

Protección de Datos Personales

CONSEJO PARA LA TRANSPARENCIA

UNIDAD NORMATIVA, DIRECCIÓN JURÍDICA CPLT / ABRIL 2011

Protección de Datos Personales

CONSEJO PARA LA TRANSPARENCIA

UNIDAD NORMATIVA, DIRECCIÓN JURÍDICA CPLT / ABRIL 2011

Índice

I. INTRODUCCIÓN	5
II. ANÁLISIS CUALITATIVO	8
1. Datos de carácter personal o datos personales	10
1.1 Personas fallecidas	10
1.2 Menores	11
1.3 Padrón electoral	11
1.4 Persona jurídica	12
1.5 Domicilio	12
1.6 Teléfonos celulares	13
2. Datos sensibles	13
2.1 Datos sensibles/salud	13
2.2 Datos sensibles/afiliación política	13
3. Principios de la LPDP	14
3.1 Principio de seguridad	14
3.2 Principio de finalidad	14
4. Acceso a datos personales a través de la LT	16
5. Datos personales y transparencia activa	16
6. Datos personales, información entregada vía LT y terceros	17
7. RUT o RUN	19
7.1 RUT de los funcionarios públicos	19
7.2 RUT de terceros ajenos a la Administración	19
8. Correo electrónico	20
8.1 Dirección de correo electrónico	20
8.2 Contenido del correo electrónico	20
9. Concurso público de selección de personal	21
9.1 Concurso público general	21
9.2 Concursos realizados en el Sistema de Alta Dirección Pública	22
10. Fuentes accesibles al público	24

11. Datos personales y sumario administrativo	24
12. Sanciones art. 21 LPDP	26
13. Datos personales y denuncias	27
14. Datos personales y beneficios otorgados por el Estado	28
14.1 Datos de evaluadores	28
14.2 Datos de donantes y beneficiarios	29
15. Test de daño aplicado a la protección de datos	30
16. Test de interés público aplicado a la protección de datos	30
17. Currículum vitae de los funcionarios públicos	31
18. Tratamiento de datos	31
19. Obligaciones tributarias y protección de datos	32
20. Afiliación sindical y protección de datos	33
20.1 Identidad de los trabajadores afiliados a un sindicato	33
20.2 Instrumentos colectivos y convenios colectivos	36
III. ANÁLISIS CUANTITATIVO	37
IV. RECOMENDACIONES	45

I. Introducción

I. Introducción

El Consejo para la Transparencia, conociendo de reclamos por incumplimiento de los deberes de transparencia activa o de amparos por denegación de acceso a la información se ha visto en la necesidad de ejercer, además, la atribución consagrada en el artículo 33 letra m) de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N° 20.285, de 2008 (en adelante LT), esto es, velar por el debido cumplimiento de la Ley N° 19.628, sobre protección de datos de carácter personal (en adelante LPDP), por parte de los órganos de la Administración del Estado.

Dicho pronunciamiento se ha realizado principalmente a través de dos vías:

- Las partes han impetrado la protección de un dato personal y el Consejo ha debido referirse a ello en su decisión, o
- El propio Consejo ha optado por aplicar directamente la legislación sobre protección de datos, sea porque esta aplicación influía directamente en la decisión o se estimó que constituía una consideración adicional que debía tenerse en cuenta al momento de decidir el caso.

El presente Informe tiene por objeto realizar un levantamiento cualitativo y cuantitativo de la jurisprudencia del Consejo para la Transparencia en materia de protección de datos personales, entre los meses de agosto de 2010 y marzo de 2011. En la primera parte (análisis cualitativo) sistematiza las líneas jurisprudenciales más relevantes y, en la segunda (análisis cuantitativo), establece el porcentaje de las decisiones entre agosto de 2010 y marzo de 2011 que aplicaron la LPDP.

Finalmente, se incluye en este documento el texto de las Recomendaciones del CPLT sobre protección de datos personales por parte de los órganos de la Administración del Estado, aprobadas por el Consejo Directivo el 31 de agosto de 2001 y publicadas en el

Diario Oficial de 14 de septiembre de 2011, que —recogiendo la experiencia acumulada por este Consejo— proponen una serie de buenas prácticas complementarias de la Ley N° 19.628, que procuran facilitar su comprensión y orientar un mejor cumplimiento de las obligaciones que impone.

II. Análisis Cualitativo

II. Análisis Cualitativo

El propósito de este análisis es observar las líneas jurisprudenciales más importantes en la materia y los criterios jurídicos aplicados, así como las obligaciones y limitaciones que deben observar los órganos de la Administración del Estado en el tratamiento de datos de carácter personal que obren en su poder; con la finalidad de garantizar a la persona el derecho a la protección de los datos de carácter personal que le conciernen y asegurar el debido manejo de los registros o bancos de datos personales necesarios para el ejercicio de las competencias de dichos Servicios. Se intentará arribar con ello a un análisis de los referidos casos en función de la materia, de modo que podamos agruparlos de acuerdo a este criterio facilitando su comprensión y estudio. Si bien las decisiones examinadas corresponden al periodo que media entre agosto de 2010 y marzo de 2011, como ya se indicó, en aquellos casos en que no logramos encontrar ejemplos relevantes en el período indicado, o cuando sea importante destacar decisiones emblemáticas en materias específicas o variaciones en los criterios adoptados durante ese periodo, se han incluido anteriores o posteriores a

ese periodo.

El Consejo Directivo del Consejo para la Transparencia, del que emana la jurisprudencia que procederemos a analizar, está conformado por cuatro consejeros, los que elijen a uno de ellos como Presidente (en el que queda radicado el voto dirimente en caso de empate, de acuerdo al artículo 36 de la LT). Entre octubre de 2008 y julio de 2010 estuvo integrado por don Alejandro Ferreiro Yazigi, don Juan Pablo Olmedo Bustos (presidente en el periodo octubre de 2008 – abril 2010), don Raúl Urrutia Ávila (presidente en el periodo mayo de 2010 – octubre 2011) y don Roberto Guerrero Valenzuela. Desde agosto de 2010 y tras la renuncia de éste último, asumió don Jorge Jaraquemada Roblero.

Para efectos de agrupar las líneas jurisprudenciales centrales, estableceremos como factores de reconocimiento las siguientes materias:

1. Datos personales
2. Datos sensibles
3. Principios de la LPDP
4. Acceso a datos personales a través

de la LT

5. Datos personales y transparencia activa
6. Datos personales, información entregada vía LT y terceros
7. RUT o RUN
8. Correo electrónico
9. Concurso público en selección de personal
10. Fuentes accesibles al público
11. Datos personales y sumario administrativo
12. Sanciones artículo 21 LPDP
13. Datos personales y denuncias
14. Datos Personales y beneficiarios del Estado
15. Test de daño aplicado a la protección de datos
16. Test de interés público aplicado a la protección de datos
17. Currículum Vitae de los funcionarios públicos
18. Tratamiento de datos
19. Obligaciones tributarias y protección de datos
20. Afiliación sindical y protección de datos

1.- DATOS DE CARÁCTER PERSONAL O DATOS PERSONALES

los relativos a cualquier información concerniente a personas naturales, identificadas o identificables (artículo 2º, letra f) LPDP).

1.1 Personas fallecidas

1.1.1 Ficha Clínica (C398-10, C322-10, C556-1, C740-10). El Consejo ha establecido que una persona fallecida no es titular de datos personales a la luz de lo dispuesto en el artículo 2º, letra ñ) de la LPDP, al no tratarse de una persona natural. Su honra, sin embargo, se proyecta como un derecho propio de sus familiares, toda vez que su memoria constituye una prolongación de dicha personalidad, protegida y asegurada como parte de la honra de la familia. De acuerdo a lo anteriormente expresado los llamados a cautelar dicha honra y, por ende, a determinar qué información desean sustraer del conocimiento de terceros no vinculados al fallecido, son los familiares del mismo, derecho al que subyace el supuesto lógico de conocer tal información (C322-10). Por otro lado, indica en la misma decisión, aceptar la confidencialidad absoluta de la ficha clínica de un fallecido impediría el acceso a los antecedentes que pudieran revelar la existencia de eventuales negligencias médicas y ejercer el derecho a perseguir

las responsabilidades civiles y penales correspondientes, si fuera el caso, como también el ejercicio de otros derechos.

El Consejo, sin embargo, ha sido claro en señalar que para acceder a esta ficha clínica no basta con acreditar una relación de parentesco, sino que debe constar alguna de las siguientes características (556-10):

- Ser heredero (a) del fallecido, de acuerdo a lo dispuesto en el artículo 983 del Código Civil, o que se actúa en representación de uno o más herederos.
- Tener una legitimación activa para ejercer otros derechos que supongan el acceso previo a la ficha clínica del difunto.

Las consideraciones anteriores establecen un criterio diferenciador, el cual fue manifestado en dos solicitudes de información analizadas por el Consejo. En una de ellas (C556-10), al ser la solicitante una sobrina del fallecido y no concurrir alguno de los supuestos indicados anteriormente, su solicitud fue rechazada. En otra (C322-10), en cambio, tratándose del hijo del difunto, y habiendo acreditado éste su calidad de heredero, el Consejo accedió a la entrega de la ficha solicitada.

1.1.2 Identidad del fallecido (C64-10, C840-10). En el primero de los casos citado, y frente al requerimiento de un listado de personas fallecidas por accidentes laborales, el Consejo señaló que de aceptarse la hipótesis planteada por el organismo reclamado, en cuanto a que lo requerido es un dato sensible, dicha información no podría ser objeto de tratamiento alguno y, por lo tanto, no podría ser comunicada al reclamante, salvo que la Ley lo autorizara o el titular consintiera en ello, de acuerdo al artículo 10 de la LPDP, lo que no ocurre en el supuesto planteado. En este sentido, y conforme a lo dispuesto en los artículos 55, 77 y 78 del Código Civil, el titular del derecho a la protección de datos personales, al ser un derecho fundamental y personalísimo, es la persona natural y, por ello, las personas fallecidas no pueden ser titulares de aquel, toda vez que este tipo de derechos se extingue con la muerte. Por lo anteriormente expuesto, el Consejo estimó que la información requerida no constituía datos sensibles toda vez que las personas a las que se refiere han fallecido, extinguiéndose con ello su derecho fundamental a la protección de datos personales. A mayor abundamiento, indica, tampoco estamos frente a un dato personal que se haya recolectado en vida de los fallecidos, sino que el dato mismo es la muerte de la persona por lo que, en

ningún caso, se trataría de un dato personal y, por ende, tampoco sensible.

En este caso el Consejo aborda también el tema de si la divulgación de la muerte de una persona debido a un accidente laboral puede vulnerar el derecho a la honra de ésta o de sus familiares, ya que se ha entendido que la lesión a la honra de una persona fallecida se hace extensible a las personas que guardaban con ella una estrechísima relación. Se analiza si procedía emplear el procedimiento contemplado en el artículo 20 de la LT y notificar a los terceros que tuviesen derechos que pudieran verse afectados con la entrega de la información, concretamente, los familiares de los fallecidos. El Consejo estimó que ello implicaría una distracción indebida de los funcionarios del órgano reclamado de sus labores habituales, tanto por tener que identificar primeramente a los interesados (familiares, sucesores o personas que constituyen el círculo más cercano del fallecido, por ejemplo), como por el alto número de aquéllos a los que habría que notificar. Sin embargo, resuelve que aunque no fuera así no procede efectuar dicha notificación ya que la información no tiene una carga negativa que pueda violar el buen nombre de la persona fallecida o su familia o afectar la reputación de sus familiares. Por esto,

no se entiende que en este caso haya un interés legítimo de los familiares, sucesores o personas cercanas a los fallecidos que se deba proteger y que amerite reservar esta información pública.

1.2 Menores (C80-10, C579-10, C816-10, C906-10)

Frente a la solicitud de acceso por parte del solicitante de información de la hoja de vida de una menor, cita el Consejo lo señalado por la profesora Lorena Donoso en el sentido que “los datos personales de los menores que son tratados en el sistema educacional no pueden considerarse como provenientes de fuentes de acceso al público para proceder a su revelación (artículo 7° de la LPDP) y merecen protección pese a las falencias de nuestra legislación en la materia, especialmente teniendo en consideración que uno de los principios de nuestra legislación es el del interés superior del niño”¹. Asimismo, la Convención de Derechos del Niño, en su artículo 16.1, establece que “*Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación*”. En la decisión C80-10, el Consejo estimó que la publicidad, comunicación o conocimiento de la hoja de vida de la menor afecta la esfera de su vida privada,

derecho que también es consagrado en la Constitución en el artículo 19 N° 4, configurándose así la causal del artículo 21 N° 2 de la LT, por lo que fue declarada secreta o reservada dicha información, rechazándose la solicitud de amparo.

1.3 Padrón electoral (C407-09)

Respecto de una solicitud de acceso a los datos personales contenidos en el padrón electoral a cargo del Servicio Electoral (SERVEL), el Consejo ha señalado que la Ley N° 18.556 prescribe categóricamente que los Registros Electorales serán públicos. Por lo tanto, estimó que existiendo una ley orgánica constitucional que declara que la información contenida en los registros electorales es pública, no se puede requerir al órgano reclamado que tarje aquellos datos personales, ni aún bajo el amparo de la LPDP, ya que ésta fue aprobada con un quórum de ley simple que impide a este Consejo estimar que pudiese haber derogado tácitamente a una norma aprobada con quórum orgánico constitucional, como el artículo 25 de la Ley N° 18.556. A mayor abundamiento, indica, el carácter orgánico constitucional de esta ley deriva del artículo 18 de nuestra Carta Fundamental lo que impide que la interpretación del sistema electoral pueda subordinarse a lo dispuesto en una ley de quórum simple. Por otro lado, la entrega de los datos relativos al RUT

¹ Donoso, Lorena, “El tratamiento de datos personales en el sector de la educación”, en Foco N° 136, Expansiva UDP, de 15 de abril de 2009.

de las personas inscritas es indispensable para asegurar el control social del padrón electoral, pues sólo a través de este código numérico es posible verificar que no existan inscripciones duplicadas, ya que identifica y diferencia a todos los ciudadanos con absoluta precisión. Por todo lo anterior, el Consejo opta por la entrega de la información solicitada.

En el caso particular, sin embargo, se contó con la disidencia parcial del Consejero Olmedo, quien postuló que si bien es cierto que la Ley N° 18.556 establece que los Registros Electorales serán públicos, lo solicitado era el padrón alfabético computacional. Los datos contenidos en el padrón sólo pueden utilizarse en los fines para los cuales se recolectaron, pues no provienen de fuentes accesibles al público. Además, de acuerdo a la ley, el Padrón Electoral contiene la nómina alfabética de personas habilitadas para ejercer el derecho a sufragio y no la totalidad de los datos contenidos en los “Registros Electorales”: no están la profesión, la fecha de nacimiento, el domicilio, ni el RUT, que tampoco son indispensables para controlar los procesos electorales. Además, su tráfico arriesga severamente la intimidad de las personas, más aún si se incluyen las condiciones de no vidente y analfabeto, datos sensibles que no podrían

tratarse en este caso.

