Informático PUCV
www.jijena.com

[19] Esta opción de publicidad aparecería como un punto intermedio, donde no se comunicarían las calificaciones propiamente tales, el puntaje ni el lugar en que el funcionario quedó entre los evaluados.