1.4 Persona Jurídica (C39-10, C184-10, A33-10, A265-09, C298-10, C461-09, C822-10, C734-10)

El Consejo ha indicado que la LPDP no es aplicable a las personas jurídicas, por lo que en el caso concreto no se puede alegar vulneración de sus disposiciones (A39-10). A modo de ejemplo, tratándose de las Empresas Individuales de Responsabilidad Limitada (EIRL) el Consejo advierte que éstas son una persona jurídica con patrimonio propio distinto del titular, conforme al artículo 2° de la Ley N° 19.857 que las regula. En consecuencia, si bien toda EIRL puede relacionarse con la persona natural que es su titular, no coincide una y otra y al ser la primera una persona jurídica no cabe aplicarle las normas sobre protección de datos personales que contempla la LPDP (C461-09).

Con todo, el Consejo ha reconocido la existencia de un derecho al honor por parte de las personas jurídicas privadas que las ha hecho acreedoras de algún nivel de protección (p. ej., decisión A265-09).

1.5 Domicilio

1.5.1 Como dato personal (A33-09, A140-09, C415-09, C713-10, C832-10). En

la decisión A33-09 se requirió al organismo público entregar los documentos que se tuvieron en consideración para rechazar la declaración de una herencia vacante, entre los que se cuenta una copia de la red familiar del causante de dicha herencia. El Consejo advierte que la información solicitada contiene datos personales de los integrantes de dicha red, concretamente su RUN o RUT, su domicilio y los datos de algunas inscripciones de matrimonio y de nacimiento que no provienen o no han sido recolectados de fuentes accesibles al público. Añade el Consejo que se trata de datos personales a los cuáles sólo puede accederse con la autorización de su titular o cuando la ley lo permite. Por ello, junto con acogerse el amparo, se indicó al órgano reclamado que tarjara de la información entregada los datos personales señalados.

1.5.2 Como dato sensible (A190-09).

En este caso se solicitó acceso a la base de datos de la Encuesta de Calidad de Vida y Salud elaborada por el organismo reclamado. El Consejo detectó la existencia, en la base de datos requerida, de información que pudiera haber afectado derechos de terceros como lo son el domicilio (“dirección de la vivienda seleccionada”), el registro de personas en el hogar, parentesco, nivel de educación y

estado conyugal, así como preguntas sobre la vida sexual del encuestado, estado de salud, entre otros, que el artículo 2º, letra g) de la LPDP ha establecido como datos personales sensibles. El Consejo acogió el amparo pero requirió que se tarjasen de la información entregada todos aquellos datos personales y sensibles de las personas encuestadas.

1.6 Teléfonos celulares (C611-10)

El reclamante, en este caso, solicitó el acceso a los números de los teléfonos móviles financiados por una Municipalidad. El Consejo indicó que desde el punto de vista de la protección de los datos personales, en tanto el número telefónico se encuentre asociado o sea susceptible de asociarse al nombre de una persona natural, dicha información constituye un dato personal, por lo que quienes trabajen en su tratamiento están obligados a guardar secreto sobre los mismos, cuando estos provengan o hayan sido recolectados de fuentes no accesibles al público (artículo 7º LPDP). En el caso particular, el dato personal no ha sido proveído al municipio por la persona natural sobre la que éste versa, sino que tiene por fuente información elaborada con presupuesto público y concerniente a herramientas para el ejercicio de las funciones públicas, por lo que se presume pública, a menos que esté sujeta a las

excepciones indicadas en el artículo 21 de la LT. Sobre este punto, el Consejo estimó que divulgar aquellos números telefónicos respecto de los cuales el órgano no cuenta con el mecanismo de canalización de comunicaciones que la entidad edilicia describe o aquellos que permiten el acceso directo a autoridades o funcionarios respecto de los cuales precisamente se ha elaborado dicho mecanismo, permitiría a las personas sortear el sistema de acceso telefónico a las autoridades o funcionarios públicos dispuesto por el órgano, impidiendo a los funcionarios que ejecutan dicha labor cumplir regularmente con los fines por los cuales han sido contratados. Por ello, y en aplicación con el artículo 33, letra j) de la LT, el Consejo declaró reservada la información solicitada, fundado en que su entrega afectaría el adecuado cumplimiento de las funciones del municipio.

2.- DATOS SENSIBLES

Los datos sensibles corresponden a 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 (artículo 2º, letra g) LPDP). No pueden ser objeto de tratamiento, vale decir, almacenados o comunicados salvo en los casos excepcionales del artículo 10 de la citada ley.

2.1 Datos sensibles/salud (C267-10, A211-09, C240-10, C394-10, C418-10)

El Consejo consideró que tanto las licencias médicas (lo que en la decisión C267-10 incluye la fecha de emisión de las mismas y la de recepción por parte del empleador, su número identificador, así como el número de días prescrito y la institución a la cual se deben despachar) como la ficha clínica de un paciente (C240-10) y el listado de personas a las cuales se les haya diagnosticado una enfermedad determinada (A211-09) constituyen datos sensibles, por referirse a estados de salud físicos o psíquicos, dando cuenta así de datos personales que se refieren a hechos o circunstancias de su vida privada o íntima. En todos estos casos (con excepción de la decisión C418-10 que se detalla más adelante) se rechaza el amparo interpuesto, ordenando la reserva de la información indicada.

2.2 Datos sensibles/afiliación política (A152-09)

En el caso citado, la requirente solicita el nombre de todos los integrantes de un

Comité Evaluador de Fondos Concursables, sus títulos profesionales, su lugar de desempeño y su afiliación política. En cuanto a este último requerimiento, el Consejo aplicó el artículo 21 N° 5 de la LT en relación con lo prescrito por el artículo 2 letra g) de la LPDP, que califica a esta información como un dato sensible. Por estas razones, se deniega la entrega de la información relativa a la afiliación política de los evaluadores.

3.- PRINCIPIOS DE LA LPDP²

3.1 Principio de seguridad (C418-10, C351-10)

En el primero de los requerimientos se solicita al órgano reclamado la ficha clínica del padre del requirente. El Consejo señaló que al tratarse de datos personales sensibles, resulta aplicable lo dispuesto en el artículo 10 de la LPDP que dispone que aquéllos no pueden ser objeto de tratamiento—particularmente en lo relativo a su cesión a terceros—, salvo en tres hipótesis:

- a) Cuando la Ley lo autorice.
- b) Cuando exista consentimiento del titular de los datos.
- c) Cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a

sus titulares.

Al respecto, el Consejo estimó que no concurría en la especie la hipótesis de una autorización legal para el tratamiento de datos sensibles contenidos en la ficha clínica de un paciente, ni tampoco se trataba de datos necesarios para el otorgamiento de un beneficio de salud, quedando, al efecto, sólo la hipótesis del consentimiento del titular de los datos requeridos. En relación a esto, el Consejo (luego de la aplicación, entre otras disposiciones legales, de los artículos 4°, inciso 2° y 5° de la LPDP que consagran los principios de finalidad y de seguridad de los datos respectivamente) concluyó que el consentimiento que debe prestar el titular de datos para la comunicación o cesión de los mismos debe, al menos, ser informado, expreso, por escrito y específico, para la finalidad que se indique. La especificidad debe estar referida a la indicación expresa de los datos o documentos que se autoriza tratar, en la especie, ceder o recolectar. A juicio del Consejo, los requisitos señalados precedentemente deben tenerse por cumplidos en el mandato especial acompañado por el reclamante, pues revelan inequívocamente la intención del titular de los datos requeridos de consentir en el acceso a los mismos por parte del reclamante, por lo que acoge el amparo.

3.2 Principio de finalidad (C351-10, C418-10)

A primera vista, señala el Consejo en la decisión C351-10, la información requerida (listado de cotizantes de una determinada ISAPRE) efectivamente estaría cubierta por la presunción de publicidad establecida en el artículo 5° de la LT. Sin embargo, por tratarse de una solicitud de datos personales de terceras personas, a la luz del concepto previsto en el artículo 2°, letra f) de la LPDP, el Consejo indicó que de no contar con el consentimiento del titular de datos personales para el tratamiento de los mismos, según la regla general del artículo 4° de la LPDP, un organismo público puede tratarlos cumpliendo con dos supuestos: efectuarse dicho tratamiento respecto de materias de su competencia y la sujeción para ello a las disposiciones de la LPDP. Respecto del segundo supuesto indicado, agrega, cabe tener a la vista lo indicado por la Comisión mixta en el tercer trámite constitucional de la tramitación de la LPDP³. En relación a que el tratamiento de datos debe efectuarse en el marco de las competencias del organismo público, el DFL N°1/2005, que regula las atribuciones del organismo reclamado con las ISAPRES, establece que uno de los deberes de información que deben cumplir dichas instituciones es el tener actualizada la información relativa al número

² Véase respecto a estos principios el punto 4 de las Recomendaciones del CplT sobre protección de datos personales por parte de los órganos de la Administración del Estado.

³ “La segunda parte de la disposición, que somete el tratamiento de datos personales que hagan los organismos públicos “a las reglas precedentes”, deja de manifiesto que -como anticipó el artículo 1°, inciso primero-, son unos mismos los preceptos que se aplican a los organismos públicos y a los particulares. No hay regulaciones

e identificación de sus cotizantes, grupo familiar y terceros beneficiarios, monto de cotizaciones percibidas, prestaciones médicas y pecuniarias otorgadas y número de licencias o autorizaciones médicas presentadas, con indicación de las autorizadas, de las modificadas y de las rechazadas (artículo 217). Se concluye, entonces, que el organismo reclamado almacena los datos entregados directamente por las ISAPRES respectivas en cumplimiento de un imperativo legal en el DFL N° 1/2005, en cuyo tratamiento debe cumplir con los supuestos previstos en el artículo 20 de la LPDP, vale decir, sólo respecto de las materias que son de su competencia y con sujeción a las disposiciones de la LPDP. De esta conclusión se desprende lo siguiente:

- El titular de dichos datos tiene limitados sus derechos de solicitar la modificación, cancelación o bloqueo de éstos, por aplicación del artículo 15 inciso 2° de la LPDP, no obstante lo cual el tratamiento de datos personales efectuados por un organismo público, como es el caso, debe respetar, entre otros, los principios de finalidad y seguridad, consagrado en los artículos 4° inciso 2° y 5° y 11° de la LPDP, respectivamente.

- Al tratarse de datos aportados directa-

mente por las ISAPRES, y al no constituir información que deba mantenerse disponible al público, se descarta la aplicación del artículo 4° inciso 5° de la LPDP, por cuanto dichos datos no obran en poder del organismo reclamado por haber sido recolectados de fuentes accesibles al público. Así, aún cuando el tratamiento de datos personales pueda darse en dichas condiciones por parte de un organismo público, el titular de los mismos no pierde el núcleo esencial de su derecho a la protección de sus datos personales, cual es el poder de control sobre el uso que se haga de los mismos. De ahí el deber del organismo de respetar los principios básicos de la protección de datos y el deber de reserva que pesa sobre las personas que trabajan en el tratamiento de los datos, en la especie, los funcionarios del organismo reclamado.

En consecuencia, señaló el Consejo, al tratarse de una solicitud de acceso parcial a una base de datos personales, cuyo tratamiento se da en las condiciones señaladas precedentemente, otorgar el acceso a dicha información implica inequívocamente una intromisión a la vida privada de los titulares de dichos datos, sin que éstos hayan consentido en su utilización para fines diversos.

Además, indica, el acceder a la entrega de la información requerida implica no sólo una intromisión a la vida privada de los cotizantes cuya individualización se pide, sino que ésta, además, sería injustificada, lo que viene determinado por dos factores:

- La entrega de información en sede de acceso a la información “se hará por parte del órgano requerido sin imponer condiciones de uso o restricciones a su empleo, salvo las expresamente estipuladas por la ley” (artículo 17 LT), por lo que, entregada la información el titular de los datos personales se vería despojado de todos los derechos y garantías que le son otorgadas por la LPDP lo que supone una afectación al núcleo central del derecho a la protección de datos, la autodeterminación informativa.

- No se advierte el interés público que justifique dicha intromisión, y que habilite para afectar la privacidad de los titulares de los datos requeridos.

Si bien el tratamiento por parte del organismo reclamado de los datos personales solicitados no requiere del consentimiento de sus respectivos titulares, pues se trata de un almacenamiento encomendado por la ley; el Consejo estimó que los derechos

separadas y diferentes, que permitan a unos inmiscuirse en mayor medida que a los otros en aspectos que conciernen tan estrechamente a las garantías constitucionales de respeto y protección a la vida pública y privada y a la honra de la persona y de su familia. Las normas contenidas en este título, por consiguiente, son especiales, pero sólo en cuanto recaen sobre aspectos propios del sector público”. (Tercer Trámite Constitucional, Comisión Senado-Cámara de Diputados, sesión 2 de junio de 1999, cuenta en Sesión 02 de la Legislatura 340 del Senado, p.156-157).

de los mismos se ven seriamente limitados por lo que optó por el rechazo del amparo interpuesto, declarando los datos requeridos como reservados.

4.- ACCESO A DATOS PERSONALES A TRAVÉS DE LA LT (C491-10, C323-10, C351-10, C237-10, C707-10, C426-10, C752-10, C27-11, C915-10, C49-11, C103-11)

Respecto a una solicitud de información de la totalidad de los antecedentes relativos a la petición de indulto del requirente, que fuera denegada mediante Decreto Exento (C323-10), el Consejo indicó que al referirse parte de la información requerida al propio reclamante, se entiende que dicha solicitud se realiza en ejercicio del habeas data. Acota el Consejo que el artículo 12 de la LPDP establece que uno de los derechos del titular de los datos personales es 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. Este derecho es también conocido como derecho de acceso del titular de datos

personales y se comprende dentro del habeas data. Esto ha sido recogido en el punto 5.1 de las Recomendaciones del CPLT sobre protección de datos personales por parte de los órganos de la Administración del Estado.

Igual criterio es aplicado cuando se le solicita a un organismo público, a través de su Oficina de Partes, la remisión de las evaluaciones obtenidas a propósito del proceso de postulación al cargo de Encargado de Sección de Servicios Generales (C707-10). El Consejo estimó que el organismo reclamado no podía menos que contar con las actas del concurso en el que consten los puntajes asignados al requirente, la que deberá entregársele, ya que los puntajes que obtuvo en las distintas evaluaciones que le fueron practicadas –evaluación curricular (título profesional y experiencia profesional), evaluación psicolaboral y entrevista técnica, en su caso– constituyen datos personales respecto de los cuales es titular, de acuerdo al artículo 2, letra ñ) de la LPDP.

En la decisión C426-10 se solicitó copia de todas las actas e informes relacionados con la persona del reclamante, evacuados en las sesiones del Consejo Técnico de un Centro Penitenciario en que se analizaron y resolvieron sus fallidas postulaciones al

beneficio de salida dominical. El Consejo estimó que si bien parte de los documentos solicitados, como los informes psicológicos y sociales, contienen información que puede considerarse como datos de carácter sensible; estos serían del propio requirente, por lo que cabe desechar la alegación planteada por el organismo reclamado, toda vez que dicho precepto legal sólo establece una causal de reserva o secreto de los datos de carácter personal respecto de terceros y no de su titular, y proceder en consecuencia a la entrega de la información solicitada.

5.- DATOS PERSONALES Y TRANSPARENCIA ACTIVA (C579-10)

En la especie, la reclamante indicó que el órgano administrativo publicaba en su sitio electrónico el contrato suscrito por dicha entidad con la sala cuna a la que asiste su hija, señalándose el nombre completo y RUT de ésta última. Al respecto, el Consejo estimó que siendo competente para pronunciarse sobre el cumplimiento de la LPDP, al establecer el artículo 8° de la LT que la acción de reclamación resulta procedente cuando el organismo público “no informa lo prescrito” en el artículo 7° de la Ley, debe entenderse que el incumplimiento de la obligación de informar del organismo no se reduce a verificar la concurrencia de

la acción positiva de publicar información en el sitio electrónico del Servicio, sino que también el incumplimiento de la obligación de divulgar información en los términos y dentro de los límites previstos por el ordenamiento jurídico, lo que supone respetar las causales de reserva contempladas en el artículo 21 de la LT y las disposiciones aplicables de la LPDP. Conforme a lo anterior, en aplicación del artículo 47 de la LT, el Consejo podrá sancionar a la autoridad que “injustificadamente”:

- no divulgue la información requerida por el artículo 7°;
- lo haga comunicando datos personales cuya comunicación no responde a la finalidad autorizada por el legislador; o
- divulgue información secreta o reservada.

En la situación planteada, agrega el Consejo, la información relativa a la menor de edad ha sido provista al órgano administrativo con la exclusiva finalidad de identificar a los asistentes de las salas cunas contratadas por éste, razón por la cual, conforme a lo prescrito por el artículo 9° de la LPDP, en principio, el órgano administrativo sólo se encuentra autorizado para utilizar dichos datos personales de acuerdo con aquellos fines para los cuales han sido recolectados.

Ahora, el artículo 7° de la LT ordena a los órganos de la Administración divulgar en sus sitios electrónicos los contratos de prestación de servicios celebrados por éstos, entre los que se encuentran los citados contratos de prestación de servicios de sala cuna. En el presente caso, sin embargo, la divulgación de la identidad del menor no tiene por objeto satisfacer el objetivo perseguido por el legislador al ordenar dicha divulgación, toda vez que éstos han sido incorporados al contrato como antecedentes de contexto del mismo y han sido proveídos por el reclamante con la exclusiva finalidad de que se le asigne determinado beneficio laboral. Por lo tanto, finaliza el Consejo, dichos antecedentes deben ser tachados por el organismo por suponer un tratamiento de datos personales no autorizado por la LPDP.

En materia de datos personales y transparencia activa pueden consultarse los criterios expuestos en el punto 6.3 de las Recomendaciones del CPLT sobre protección de datos personales por parte de los órganos de la Administración del Estado y los puntos 1.7 y 1.9 de las Instrucciones Generales N° 4 y N° 9, del CplT, publicadas en el Diario Oficial de 03.02.2010 y 20.08.2010, respectivamente.

6.- DATOS PERSONALES, INFORMACIÓN ENTREGADA VÍA LT Y TERCEROS (C748-10, C755-10, C757-10)

En las tres decisiones citadas, el reclamante requería copia de las solicitudes de acceso a la información presentadas durante un cierto período de tiempo y ante determinados órganos de la Administración del Estado, junto con las resoluciones que las resolvían y los documentos entregados por éstos como respuesta a estas solicitudes.

Al respecto, el CplT reconoció que no obstante que las solicitudes de acceso fueran complemento directo de un acto administrativo, en virtud de lo dispuesto por los artículos 4°, 9°, 10 y 20 de la LPDP, la comunicación a terceros de algunos de los datos contenidos en ellas se encontraba vedada a los órganos de la Administración.

A idénticas conclusiones arribó el Consejo en relación con las resoluciones pronunciadas con motivo de las solicitudes de acceso, toda vez que éstas podían reproducir, a su juicio, los datos personales que el solicitante incorporó a su presentación para su mejor individualización y que la asociación de la identidad del solicitante con “lo pedido” dentro del texto de la

resolución, podía incluso revelar datos sensibles de las personas o afectar sus derechos personales.

Por otra parte, y tratándose de los requerimientos acerca de documentos que los órganos administrativos ya han entregado a terceros, el Consejo indicó que de ciertas decisiones en determinadas materias (a saber, fichas clínicas, postulantes a cargos en la Administración, petición de datos personales reservados por parte de su titular y acceso al sumario administrativo por el inculpado), podía extraerse como criterio jurisprudencial del CD, el que existiría cierta información que obra en poder de órganos de la Administración a la que sólo podían acceder sujetos determinados. Esto podía ocurrir, agregó, o porque el ordenamiento jurídico protegiera el derecho de la persona a excluir a terceros de su conocimiento o porque se estimara que el acceso universal podría afectar el debido funcionamiento del órgano. En las decisiones analizadas (y que en el presente documento hemos revisado en los puntos 1.2.1, 8 y 6) el CpIT ha declarado implícitamente la reserva de los documentos requeridos con carácter general, identificando al solicitante como un sujeto excepcionalmente autorizado para acceder a ellos (en esta hipótesis la resolución del órgano administrativo que ordenaba la entrega de la información, no

estaba declarando el carácter público de los documentos requeridos, sino sólo el acceso a favor de un determinado sujeto).

En base a lo expuesto, el Consejo identificó las siguientes tareas de los órganos de la Administración para dar respuesta a las solicitudes del reclamante:

- Reproducir y revisar las solicitudes y resoluciones correspondientes a las fechas indicadas;
- Tachar en ellas los datos que permiten la individualización del solicitante;
- Identificar los documentos que contienen información reservada. Este proceso de divisibilidad responde, según el criterio del CD, a la omisión del procedimiento de oposición contenido en el artículo 20 de la LT, toda vez que al revisar las solicitudes en comento, los órganos requeridos debieron verificar si la divulgación de la información podría afectar los derechos de los terceros (solicitantes) y, en tal caso, notificar a éstos el requerimiento de información. Ahora bien, dicho reproche no cabe en los casos en que se estime que abordar dicho procedimiento de notificación afectaría el debido cumplimiento de sus funciones, en los términos del artículo 21 N°1 de la LT, caso en que podía haberse denegado el acceso a la información en virtud de dicha causal.

- Informar los datos requeridos acerca de la tramitación de las solicitudes de información presentadas a cada organismo;
- Atendida la forma de entrega requerida por el solicitante, debiese reproducir digitalmente cada una de las solicitudes y resoluciones tachadas, así como los documentos solicitados.

En este sentido, concluye el CD, y teniendo en cuenta el nivel de sistematización en que se encontraba la información solicitada, para determinar la concurrencia de la causal de reserva invocada, debía atenderse, exclusivamente, al volumen de información involucrado (lo que implica contextualizar la supuesta distracción indebida de funciones manifestada en la carga de trabajo de los funcionarios encargados, el tiempo estimado en recopilar, evaluar, reproducir y tachar la información requerida, etc.).

En la especie se acogieron parcialmente los tres amparos citados. En la Decisión C748-10, el órgano requerido había remitido al reclamante una planilla que informaba el número de solicitudes presentadas en el período indicado por el reclamante, el número de rol asignado a éstas, su fecha de ingreso al organismo, el número de rol de su respuesta y la fecha de la misma; ordenando el CD entonces, entregar copia de

las solicitudes de acceso a la información presentadas en el período indicado, copia de las resoluciones que las resolvieron y los documentos entregados por los órganos públicos como respuesta a estas solicitudes. En la Decisión C755-10 se ordenó la entrega de los mismos antecedentes al organismo reclamado, sumando ésta vez la planilla de solicitudes que dicho organismo había hecho llegar en sus descargos al CplT y no al reclamante. Finalmente, en la Decisión C757-10, se requirió al órgano incorporar en la planilla entregada los datos faltantes (que consistían en las fechas y roles de las resoluciones pronunciadas con motivo de las solicitudes de acceso presentadas), junto con la copia de las solicitudes de acceso a la información presentadas en el período indicado, copia de las resoluciones que las resolvieron y los documentos entregados por los órganos públicos como respuesta a estas solicitudes

7.- RUT O RUN

7.1 RUT de los funcionarios públicos (C283-10, A10-09, A126-09)

Acá en líneas generales, el Consejo ha calificado al RUT como dato personal obtenido de los propios interesados en acceder a la función pública (artículo 13 del Estatuto Administrativo) y no directamente de un registro público (es decir, sólo

para su tratamiento al interior del servicio público respectivo y no para su cesión a terceros), por lo que debe considerarse como información secreta o reservada, debiendo ésta tajarse en la entrega del resto de la información que se solicita (principio de divisibilidad LT).

Sin embargo, en una de las decisiones referidas a la materia (A10-09) y en la cual se solicitaban las calificaciones de todo el personal y ex-funcionarios de un organismo público, sus RUT, tipo de contrato, estamento, sexo, puntaje, lista de calificación, año, etc.; el Consejo señaló que el artículo 7°, letra d) de la LT exige identificar al personal de los servicios públicos como parte de los deberes de transparencia activa y, en tanto ley posterior, modificaría el criterio del artículo 7° de la LPDP, levantando la reserva del RUT. No obstante, para adoptar esa decisión y revelar los RUT habría sido necesario, según el Consejo, notificar a sus titulares conforme el artículo 20 de la LT, pues se trataría de información que actualmente no ha sido divulgada y que, de difundirse, podría afectar sus derechos, lo que no se hizo en el desarrollo de la solicitud en estudio, impidiendo así que el Consejo pudiera realizar un test de interés público para ponderar el daño que podría provocar a los funcionarios y ex funcionarios del

organismo reclamado, la difusión de sus RUT. El Consejo hace presente que el resultado de esta ponderación podría dar pie a su entrega, en caso de estimarse que prevalece el interés público sobre la protección del dato personal (emanación del derecho a la vida privada regulado en el artículo 19 N°4 CPR), pero siempre previa notificación al tercero potencialmente afectado. Se acogió entonces de manera parcial el amparo interpuesto en contra del organismo, requiriendo la entrega de las calificaciones solicitadas, con individualización de sus nombres, tipo de contrato, estamento o plantas de personal a que está adscrito, sexo, puntaje, lista de calificación y año, por tratarse de información pública. Rechazó el Consejo, sin embargo, la petición de entregar los RUT de dichos funcionarios por no haber sido notificados previamente como exige el artículo 20 de la LT, pero indicando que se identifique a los funcionarios por sus nombres, dado que esta información es pública en virtud del art. 7 d) de la misma ley.

7.2 RUT de terceros ajenos a la Administración (C630-10, C678-10, C272-10, A33-09, C595-10, C666-10, C958-10)

En otros casos, cuando dentro de la información que se ordena entregar (como,

por ejemplo la copia de Estatutos de un Sindicato determinado, decisión C272-10), se contiene el RUT de personas naturales que no corresponden a funcionarios públicos, se solicita el resguardo de dicho antecedentes pues se le considera dato personal, al cual sólo puede accederse con la autorización de su titular o cuando la ley lo permite, de acuerdo al artículo 4° de la LPDP.

Tratándose de beneficiarios del Estado (particularmente quienes reciben becas o similares como ocurre en las decisiones C630-10 y C678-10), se les aplica el mismo criterio; pues aún cuando este hecho hace que se reduzca el ámbito de la privacidad de estas personas en aras del necesario control social que debe propiciarse en la materia, no se observa de qué modo el conocer el RUT de los beneficiarios pueda revestir interés público para el ejercicio de dicho control.

8.- CORREO ELECTRÓNICO

8.1 Dirección de correo electrónico (C521-10, A140-09)

El Consejo ha estimado que la dirección de correo electrónico constituye un dato personal, de conformidad con lo previsto en la LPDP, por lo que debe protegerse su divulgación.

En el caso C521-10 se dedujo reposición administrativa en contra del pronunciamiento del Consejo sobre un amparo por denegación de información, solicitando que se dejase éste parcialmente sin efecto y, en su reemplazo, se acogiera en forma total el requerimiento planteado, lo que incluía acceder a las direcciones de correo electrónico de entes fiscalizados por una Superintendencia. El Consejo indicó que dicha información no obraba en una fuente de acceso público y, en el caso de las personas naturales (haciendo la distinción respecto de las jurídicas), se trataba de un dato de carácter personal, motivo por el cual, no cabía su tratamiento o cesión, en aplicación de lo dispuesto en los artículos 4°, 7° y 9° de la LPDP. De este modo se acogió la reposición en ese caso, sólo en cuanto a la información relativa a las direcciones de correo electrónico de las personas jurídicas.

8.2 Contenido del correo electrónico (C83-10, C640-10)

Refiriéndose al contenido de un correo electrónico, el Consejo estimó en la decisión C83-10 que la información solicitada (carta enviada desde un particular a la casilla de correo electrónico de un funcionario público) no puede estimarse privada, en los términos del artículo 19 N° 5 de la Constitución Política de la República,

pues ésta versa, exclusivamente, sobre materias objeto de la relación jurídica que mantiene el particular con la Administración del Estado acerca de las consecuencias en la ejecución de un contrato regido por las normas de contratación pública —que tiene en la transparencia uno de sus principios fundamentales—, y producto del desempeño o actividades de un funcionario público, actuando en dicha calidad. En ellas no se expone antecedente alguno acerca de la intimidad o la vida privada del emisor del mensaje, y ha sido formulada en el contexto de la comunicación cotidiana y expedita que debe sostener un particular con la Administración del Estado, cuando ésta es su contraparte en una relación jurídica, no pudiendo sino ser de conocimiento del particular, el carácter público del destinatario y del medio utilizado. Consecuentemente, la divulgación de la información en este caso, no supone una afectación a los derechos del tercero involucrado, en los términos del artículo 21 de la LT. En la decisión correspondiente el Consejo acoge parcialmente el reclamo, requiriendo la entrega de copia íntegra de la información solicitada, pero rechazando la solicitud de entregar la nómina del personal del órgano reclamado a quienes se les divulgó el contenido de los mencionados correos electrónicos, ya que a juicio del Consejo, aquello requeriría

de la elaboración de dicha nómina por no obrar la información en un soporte material en poder de la Administración del Estado, conforme exige el artículo 10, inciso 2º de la misma ley.

Este criterio fue reiterado en la decisión C640-10 en que se solicitó copia de un correo electrónico remitido por un tercero a una funcionaria en el cual el requirente sostenía que se le desprestigiaba. Con todo, en este caso hubo una disidencia del Consejero Jaraquemada quien sostuvo que “los correos electrónicos se encuentran protegidos por la garantía contenida en el artículo 19 N°5 de la Constitución, lo que implica el deber positivo de protección de ese espacio de intimidad y, asimismo, prohíbe acciones u omisiones que puedan afectar el núcleo esencial de este derecho constitucional o su libre ejercicio, pues éstas contravendrían la seguridad que garantiza el numeral 26 del artículo 19 de la Constitución”, que la LT no tiene la especificidad ni la determinación que exige la Constitución para restringir este derecho al no determinar los casos ni las formas en que sería admisible su limitación y que, a diferencia del caso anterior, el mensaje electrónico que se pretende divulgar no versaba “exclusivamente” sobre una petición formulada por un particular a la Administración del

Estado en el ejercicio de funciones públicas, pues contenía también las motivaciones personales del emisor para solicitar ciertos documentos de carácter público, lo que sería parte de su vida privada y habría debido reservarse.

9.- CONCURSO PÚBLICO DE SELECCIÓN DE PERSONAL

En este tipo de concursos, el Consejo ha exigido informar los criterios utilizados para adoptar la decisión final cuando en ella no se ha hecho expresión adecuada de los motivos tenidos a la vista para decidir, afirmando que “el ejercicio de potestades discrecionales no implica una exención del deber de fundamentar las decisiones adoptadas”, particularmente si la persona seleccionada no fue quien tenía el mejor puntaje de entre los postulantes (A39-09).

9.1 Concurso Público General (A34-09, A39-09, A110-09, C91-10, C190-10, C236-10, C368-10, C803-10)

En relación a dos solicitudes de información sobre concurso público para proveer el cargo de Director de un colegio municipal en las decisiones C91-10 y C190-10 (criterio que igualmente es aplicado en las otras decisiones citadas), el Consejo estimó que era necesario distinguir entre la información relativa al propio reclamante y la que le

resulta ajena. Ésta última se diferencia según sea aquella vinculada al postulante seleccionado para el cargo concursado, aquella referida a los postulantes seleccionados en la quina a que se refiere en el artículo 32, inciso 1º, del Estatuto Docente y aquella relacionada con los demás postulantes no seleccionados:

- En cuanto al propio requirente, se estima que tiene derecho a acceder a los puntajes que obtuvo en las distintas evaluaciones que le fueron practicadas, por cuanto se trata de datos personales respecto de los cuales es titular, de acuerdo al artículo 2º, letra ñ) de la LPDP.

- En cuanto al puntaje obtenido por el postulante que fue designado para el desempeño del cargo de Director objeto del concurso a que se refiere la solicitud de acceso, el Consejo autoriza la entrega de los puntajes asignados, concluyendo que la confidencialidad de los procesos de selección de altos directivos públicos termina al finalizar éstos, vale decir, al determinarse la nómina de candidatos a proponer al jefe superior del servicio que corresponde —o al Presidente de la República, en su caso— y seleccionar éste último a uno de los candidatos. Producido lo anterior se aplica plenamente la regla general de publicidad establecida en el

artículo 5° de la LT, pues como afirma el propio artículo 21 N° 1, letra b), los fundamentos de las decisiones son públicos una vez que sean adoptadas.

- En relación a los postulantes seleccionados en la quina del concurso, al no haber sido seleccionados para el cargo, se encuentran en una situación diferente al que sí lo fue, ya que la decisión de postular a un cargo, a juicio del Consejo, no tiene por qué exponerse a la comunidad en caso de no ser exitosa, por lo que ha de mantenerse la reserva de la identidad del postulante.

- Por último en cuanto a los postulantes al concurso (y que no clasificaron a la quina), las tablas requeridas contienen los puntajes por experiencia y perfeccionamiento obtenidos por ellos, debiendo el órgano requerido, por las mismas razones que en el punto anterior, resguardar la identidad de estos postulantes.

Cabe destacar el pronunciamiento que en esta materia y a raíz de un reclamo de ilegalidad interpuesto por un organismo público en el caso A110-09, ha tenido la Corte de Apelaciones de Santiago. Bajo el Rol N° 8067-2009, el Tribunal Superior estimó que no se divisa razón valedera para que el reclamante no entregara al

petionario el informe psicolaboral que le fuera realizado con motivo de su postulación al cargo público, ya que dicho informe fue realizado precisamente en base a los datos de carácter personal e incluso sensibles, que el petionario debió proporcionar al servicio reclamante para el análisis de un especialista evaluador al tiempo de su postulación, consintiendo de paso que ellos, junto con otros antecedentes propios de su personalidad, formaran parte de la evaluación final, con las ponderaciones correspondientes, en los distintos aspectos comprendidos en el examen, por lo que rechazaba el recurso en esta parte. Sin embargo, en el mismo pronunciamiento, la Corte acoge el reclamo en cuanto a la decisión del Consejo de que el Servicio entregue al petionario el informe y evaluación psicológica de la o las personas designadas para el cargo, excluidos los datos sensibles y reservados que pudiese contener, teniendo en especial consideración que no existe para ello, a juicio del Tribunal, autorización o consentimiento del titular de los datos, no constando en autos, por otra parte, que estos terceros que pudieren ver afectados sus derechos, hayan sido notificados de lo que a su respecto se está requiriendo, con lo que no se da cumplimiento a lo dispuesto en el artículo 20 de la LT.

No obstante lo anterior, la sentencia contó con el voto disidente de la ministra Chevesich, quien estuvo por rechazar en todas sus partes el reclamo de ilegalidad interpuesto, en razón de que sólo los terceros que pueden resultar afectados con la publicidad de determinados datos o antecedentes que les conciernen pueden invocar ante el Consejo para la Transparencia la causal establecida en el número 2 del artículo 21 de la LT para obtener mediante la oposición pertinente, el que se desestime la petición de acceso formulada al efecto; razón por la que el órgano reclamante no se encuentra legitimado para invocarla en sede administrativa ni tampoco para fundamentar el reclamo de ilegalidad consagrado en dicha ley. El incumplimiento por parte del órgano público a la normativa señalada, indicó la ministra, no lo faculta para erigirse en una suerte de agente oficioso de aquellos terceros, pues no existe norma legal que lo autorice para ello.

9.2 Concursos realizados en el Sistema de Alta Dirección Pública *(A29-09, A107-09, A186-09, A35-09, A162-09, C488-09, C94-10)*

En la decisión A29-09, el Consejo se pronunció respecto de una solicitud dirigida a la Dirección Nacional del Servicio Civil (DNSC) en orden a acceder a información

sobre el proceso de selección implementado para proveer un cargo de Jefatura en un órgano público y, específicamente, a los resultados de su evaluación personal en el proceso y los resultados de la evaluación de la persona que resultó finalmente nombrada en dicho cargo. Aquí, el Consejo estableció la publicidad de las evaluaciones personales de los candidatos a cargos del Sistema de Alta Dirección Pública, indicando que los postulantes tenían derecho a conocer sus propios informes íntegramente y que los terceros podían acceder a los informes de los candidatos nombrados en el cargo, con la sola exclusión de los datos sensibles y reservados conforme al artículo 2º g) de la LPDP (aplicando en su entrega el principio de divisibilidad). Importante destacar que contrariamente a lo afirmado por el órgano reclamado, el Consejo entiende que aunque el informe psicolaboral haya sido encargado por la DNSC a una consultora externa, el titular de los datos allí contenidos es la persona a que se refieren dichos datos, en este caso, el postulante requirente. Se excluyó de dichos informes los anexos que detallan la información de las personas que dan referencias de los candidatos y el contenido de éstas, pues se entendió que *“en caso contrario la sinceridad de estos testimonios se reduciría y les quitaría buena parte de su valor”*, acogiéndose parcialmente los

amparos respectivos.

Respecto a este Sistema de Alta Dirección Pública, cabe hacer mención a dos pronunciamientos que, en la materia, ha tenido la Corte de Apelaciones de Santiago. En el primero de ellos, bajo el Rol Nº 943-2010 de septiembre de 2010, se acogió el recurso de ilegalidad interpuesto en contra de una decisión del Consejo (A29-09) que ordenaba la entrega de la información solicitada en razón de que la confidencialidad del proceso de selección dispuesta por el artículo 55 de la Ley Nº 19.882 y el secreto de las evaluaciones individuales contemplado en su artículo 50 son exigencias ineludibles, tal y como sucede también con el secreto de las nóminas de candidatos propuestos y de todos los que participaron en el proceso. Sólo un procedimiento con estas características, a juicio del Tribunal, provocará que estén dispuestos a participar todas las personas que se encuentren interesadas, exentos de presiones ex ante o de secuelas negativas ex post, hallándose en la confidencialidad una condición sine qua non para la consecución de esa finalidad. Respecto de la defensa de derechos de terceros, la reserva se manifiesta como algo evidente para el Tribunal, dado que en la evaluación psicolaboral constan apreciaciones del examinador que fuera

del contexto técnico y experto en que ellas se emiten, pueden estimarse que dañan la dignidad de la persona, sobre todo si ha sido objetiva, rigurosa y carente de preferencias o prejuicios lo que, además, expondría a los evaluadores al escrutinio descontextualizado y, en la mayoría de los casos, realizado por quienes carecen del conocimiento y las habilidades necesarias para dimensionarlo adecuadamente.

Sin embargo, en el mes de noviembre del mismo año, la Corte rechazó, bajo el Rol Nº 2080-2010, un recurso de ilegalidad interpuesto en contra de una decisión del Consejo que ordenaba la entrega de la información solicitada (A90-09), en el entendido que tanto la LT como la Ley Nº 19.882 llevan a concluir que la confidencialidad del proceso de selección que lleva a cabo la reclamante de ilegalidad, termina al finalizar éste, vale decir, al determinarse la nómina de candidatos a proponer al jefe superior del servicio que corresponda. Producido lo anterior, razona la Corte, se aplicaría plenamente la regla general de publicidad establecida en el artículo 5º de la LT, pues como afirma el propio artículo 21 Nº 1 b), los fundamentos de las decisiones son “públicos una vez que sean adoptadas”. Esta última sentencia está recurrida de queja bajo el Rol Nº 9065-2010.

10.- FUENTES ACCESIBLES AL PÚBLICO (C521-10, C610-10, C867-10)

Se trata de todos los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes (artículo 2º, letra i) LPDP).

En uno de los casos, ya citado anteriormente, se dedujo reposición administrativa en contra del pronunciamiento del Consejo sobre el amparo por denegación de información Rol C521-10 (el que se acogió en parte), solicitando que se dejase parcialmente sin efecto y, en su reemplazo se acogiera en forma total el requerimiento planteado, lo que incluía las direcciones de correo electrónico de entes fiscalizados por una Superintendencia. El Consejo indicó que dicha información no obraba en una fuente de acceso público y, en el caso de las personas naturales (haciendo la distinción respecto de las jurídicas), se trataba de un dato de carácter personal, motivo por el cual, no cabía su tratamiento o cesión, en aplicación de lo dispuesto en los artículos 4º, 7º y 9º de la LPDP. De este modo se acogió la reposición en ese caso, sólo en cuanto a la información relativa a las direcciones de correo electrónico de las personas jurídicas.

En la decisión C610-10, al Consejo le correspondió resolver si la eventual publicidad de unas patentes municipales autorizaba necesariamente la divulgación de los datos que son de particular interés del reclamante, esto es, el nombre o razón social de los contribuyentes: su dirección, incluyendo calle y número; la ciudad en que ejercen su actividad, y su giro comercial. Frente a ello, el Consejo estimó que dicha información no ha sido recolectada de fuentes accesibles al público, pues se entiende que se trata de antecedentes proporcionados por el contribuyente al solicitar el otorgamiento de la patente municipal respectiva para este sólo efecto, razón por la cual tampoco puede entenderse que ha consentido en su publicidad y, por otra parte, no existe una norma legal que establezca su carácter público en términos generales. No obstante lo anterior, a juicio del Consejo los datos de las personas naturales contribuyentes de patentes municipales, especialmente, los que son de interés del reclamante, en cuanto están directamente vinculados con la actividad gravada, revisten relevancia especialmente sobre las siguientes dos cuestiones, a saber:

- El cumplimiento de los requisitos necesarios para el ejercicio de la actividad que se autoriza por medio de la patente, cuestión que está directamente relacionada

con la publicidad de los datos relativos a los contribuyentes. Así, el conocimiento del nombre del contribuyente, permitiría saber quién ejerce la actividad respectiva y verificar las condiciones subjetivas para el ejercicio de la actividad, lo que es especialmente importante en el caso de la patente que habilita el ejercicio de una profesión; la publicidad del giro o actividad desarrollada por el contribuyente, permitiría conocer si éste cumple con la regulación sectorial correspondiente; y

- Los ingresos que se perciben por concepto de patentes municipales.

En consecuencia, en este caso, el Consejo señala que la reserva de los datos personales que interesan al reclamante podría ceder en beneficio de su publicidad, por el manifiesto interés público que revisten, por lo que acogió el amparo, requiriendo a la Municipalidad reclamada la entrega de la información solicitada.

11.- DATOS PERSONALES Y SUMARIO ADMINISTRATIVO (C617-09, C411-09, C463-10, C847-10, C854-10)

Ante la solicitud de copia del sumario administrativo instruido en contra de determinados funcionarios de una Universidad Pública y respecto de la posible

afectación del derecho a la vida privada de los terceros con la divulgación de esta información (C617-09), el Consejo estimó que aunque hubiesen existido derechos de los ex-funcionarios que pudieren verse afectados, realizando un test de daño, el beneficio de conocer los resultados de un sumario incoado por supuestas irregularidades, que ya es público, así como las medidas que las autoridades tomaron frente a dichas irregularidades, es mucho mayor que el de mantener la información en reserva para proteger la reputación de los sancionados. Si un funcionario incurre en un acto ilegal o irregular es del todo relevante que la ciudadanía conozca dichos actos y las medidas aplicadas para restaurar el imperio del Derecho. La condición de funcionario público, señala, supone un estándar de escrutinio público en el que la privacidad, en lo relativo al ejercicio de dicha función, debe ceder en pos del necesario control social que debe ejercerse para garantizar el debido cumplimiento de aquéllas. Además, el Consejo entiende que el archivo de los expedientes disciplinarios al interior de un organismo, así como el de los actos administrativos que disponen una medida disciplinaria, no constituiría un tratamiento de datos personales según el tenor del artículo 1° de la LPDP, por lo que el artículo 21 de dicha Ley no impediría entregar la copia de un

decreto o resolución como los solicitados en este caso.

En la decisión C411-09, en la cual se solicitaba el acceso a decretos alcaldicios en virtud de los cuales se aplicaron medidas disciplinarias consistentes en la destitución de sus respectivos cargos a la Directora de Obras y a la Jefa del Departamento de Edificación, el Consejo indicó no obstante que en este caso concreto y, aunque de una primera lectura del artículo 21 de la LPDP pareciera proceder la no comunicación de la información requerida, esta vía dejaría abierta la siguiente interrogante a la luz de la Constitución y la LT: si en virtud de la aplicación del artículo 21 citado no se pueden comunicar por parte de los organismos públicos que someten a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, una vez que haya prescrito la acción penal o administrativa o cumplida o prescrita la sanción o la pena, se podría llegar a la conclusión de que los resultados de un sumario incoado en contra de un funcionario público que termine en la aplicación de una medida disciplinaria y que se haya cumplido o haya prescrito, nunca podrá comunicarse, lo que atenta contra el principio de transparencia y publicidad. En vista de lo anterior, agrega el Consejo en este

caso, de acuerdo con la voz “tratamiento” utilizada en el mencionado artículo de la LPDP no se refiere ésta al archivo de actos administrativos que dispongan una medida disciplinaria en contra de un funcionario público, sino más bien al volcamiento de los datos allí contenidos en registros o bancos de datos, según expresamente lo señala el artículo 1° del cuerpo legal citado. Por lo tanto, en el presente caso, no se cumplirían las hipótesis contempladas en el artículo 21 de la Ley, procediendo, entonces, la comunicación o entrega de la información solicitada, acogiéndose el amparo interpuesto.

A mayor abundamiento, el Consejo estimó, en la decisión analizada, que en el evento que hubieren derechos de las ex funcionarias que pudieren verse afectados, realizando un test de daño, el beneficio de conocer los resultados de un sumario incoado por supuestas irregularidades que ya es público, así como las medidas que las autoridades tomaron frente a dichas irregularidades, es mucho mayor que el beneficio de mantener la información en reserva para proteger la reputación o derechos económicos de los sancionados; debido al control social que exige la función pública. El razonamiento anterior, agrega el Consejo, está directamente relacionado con la función que ejercen

los funcionarios públicos (se atiende a la naturaleza o calidad del cargo ejercido por las ex funcionarias). En efecto, en virtud del ejercicio de la función pública, los funcionarios del Estado tienen una vida o esfera privada mucho más restringida que los particulares (A29-09, considerando 10º, letra e).

El mismo criterio se aplica en la decisión C463-10, donde el Consejo reitera que el archivo de los expedientes disciplinarios al interior de un organismo, así como el de los actos administrativos que disponen una medida disciplinaria, no constituiría un tratamiento de datos personales según el tenor del artículo 1º de la LPDP, por lo que el artículo 21 de dicha Ley no impediría entregar la copia de un decreto o resolución como los solicitados en este caso (antecedentes de investigación sumaria efectuada en relación al requirente). El Consejo cita lo indicado por la Contraloría General de la República (CGR) en su Dictamen N° 59.7981-2008, donde señala que el secreto del proceso sumarial tiene por objeto asegurar el éxito de la investigación, el resguardo del debido proceso, la honra y respeto a la vida pública de los funcionarios que, eventualmente, podrían tener comprometida su responsabilidad en los hechos investigados y que las conclusiones a que se llegue en tal proceso sólo que-

dan firme una vez totalmente tramitado. Agrega el Dictamen en comentario, que la resolución que dispone la aplicación de una medida disciplinaria, la absolución o sobreseimiento y los documentos que le sirven de sustento, constituye un acto administrativo sometido al principio de publicidad, aplicable a todos los actos de la Administración, razón por la cual desde que se encuentra totalmente tramitado, procede para los terceros interesados requerir de la autoridad copia del expediente respectivo. Todo lo señalado llevó al Consejo a acoger el amparo interpuesto.

12.- SANCIONES ART. 21 LPDP (C339-10, C111-10, C664-10, C73-10)

El artículo 21 de la LPDP prescribe que los organismos públicos *“que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena”*. Frente a una solicitud de información referente a sumarios sanitarios afinados en los que se hubiera aplicado alguna sanción a personas naturales (C664-10), el Consejo indica que en el caso que dicha sanción hubiere sido cumplida, si bien

el citado artículo 21 establece un manto de protección —pasaría a ser en la nomenclatura de la LPDP un “dato caduco”, conforme lo señala su artículo 2º, letra d) —, debe concluirse que la afectación de dicho derecho ha de ser valorada a la luz del efectivo perjuicio que produciría la entrega de esa información. En tal sentido, indica, es pertinente aplicar un test de daño destacando el elevado interés público que trae consigo el conocimiento de las fiscalizaciones relacionadas con exámenes técnicos a productos agrícolas que podrían originar enfermedades en la ciudad, derivadas de problemas en la sanitización de aguas para riego. Ante ello cede el derecho de las personas naturales que hayan sido sancionadas a no dar a conocer la entidad de dichas medidas, no obstante estar cumplidas.

En otra decisión (C111-10), relacionada con la solicitud de antecedentes relativos a la autorización y funcionamiento de dos locales correspondientes a patentes de Cabaret y Restaurant ante una Municipalidad, el Consejo señaló que en cuanto a las infracciones cursadas a cada contribuyente por el Juez de Policía Local, cabía hacer presente que tales juzgados son tribunales especiales; siendo el Juez de Policía Local designado por la Municipalidad que corresponde, a propuesta en terna de la

Corte de Apelaciones respectiva. En ese contexto, y encontrándose en poder del municipio las resoluciones dictadas por dicho tribunal en las que se impongan sanciones por las citadas infracciones, conforme lo dispone el artículo 5° de la LT, éstas debiesen ser entregadas al reclamante. Sin perjuicio de lo anterior, agrega, en caso de que las sanciones a las que se refieren las resoluciones que hayan cursado tales infracciones se encuentren cumplidas o prescritas, en conformidad con el artículo 21 de la LPDP, éstas no podrán ser comunicadas al solicitante.

Igualmente y respecto de un requerimiento de copias de las sanciones que les fueron aplicadas a funcionarios públicos de las que se da cuenta en los memorándums respectivos (C73-10), el Consejo señala que la aplicación del artículo 21 de la LPDP ha sido interpretada en la decisión C411-09 (ya analizada) donde se estimó que en el evento que hubieren derechos de los ex funcionarios que pudieren verse afectados, realizando un test de daño el beneficio de conocer los resultados de un sumario incoado por supuestas irregularidades, que ya es público, así como las medidas que las autoridades tomaron frente a dichas irregularidades, es mucho mayor que el beneficio de mantener la información en reserva para proteger

la reputación o derechos económicos de los sancionados, debido a que así lo exige el control social de la función pública. El razonamiento anterior, agrega el Consejo, está directamente relacionado con la función que ejercen los funcionarios públicos involucrados (se atiende a la naturaleza o calidad del cargo ejercido por las ex funcionarias). En efecto, en virtud del ejercicio de la función pública, los funcionarios del Estado tienen una vida o esfera privada mucho más restringida que los particulares. Por ello, en definitiva, se ordena entregar lo solicitado.

A este respecto pueden consultarse los criterios expuestos en el punto 6.3 de las Recomendaciones del CPLT sobre protección de datos personales por parte de los órganos de la Administración del Estado, incluida en este documento.

13.- DATOS PERSONALES Y DENUNCIAS (A53-09, A58-09, A91-09, C520-09, C56-10, C302-10, C781-10, C744-10)

Frente a una solicitud de información acerca de expedientes relativos a multas aplicadas por la Dirección del Trabajo (A53-09), el Consejo reconoce que a pesar de la publicidad de aquéllas, cierta parte de la información contenida en los

expedientes solicitados por el reclamante podría contener datos personales e incluso sensibles de terceros, los que deberían ser protegidos de acuerdo a los artículos 2°, 4°, 7°, 10 y 20 de la LPDP. Por otro lado, agrega, no se puede desconocer la naturaleza especial de las denuncias realizadas por los trabajadores ante la Dirección del Trabajo y el riesgo de que su divulgación, así como la de la identidad de los denunciantes o la de los trabajadores que han declarado en un proceso de fiscalización en contra del empleador, afecte su estabilidad en el empleo o los haga víctimas de represalias (especialmente si se mantienen laboralmente vinculados con el mismo empleador). Por consiguiente, respecto de aquellos datos personales, 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 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 LT. Lo anterior y en aplicación del principio de divisibilidad, no constituye obstáculo, entiende el Consejo, para la obligación de entregar la restante información contenida en los expedientes

solicitados, al no estar ésta amparada por causal de secreto o reserva alguna. Se acoge aquí parcialmente el amparo interpuesto.

En el caso de denuncias realizadas ante Carabineros de Chile (A58-09), el Consejo estimó que la relación del nombre de un denunciante con las denuncias o reclamos respectivos puede, ciertamente, afectar derechos de los que es titular, como el derecho a la vida privada o privacidad o el derecho a su honra o imagen. Por lo anterior, el Consejo reconoce que la divulgación o entrega de los nombres de todos los denunciantes o reclamantes solicitados por el requirente podría inhibir futuras denuncias o reclamos ante la Subsecretaría de Carabineros. De la misma manera, el Consejo estima necesario distinguir si la denuncia o reclamo presentado proviene de una autoridad pública o de un particular:

- En el caso de los reclamos o denuncias presentados por autoridades públicas, o por funcionarios públicos en el ejercicio de su cargo o función pública, no puede sostenerse que la revelación de sus identidades fuese a causarles algún perjuicio. En efecto, conforme el artículo 30, inciso 3º, letra a) de la Ley Nº 19.733, sobre las libertades de opinión e información y

ejercicio del periodismo, se consideran como hechos de interés público de una persona los referentes al desempeño de funciones públicas; de manera que si la denuncia o reclamo se efectúa invocando una función de esta naturaleza o detentando la calidad de autoridad (sea en el ámbito de la Administración del Estado, del Congreso Nacional o de cualquiera otra de las autoridades establecidas en la Constitución) la identidad deberá ser revelada sin más, entregando los nombres completos.

- Tratándose de los reclamos o denuncias presentados por particulares el organismo reclamado deberá comunicarles, en caso que considere que la revelación de su identidad podría afectar sus derechos, mediante carta certificada, la facultad que les asiste para oponerse a la entrega de su identidad, en conformidad con el artículo 21 Nº 2 y el artículo 20 de la LT. Lo anterior, indica el Consejo, reducirá el número de comunicaciones a terceros que deban realizarse en virtud del artículo 20 de la LT, con lo que se estima que no se distraerá en forma indebida a los funcionarios de las funciones del órgano reclamado ni se afectarán, en consecuencia, sus funciones habituales.

En el caso en estudio y por las ra-

zones expuestas, se acogió parcialmente el amparo.

Igual criterio fue aplicado tratándose de denuncias ante una Municipalidad (C520-09), estableciéndose que el acceder a la entrega del nombre de él o los denunciantes de determinadas obras a realizar en un edificio de la comuna o el reporte de determinados ruidos molestos, podría inhibir a realizar futuras denuncias e impedir que los órganos de la Administración, como las Municipalidades, realicen las fiscalizaciones necesarias que surgen de dichas denuncias. Por otra parte, en este caso no se percibía un interés público en conocer dicha información, denegándose el acceso solicitado.

14.- DATOS PERSONALES Y BENEFICIOS OTORGADOS POR EL ESTADO

14.1 Datos de Evaluadores (C221-10)

En relación a una consulta llevada a cabo ante CONICYT, específicamente en lo relativo al acceso al Currículo Vitae ciego con los nombres, títulos, las calificaciones académicas y profesionales, de los tres evaluadores que revisaron y calificaron la postulación presentada por la peticionaria/postulante a una beca, el Consejo destaca que ha sentado como principio fundamental

el que la esfera de privacidad de las personas que trabajan para la Administración del Estado —en este caso, ejerciendo una función pública específica aunque sea bajo un contrato a honorarios—, es más reducida que la del resto de las personas, en virtud, precisamente, de las funciones que éstos ejercen. Así las cosas, se ha resuelto en otras decisiones la entrega del currículum vitae de particulares que se hallan en poder de la Administración del Estado, para lo cual ha considerado el interés público comprometido, la imparcialidad de los procesos de licitación y concurso y su control por la ciudadanía. Según lo razonado precedentemente, el Consejo estima que la información tanto del currículum vitae ciego, así como del nombre de los evaluadores que calificaron y evaluaron los antecedentes de la solicitante, constituye información de carácter público que debe ser entregada a quien la solicita, lo que llevará en definitiva a acoger el amparo. En este caso, además, existió la oposición de los terceros, quienes estimaban que proporcionar a los postulantes a estos concursos tal información, implicaría un grave riesgo al exponer a los evaluadores a eventuales presiones indebidas por parte de los evaluados, sus recomendadores u otras personas naturales o jurídicas que puedan tener interés en que los resultados de sus postulaciones sean favorables,

lo cual desvirtúa claramente y pone en riesgo la imparcialidad en los procesos de evaluación respectivos. Al respecto, el Consejo estimó que no se vislumbra de qué manera podrían producirse los perniciosos efectos de que temen los opositores, especialmente tratándose de antecedentes que reflejan una opinión técnica de su parte, como expertos en sus respectivas áreas, que ya se ha informado y entregado a la autoridad competente de asignar los correspondientes beneficios, lo que descarta la posibilidad de que se produzcan presiones indebidas o que exista riesgo alguno en relación con la imparcialidad del proceso. Por lo demás, finaliza, en este caso no es posible vincular la identidad de los evaluadores con su calificación concreta, lo que disuelve el riesgo alegado.

14.2 Datos de donantes y beneficiarios (C361-10, C678-10, C488-10, C831-10, C893-10, C968-10)

Se solicitó al organismo reclamado un listado de las donaciones que Universidades, Institutos Profesionales y Centros de Formación Técnica recibieron durante un período determinado, en virtud de la Ley N° 18.681, con la individualización del donante, el monto donado y la institución de educación superior beneficiada (C361-10). El Consejo consideró que la

calidad de donante revela la calidad de beneficiario de una exención tributaria por parte del Estado de Chile —consistente, en definitiva, en un descuento en el monto del pago que el contribuyente debe realizar por concepto de impuesto de Primera Categoría o Global Complementario—, por lo que el conocimiento de dicha información propicia el control social sobre el reconocimiento de la calidad de donante por parte del organismo reclamado y, en consecuencia, la procedencia o no del otorgamiento de tal beneficio al donante de que se trate —máxime si se trata de la aplicación voluntaria, a una determinada institución de Educación Superior que se escoja, de sumas de dinero por parte de contribuyentes en los términos previstos en la Ley, sumas que, de no mediar tal donación, estarían íntegramente gravadas con impuestos—, circunstancia que le lleva a considerar que, en este caso, la reserva de tales datos debe ceder en beneficio de su publicidad, por el manifiesto interés público que revisten.

En el caso C488-10 se resolvió que la identidad de donantes que no recibían beneficios tributarios debía reservarse salvo si eran personas jurídicas, pues en tal caso no las amparaba la LPDP, con la disidencia del Consejero Jaraquemada que estimó que aún respecto de ellas debía

valer la reserva pues ninguna finalidad pública justificaba revelar su identidad. En cambio, hubo unanimidad para entregar los datos de un donante en la decisión C758-10 por estimarse que en este caso había un interés público en conocer la información, considerándose que existía un potencial conflicto de interés entre donante y donatario.

En otra decisión y frente a la solicitud de información realizada en relación con la Beca de Integración Territorial (C678-10), el Consejo reitera la lógica en cuanto a que el recibir un beneficio del Estado hace que se reduzca el ámbito de la privacidad de las personas que gozan de éstos; en aras del necesario control social que debe propiciarse en la materia, y del hecho que esté asentado el criterio de publicidad en torno a quienes reciben tales beneficios del mencionado Estado, por lo que se acogió aquí el amparo respectivo.

15.- TEST DE DAÑO APLICADO A LA PROTECCIÓN DE DATOS (617-09, 664-10)

En un caso ya analizado y en el que se solicitaba copia del sumario administrativo instruido en contra de determinados funcionarios de una Universidad Pública, el Consejo estimó que si hubiesen existido

derechos de los ex–funcionarias que pudiesen verse afectados, realizando un test de daño, el beneficio de conocer los resultados de un sumario incoado por supuestas irregularidades, que ya es público, así como las medidas que las autoridades tomaron frente a dichas irregularidades, es mucho mayor que el de mantener la información en reserva para proteger la reputación de los sancionados. De este modo, el Consejo resolvió la entrega del sumario requerido, revelando las sanciones administrativas ya cumplidas.

16.- TEST DE INTERÉS PÚBLICO APLICADO A LA PROTECCIÓN DE DATOS (C335-10, C626-10)

En relación a una solicitud efectuada ante una Municipalidad, consistente en la copia de una carta escrita por una ex subordinada del requirente, en la que, a su juicio, se haría referencia a supuestas conductas que mancillan su calidad profesional y honra, el Consejo indicó que por aplicación del artículo 5º, inciso segundo, de la LT, la información materia del amparo sería en principio pública. Sin perjuicio del principio general antes constatado, el Consejo ha estimado en casos similares (A115-09 y A244-09) que habiendo oposición de un tercero es indispensable verificar el daño que éste sufriría de entregarse la

información y aplicar lo que en doctrina se ha llamado un “test de interés público”, a efectos de determinar si existe un interés público que justifique la divulgación de la información o si, por el contrario, debe prevalecer su reserva para resguardar los bienes jurídicos protegidos por la ley, concretamente los derechos del tercero que se opuso, en este caso la vida privada y la salud de la autora de la carta, que serían vulnerados de publicarse la información requerida. En este sentido, el Consejo estimó especialmente que al momento de ser presentada la carta en comento, su autora dependía laboralmente de la calificación que el reclamante hiciese de su labor. En este contexto, se entendió que resultaba razonable el temor a que su divulgación afectara por una parte el ámbito de su vida privada y su salud y, por otra, desincentivara el ejercicio de análogas denuncias a otras personas en similares circunstancias, configurándose de esta forma y respecto de aquellos datos la causal del artículo 21, numeral 2 de la LT, causal que se encuentra reforzada por la especial función que el artículo 33, letra m), de la LT encomienda al Consejo, en orden a velar por el adecuado cumplimiento de la LPDP por parte de los órganos de la Administración del Estado. En cuanto al interés público que podría representar la publicidad del documento solicitado, el

Consejo consideró que no se encuentra suficientemente acreditado el hecho de que la carta escrita constituya el fundamento de la decisión de poner término al contrato que mantenía el solicitante con la Municipalidad reclamada, como aquél señala. Por todo lo anterior, el Consejo estimó reservada la información solicitada y rechazó el reclamo interpuesto.

17.- CURRÍCULUM VITAE DE LOS FUNCIONARIOS PÚBLICOS (C94-10, C279-10, C264-10)

En el caso C94-10, se solicita al organismo respectivo, información concerniente a la experiencia laboral y curricular de quienes superaron la primera etapa en el proceso de selección de personal que indica. Al respecto, el Consejo señaló que encontrándose la información requerida en el currículum vitae de los postulantes, documento que por su naturaleza expone eminentemente datos de carácter personal, estimaba que en aplicación del principio de divisibilidad en materia de acceso a la información, es posible hacer entrega al reclamante de dicho documento, sin afectar los derechos de las personas involucradas, mediante la tacha de toda aquella información que permita la individualización del titular de los datos que serán revelados (como lo serían nombres,

apellidos, RUT, domicilio, teléfono, fax, casilla de correo electrónico, etc.).

En otras solicitudes en que se pide el currículum vitae de funcionarios públicos determinados (C279-10), el Consejo señala que tratándose del currículum vitae de aquel personal empleado en los órganos y servicios públicos, sólo el acceso a dicha información permite a la ciudadanía evaluar las capacidades de la persona seleccionada para desempeñar su labor, resguardando el adecuado ejercicio de las funciones públicas. Por ende, no puede existir afectación del derecho de un determinado funcionario por dar a conocer información necesaria para acreditar su capacidad e idoneidad funcionaria. Se ha establecido, por consiguiente, que son datos necesarios para evaluar las capacidades para el desempeño de las labores encomendadas, los siguientes: trayectoria académica, profesional, laboral y aquellos que acrediten su capacidad, habilidades o pericia para ocupar el cargo público. Lo anterior, sin embargo, debe ir acompañado de la tacha de aquellos datos que no tienen por objeto evaluar las antedichas capacidades, sino que aparecen incorporados meramente como datos de contexto de los mismos, como son por ejemplo, el número de cédula de identidad, domicilio particular o profe-

sional, fecha de nacimiento, nacionalidad, estado civil, teléfono y correo electrónico particular, entre otros.

18.- TRATAMIENTO DE DATOS (C383-10, C351-10, C876-10, C925-10, C885-10, C39-11, C929-10, C23-11)

En la decisión C383-10, el organismo reclamado señaló que la información solicitada era posible encontrarla en el sitio Web del mismo, para lo cual era necesario ingresar datos personales como el nombre, apellido, casilla de correo electrónico, ocupación, compañía, sexo, estado civil, dirección, ciudad, región, país, número telefónico y fax. El Consejo indicó que los incisos primero y segundo del artículo 4º de la LPDP, disponen 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”* y *“la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público”*. A la luz de lo dispuesto en las normas precitadas, concluye el Consejo que condicionar la entrega de la información a que el solicitante autorice el tratamiento de aquellos datos personales que el organismo exige para la

incorporación a su registro de usuarios es contrario al principio de facilitación, pues obstruye el acceso a la información pública al interponer un requisito adicional que no tiene por fundamento ninguna de las hipótesis previstas en el artículo 17 de la LT; y, asimismo, contraviene el requisito de “consentimiento” para el tratamiento de datos personales, consagrado en el artículo 4° de la LPDP, toda vez que la manifestación de voluntad destinada a autorizar dicho tratamiento tiene por causa una condición o requisito impuesto por un órgano de la Administración del Estado para la entrega de información pública, contraviniendo el presupuesto de libertad implícito en toda manifestación de voluntad.

En el caso C351-10 ya citado en el numeral 3.2 del presente informe, el Consejo indicó que de no contar con el consentimiento del titular de datos personales para el tratamiento de los mismos, según la regla general del artículo 4° de la LPDP, un organismo público únicamente puede tratarlos cumpliendo dos supuestos: efectuarse respecto de materias de su competencia y bajo la sujeción a las disposiciones de la LPDP (artículos 7 y 20). En relación al primer supuesto, el artículo 217 del DFL N°1/2005, establece que el organismo reclamado almacena los datos entregados directamente por las ISAPRES respectivas,

en cuyo tratamiento debe cumplir con los supuestos previstos en el artículo 20 de la LPDP (ya indicados). De esta conclusión se desprende lo siguiente

- El titular de dichos datos tiene limitados sus derechos de solicitar la modificación, cancelación o bloqueo de dichos datos, no obstante lo cual el tratamiento de datos personales efectuados por un organismo público, como es el caso, debe respetar los principios de finalidad, consagrado en los artículos 4° inciso 2° y 9 y de seguridad, consagrado en los artículos 5° y 11°, todos de la LPDP, entre otros.

- Al tratarse de datos aportados directamente por las ISAPRES, y al no constituir información que deba mantener disponible al público, se descarta la aplicación del artículo 4° inciso 5° de la LPDP, por cuanto dichos datos no obran en poder del organismo reclamado por haber sido recolectados de fuentes accesibles al público.

En consecuencia, señala el Consejo, al tratarse el requerimiento de la especie de una solicitud de acceso parcial a una base de datos personales, cuyo tratamiento se da en las condiciones señaladas precedentemente, otorgar el acceso a dicha información en esta sede

implica inequívocamente una intromisión a la vida privada de los titulares de dichos datos, sin que éstos hayan consentido en su utilización para fines diversos.

19.- OBLIGACIONES TRIBUTARIAS Y PROTECCIÓN DE DATOS (A265-089, C403-11)

En la primera de las decisiones citadas, se pedía el acceso a la base de datos de las empresas con domicilio en una Región determinada, que a la fecha de la solicitud se encontraran morosas en el pago de impuestos al valor agregado, con indicación del nombre, RUT y otra individualización que las identificara. En el caso de las personas naturales, se concluyó que la divulgación de deudas tributarias contrariaba lo dispuesto por el artículo 17 de la LPDP, toda vez que ésta norma regula especialmente la divulgación de datos personales relativos a obligaciones de carácter económico y comercial, estableciendo el carácter lícito de su comunicación, exclusivamente, respecto del tipo de obligaciones económicas y los instrumentos que taxativamente en él se indican. Tratándose de personas jurídicas, indicó el Consejo que si bien no resultaba aplicable la LPDP, de acuerdo al artículo 2° del mismo cuerpo legal, la honra de la persona jurídica sí encontraba protección

al no distinguir nuestro constituyente en el encabezado del artículo 19 de la CPR entre personas naturales y jurídicas. Por todo ello, el Consejo optó por rechazar el amparo. En voto concurrente el consejero Olmedo estimó que el daño a estas personas no era a su honra, sino que a la afectación de derechos de carácter comercial y económico expresamente contemplados en la causal de reserva prevista en el artículo 21 N° 2 de la LT. Por último, esta decisión contó con el voto disidente del consejero Ferreiro, quien fue partidario de acoger el amparo en el caso de las personas jurídicas, pues respecto de ellas, a su juicio, ni procedía la protección del artículo 17 de la LPDP ni la afectación de sus derechos.

En la decisión C403-11 se modificó el criterio anterior sentando una nueva línea jurisprudencial. En este caso lo solicitado era un listado de todas las ejecuciones fiscales iniciadas durante un período determinado, excluidas aquellas por impuesto territorial, con indicación, entre otros, de los datos de Rol de la causa, comuna, nombre y razón social, RUT, domicilio del deudor, etc. El Consejo determinó que las deudas tributarias constituyen el reflejo de cargas públicas, cuyo cumplimiento tiene un evidente interés público que justifica su publicidad y agregó que, si bien el artículo 17 de la LPDP proscrib

con carácter general la comunicación de deudas a terceros, lo permite tratándose de deudas que consten de una manera indubitada, esto es, de deudas cuyo fundamento y exigibilidad es claro. Por otro lado, una de las excepciones en que se permite el tratamiento de estos datos es "...el incumplimiento de obligaciones derivadas de... créditos de... organismos públicos". Tratándose de las deudas que constan en las listas o nóminas de los deudores que se encuentren en mora, firmadas por el Tesorero Comunal que corresponda, se estimó que adquirirían el carácter de indubitadas una vez que transcurra el plazo para oponer excepciones y éstas no se deducen o, habiéndose deducidas, hubiesen sido rechazadas por el juez civil. Una interpretación contraria, agregó, importaría una discriminación irrazonable respecto del Fisco acreedor, pues al permitir difundir el pago de las obligaciones contraídas con acreedores privados que consigna el artículo 17 de la LPDP se genera una herramienta para agilizar su pago, la que no tendrían las acreencias públicas que, en este contexto, serían postergadas por los deudores. Reconociendo el Consejo que la reserva de la calidad de deudor de tributos constituye un interés para quienes la tienen, indicó que éste no alcanza el estándar de un derecho afectado, que es el supuesto que

exige el artículo 21 N° 2 LT. Por último, se señaló que el correcto funcionamiento de los mercados requiere la mayor disponibilidad de información posible acerca del nivel de cumplimiento de las obligaciones comerciales de quienes participan en él, por lo que el ocultamiento del historial de cumplimiento de las obligaciones tributarias afecta negativamente el interés público. Lo razonado, indicó, regía tanto para personas naturales como jurídicas, pues al no haberse aplicado el artículo 17 de la LPDP, no existirían razones que ameritasen distinguir entre unas y otras. En definitiva, se acogió parcialmente el amparo, excluyendo la entrega de los domicilios de los contribuyentes personas naturales, por constituir un dato personal protegido en virtud de los artículos 4° y 7° de la LPDP.

20.- AFILIACIÓN SINDICAL Y PROTECCIÓN DE DATOS

20.1 Identidad de los trabajadores afiliados a un sindicato (C108-10, C250-10, C866-10, C839-10, C59-11, C188-11, C492-11 y C532-11)

La solicitud de entrega de la identidad de los trabajadores que integran un sindicato, requerida a las Inspecciones del Trabajo, ha sido analizada en diversas oportunidades por el Consejo, estableciéndose criterios

que han variado en el tiempo, en un primer momento disponiendo su entrega y, en la actualidad, prescribiendo la reserva.

Dentro de los casos en que se ha acordado la entrega de la información, acogiendo el amparo respectivo, destacan los siguientes:

· En el caso C108-10 lo solicitado eran las nóminas de los afiliados a un sindicato, de quienes participaron en su constitución y las solicitudes de afiliación respetivas, así como los documentos relacionados con dichas afiliaciones. El solicitante es el empleador, en el contexto de un procedimiento de negociación colectiva en que se debatía ante la Inspección respectiva qué trabajadores eran parte de este procedimiento. En su decisión el Consejo dispuso la entrega de las identidades de los trabajadores, afirmando que con ello no se afectaban sus derechos ni los del sindicato dado que "...la legislación laboral se ha encargado de establecer elementos disuasivos a los empleadores en el ejercicio de represalias en contra de los miembros de los sindicatos, con un marco jurídico sancionatorio aplicable a los empleadores que incurran en tales prácticas, pudiendo concluirse que, en el presente caso, no se han acompañado antecedentes que hagan presumir la concurrencia de un daño

presente, probable y específico". En la decisión C250-10, en la que lo solicitado era la copia del registro de participantes del sindicato de trabajadores también por parte del empleador, se siguió el mismo criterio, con un voto disidente del Consejero Olmedo, quien estuvo por resguardar las identidades en virtud del artículo 21 N° 2 de la LT (afectación de los derechos de las personas) y los principios enunciados en los Convenios de la OIT N° 87 y N° 98, sobre libertad sindical y negociación colectiva.

· En el caso C866-10, donde lo solicitado fueron las actas de votación de la reforma de estatutos de un sindicato, el Consejo rechazó la oposición de aquel por estimar que no lograba justificar la concurrencia de un "daño presente, probable y específico" a sus derechos, ordenándose la entrega de la información requerida. En voto disidente, el consejero Jaraquemada estimó que lo solicitado constituía información de origen y naturaleza privada, que debía resguardarse en razón de la autonomía de los sindicatos en tanto cuerpos intermedios (artículo 1°, inciso 2°, de la Constitución Política de la República).

· En el amparo C188-11 una empresa solicitó la nómina de los trabajadores afiliados a su sindicato, disponiendo el

Consejo la entrega de la información requerida por no concurrir la causal de reserva del artículo 21 N° 2 de la LT (afectación de los derechos de las personas) pues, aún cuando se trate de datos personales (nombres y cédulas de identidad), "...el amparo de tales datos cede ante el interés público prevalente consistente, por una parte, en velar por el cabal cumplimiento de las exigencias legales necesarias para la constitución definitiva de un sindicato, conforme a lo dispuesto en el inciso segundo del artículo 227 del Código del Trabajo, especialmente por parte de la empresa a la que éste pertenezca, como también en la supervigilancia del correcto ejercicio de las funciones públicas asignadas a la Dirección del Trabajo vinculadas a la cabal verificación de tales requisitos". Disidente de la mayoría los consejeros Olmedo y Jaraquemada por dar prevalencia a la protección de los datos de aquellos trabajadores cuya afiliación sindical se requiere⁴.

Por otra parte, las siguientes decisiones estimaron que debía darse protección a la identidad de las personas afiliadas a un sindicato, primero en casos específicos y luego de modo general, sentando un cambio del criterio jurisprudencial anteriormente expuesto:

· En el caso C432-10, frente a una solicitud de copia del acta de una elección sindical, el organismo reclamado proporcionó al peticionario no sólo el acta, sino también el detalle de la votación y sus partícipes, con indicación de su nombre, RUT y firma. El Consejo, en su decisión, representó al órgano reclamado no haber tarjado, en aplicación del principio de divisibilidad (artículo 11, letra e), de la LT, los datos personales señalados y los de contexto del delegado electo, tales como su RUT, domicilio, nacionalidad, fecha de nacimiento y número de teléfono celular; tanto por estar protegidos por la LPDP, como por no haber sido todos éstos solicitados y, por último, por infringir el secreto electoral establecido expresamente en el artículo 221, inciso 2°, del Código del Trabajo⁵, al indicarse que la decisión fue unánime.

· En el amparo C839-10 una empresa solicitó la identidad de los participantes en la elección y/o renovación del directorio de un sindicato, resolviendo el Consejo acogerlo en forma parcial, pues únicamente autorizó la entrega del número de afiliados que participaron en la renovación del directorio sindical y reservó las identidades de los mismos en virtud del artículo 21 N° 2 de la LT (afectación de los derechos de las personas). Lo anterior, fundado en que en este caso su difusión afectaba derechos

de esta organización, en concreto, su consolidación como sindicato, dado que estaba constituido provisoriamente bajo la modalidad especial contemplada en el artículo 227, inciso segundo, del Código del Trabajo⁶, existiendo durante el periodo provisional un riesgo cierto, probable y específico de afectar la libertad sindical, con el consiguiente perjuicio a la organización misma e, incluso, a los derechos de sus afiliados⁷. Idéntico criterio se sostuvo en el amparo C59-11, en el que una empresa solicitó fue el listado de trabajadores que concurrieron a la constitución del sindicato, resolviendo el Consejo rechazar el amparo interpuesto pues su difusión podría afectar la libertad sindical de constitución dado que también estaba constituido bajo la modalidad provisional contemplada en el artículo 227, inciso segundo, del Código del Trabajo.

· En las últimas decisiones sobre esta materia, C492-11 y C532-11, el Consejo consolidó este cambio jurisprudencial, dando prevalencia a la protección de la identidad de los trabajadores afiliados a un sindicato, pese a no tratarse de sindicatos en formación bajo la modalidad provisional que protegieron las decisiones recién explicadas. En los amparos respectivos se solicitó, por parte de las empresas respectivas, la nómina de los

participantes en una elección de delegados sindicales (C492-11) y en la constitución de un grupo de sindicatos interempresas (C532-11), resolviendo el Consejo que dicha información constituye un registro o base de datos y su divulgación, una comunicación o transmisión de los mismos, de acuerdo a lo dispuesto en el artículo 2° LPDP. Divulgar el dato personal afiliación sindical, razona, podría permitir que las empresas verificaran el cumplimiento de los requisitos legales e impugnaran los actos electorales; sin embargo, en aplicación del test de daño y de interés público, se estimó que dicha verificación resulta garantizada mediante la participación del inspector del trabajo u otro ministro de fe en tales actos, existiendo, además, una vía especial en la legislación laboral para impugnar dichas actuaciones a través de la acción respectiva ante el tribunal competente. Por consiguiente, se da preferencia a la protección del derecho a la vida privada de quienes concurren a la elección de los delegados respectivos, resolviéndose que la información requerida es secreta. En voto concurrente, el consejero Olmedo agregó al referido razonamiento, que la divulgación de información relativa a la afiliación sindical de una persona vulnera los principios enunciados en los Convenios de la OIT en materia de libertad sindical y negociación colectiva, números 87 y 98,

⁴ Siguiendo la línea argumental de las decisiones antes citadas, el consejero Olmedo estimó que existía vulneración de los principios de los Convenios de la OIT N° 87 y N° 98, sobre libertad sindical y negociación colectiva, a lo que el consejero Jaraquemada agregó que lo solicitado constituía información de origen y naturaleza privada, que debía resguardarse en razón de la autonomía de los sindicatos en tanto cuerpos intermedios.

ratificados por Chile. En cambio, en voto disidente, el consejero Urrutia estuvo por acoger el amparo en virtud de la existencia de un interés público que justificaría levantar la regla de reserva del artículo 7º LPDP, consistente en el adecuado control del ejercicio de las funciones públicas que desempeñan funcionarios públicos que concurren como ministros de fe a la verificación del cumplimiento de los requisitos legales necesarios a la elección de delegados sindicales.

20.2 Instrumentos colectivos y convenios colectivos (C306-10 y C722-10).

En estos casos se solicitaron las cláusulas de un convenio colectivo firmado entre un grupo de trabajadores y su empresa

y la copia de los instrumentos colectivos depositados en una Inspección Comunal del Trabajo determinada, respectivamente. El Consejo resolvió disponer la entrega de la información, reservando la identidad de las personas beneficiadas por el convenio e instrumentos colectivos, en la primera decisión, porque así lo pidió el requirente y, en la segunda, por aplicación de la LPDP. En ambas decisiones, se contó con el voto disidente del consejero Jaraquemada, quien indicó que la información solicitada era de naturaleza privada y sólo obraba en poder del órgano requerido con la finalidad de que ejerciera sus facultades fiscalizadoras sobre el cumplimiento de los convenios e instrumentos colectivos, pero no correspondían a fundamento de un acto ni resolución administrativa alguna.

⁵ Según este precepto, en la asamblea constitutiva de un sindicato "...y en votación secreta se aprobarán los estatutos del sindicato y se procederá a elegir su directorio".

⁶ Según esta norma "...para constituir dicha organización sindical (se refiere al sindicato de empresa) en aquellas empresas en las cuales no exista un sindicato vigente, se requerirá al menos de ocho trabajadores, debiendo completarse el quórum exigido en el inciso anterior, en el plazo máximo de un año, transcurrido el cual caducará su personalidad jurídica, por el solo ministerio de la ley, en el evento de no cumplirse con dicho requisito".

⁷ La decisión contó con los votos disidentes de los consejeros Olmedo y Jaraquemada, quienes estuvieron por rechazar totalmente el amparo, fundados en que la entrega de la información afectaría la autonomía sindical, el primero, pues permitiría que el empleador accediera a información estratégica del sindicato, y el segundo en la consideración de la organización sindical como cuerpo intermedio de la sociedad, que debe gozar de la adecuada autonomía para cumplir sus fines propios en cuanto entidad privada.

III. Análisis Cuantitativo

III. Análisis Cuantitativo

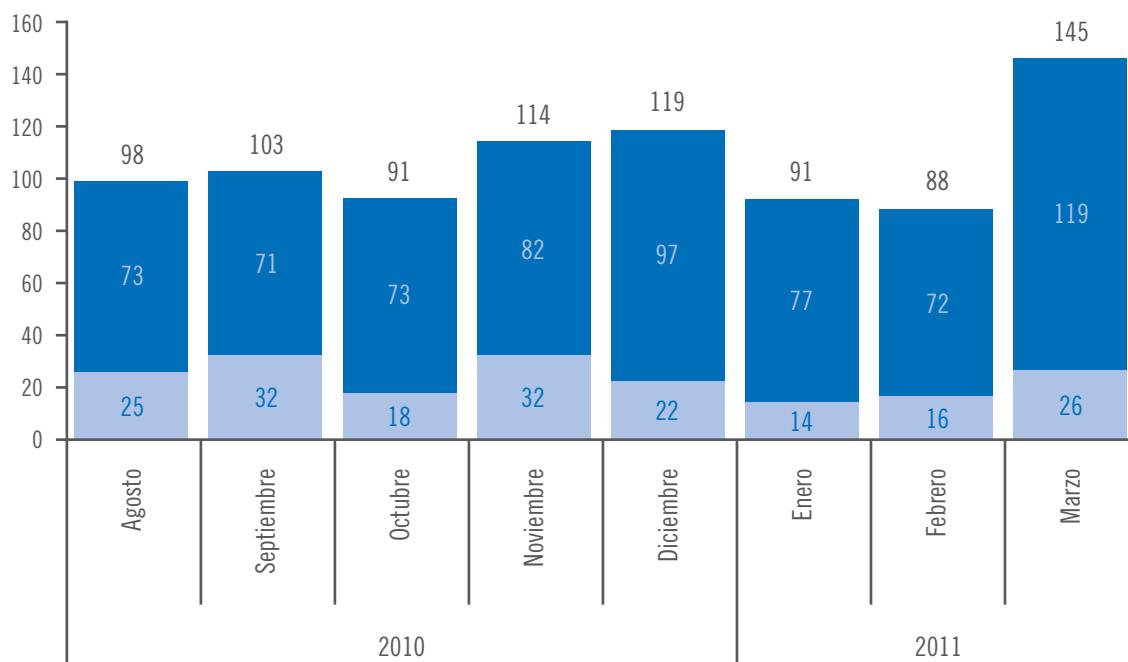
TABLA 1
Número de decisiones con decisión despachada, según su tipo, desglosada según aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

AÑO	MES	DECISIÓN DE FONDO			DECISIÓN INADMISIBLES Y OTROS			TOTAL DECISIONES		
		Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total	Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total	Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total
2010	Agosto	13	31	44	12	42	54	25	73	98
	Septiembre	16	40	56	16	31	47	32	71	103
	Octubre	9	50	59	9	23	32	18	73	91
	Noviembre	16	61	77	16	21	37	32	82	114
	Diciembre	22	49	71	0	48	48	22	97	119
2011	Enero	14	40	54	0	37	37	14	77	91
	Febrero	16	32	48	0	40	40	16	72	88
	Marzo	26	40	66	0	79	79	26	119	145
Total		132	343	475	53	321	374	185	664	849

TOTAL DE DECISIONES DESPACHADAS

GRÁFICO 1

Distribución de Número total mensual de decisiones despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

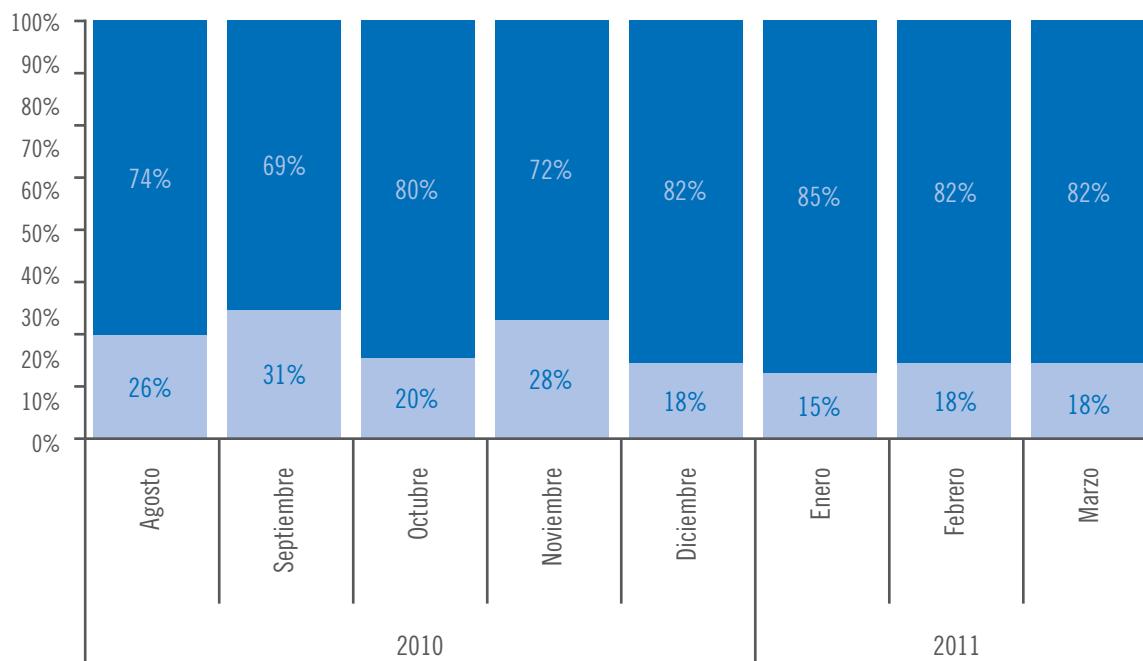


Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
 ■ Con aplicación de Ley de Protección de datos personales

GRÁFICO 2

Distribución de porcentaje mensual del total de decisiones despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



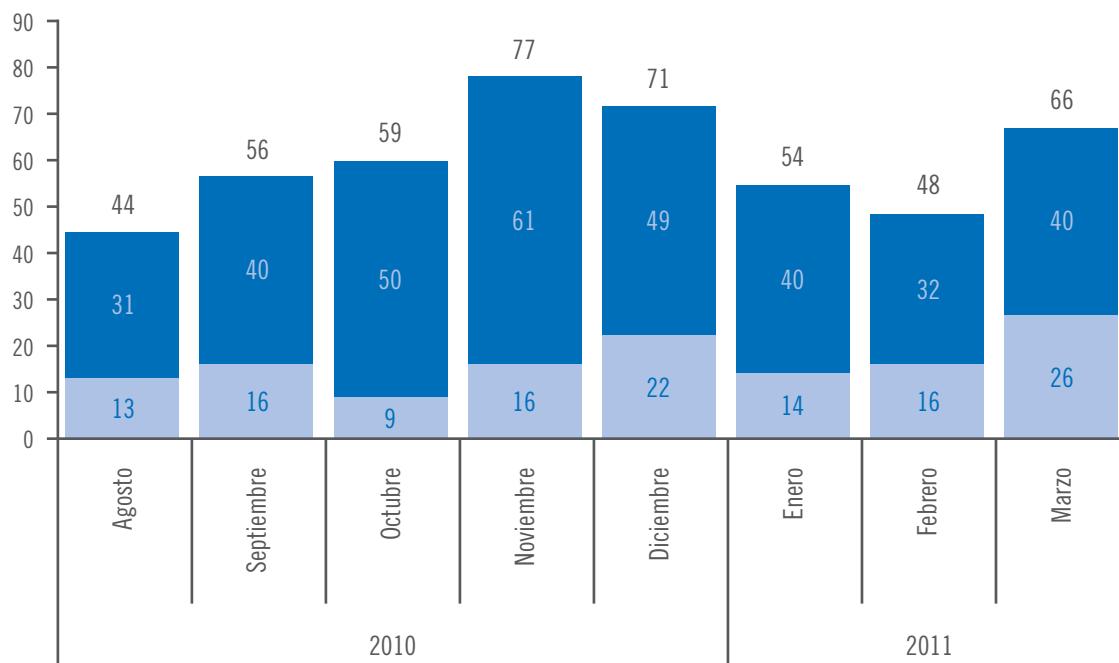
Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
■ Con aplicación de Ley de Protección de datos personales

DECISIONES DE FONDO

GRÁFICO 3

Distribución de Número total mensual de decisiones de fondo despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

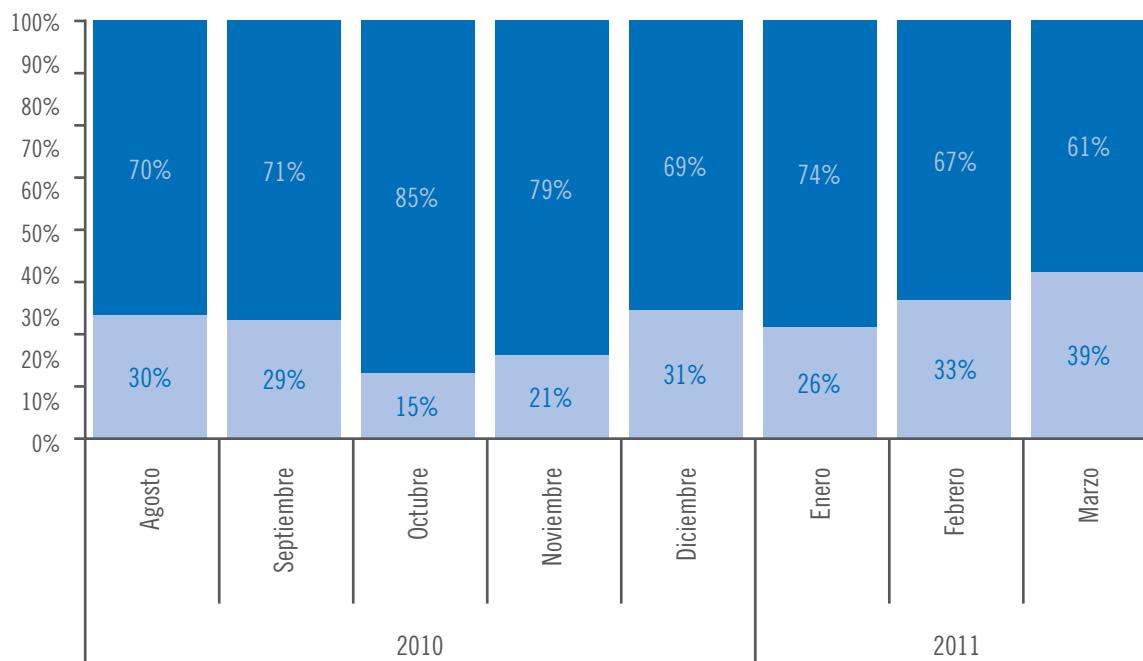


Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
 ■ Con aplicación de Ley de Protección de datos personales

GRÁFICO 4

Distribución de porcentaje mensual del total de decisiones de fondo despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



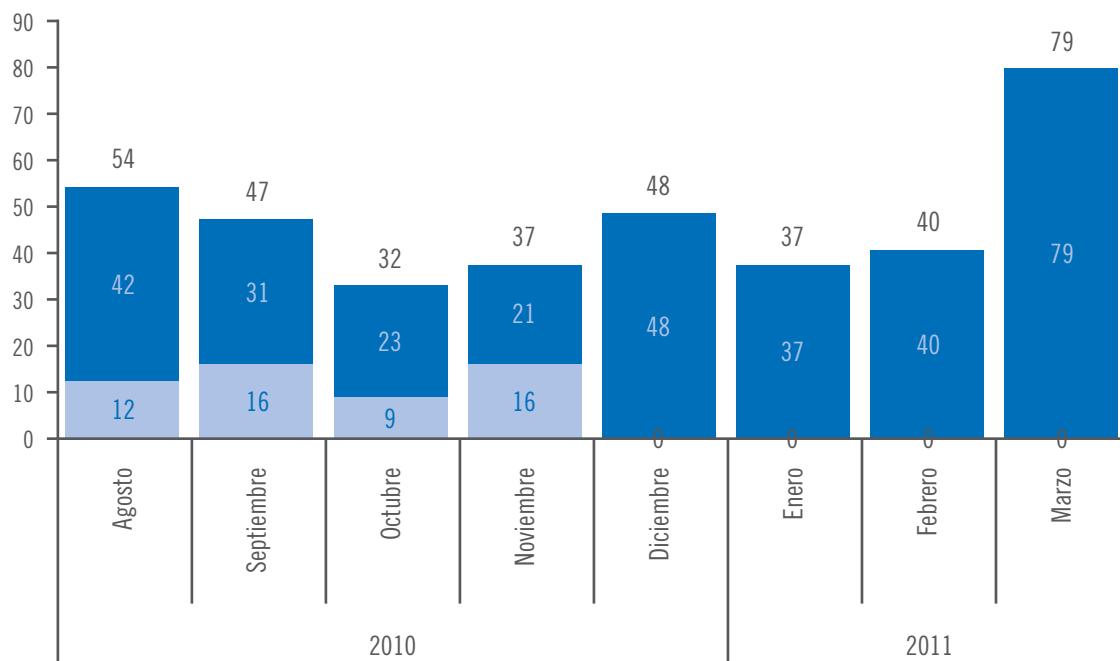
Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
 ■ Con aplicación de Ley de Protección de datos personales

DECISIONES INADMISIBLES Y OTROS

GRÁFICO 5

Distribución de Número total mensual de decisiones inadmisibles y otras despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

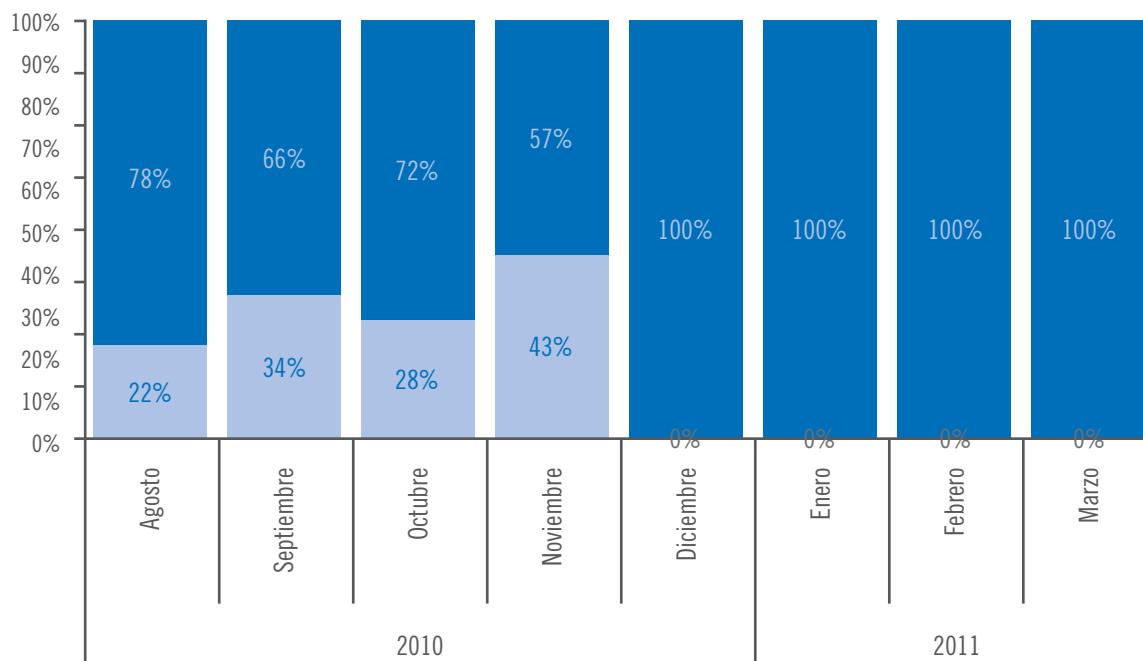


Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
 ■ Con aplicación de Ley de Protección de datos personales

GRÁFICO 6

Distribución de porcentaje mensual del total de decisiones inadmisibles y otras, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



Fuente: Unidad de Reportes y Estadísticas - CPLT

■ Sin aplicación de Ley de Protección de datos personales
■ Con aplicación de Ley de Protección de datos personales

IV. Recomendaciones

IV. Recomendaciones

RECOMENDACIONES DEL CONSEJO PARA LA TRANSPARENCIA SOBRE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO⁸

Certifico que el Consejo Directivo del Consejo para la Transparencia, en adelante, el Consejo, en su sesión N° 278, de 31 de agosto de 2011, en ejercicio de la atribución que le confiere el artículo 33 m) de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N° 20.285, de 2008, en adelante, Ley de Transparencia, consistente en velar por el debido cumplimiento de la Ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado, adoptó el siguiente acuerdo:

“I.- Recomendaciones sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado

CONSIDERANDO

1. Que la protección de datos personales,

amparada en nuestra legislación en la Ley N° 19.628, tiene por finalidad asegurar a las personas un espacio de control sobre su identidad y de libre manifestación de su personalidad, lo que presupone, en las condiciones modernas de elaboración y gestión de la información, la protección contra la recogida, el almacenamiento, la utilización y la transmisión ilimitados de los datos concernientes a su persona, es decir, el derecho a la autodeterminación informativa.

2. Que en el último tiempo han quedado en evidencia casos de accesos ilegales a registros administrados por órganos del Estado respecto de datos personales y sensibles de los ciudadanos, desconociéndose la protección que otorga la ley antes señalada. Por lo anteriormente expuesto, el Consejo para la Transparencia estima necesario contribuir a elevar los estándares de protección de los datos personales en poder de los órganos de la Administración del Estado a fin de asegurar los derechos que la ley reconoce a los titulares de los mismos.

3. Que, en esta materia, la letra m) del

artículo 33 de la Ley de Transparencia, faculta al Consejo para velar por el debido cumplimiento de la Ley N° 19.628, sobre protección de datos de carácter personal, por parte de los órganos de la Administración del Estado, y en la letra j), para velar por la debida reserva de los datos e informaciones que conforme a la Constitución y la ley tengan el carácter de secreto y reservado. Ambas disposiciones exigen, en consecuencia, una atenta observancia de la aplicación que los órganos públicos realicen de las disposiciones de la Ley N° 19.628, ya sea mediante la resolución de casos particulares o la dictación de recomendaciones.

4. Que desde la entrada en vigencia de la Ley de Transparencia, este Consejo, conociendo de reclamos por incumplimiento de los deberes de transparencia activa y de amparos por denegación de acceso a la información, se ha visto en la necesidad de ponderar este derecho fundamental con la protección de datos personales, lo que ha generado una abundante jurisprudencia al respecto.

5. Que, en virtud de la experiencia acumu-

⁸ Publicadas en el Diario Oficial de 14 de septiembre de 2011.

lada y en ejercicio de lo dispuesto en los literales m) y j) del artículo 33 de la Ley de Transparencia, se ha estimado conveniente proponer una serie de buenas prácticas complementarias de las normas obligatorias contenidas en la Ley N° 19.628, las que, en su carácter de recomendaciones, tendrán por objeto facilitar la comprensión y orientar para un mejor cumplimiento de las obligaciones que esta norma legal impone a los órganos de la Administración del Estado en materia de protección de datos personales. De esta forma, el presente instrumento normativo recogerá en su texto las obligaciones que dispone la ley y las complementará con orientaciones que faciliten su cumplimiento homogéneo por parte de la Administración.

POR TANTO, el Consejo Directivo acuerda dictar las siguientes Recomendaciones:

1. OBJETO DE LAS RECOMENDACIONES

Las presentes Recomendaciones tienen por objeto establecer orientaciones respecto de los criterios jurídicos aplicables por los órganos de la Administración del Estado en el tratamiento de datos de carácter personal que obren en su poder, a fin de dar cumplimiento a las obligaciones y limitaciones dispuestas por la Ley N° 19.628, garantizar a las personas el derecho a la protección de los datos de carácter

personal y asegurar el debido manejo de los registros o bancos de datos personales que sean necesarios para el ejercicio de sus competencias.

2. ÁMBITO DE APLICACIÓN DE LAS RECOMENDACIONES

Las Recomendaciones serán aplicables al tratamiento de datos de carácter personal que efectúen los órganos de la Administración del Estado, entendiendo por tales los comprendidos en el inciso primero del artículo 2° de la Ley de Transparencia.

Las presentes Recomendaciones no serán aplicables a los tratamientos de datos de personas jurídicas, ni al tratamiento de datos de personas fallecidas.

3. DEFINICIONES PREVIAS

Para efectos de la aplicación de estas Recomendaciones deberán considerarse las definiciones contenidas en el artículo 2° de la Ley N° 19.628, de 1999, sobre Protección de la Vida Privada, y, especialmente, se entenderá por:

3.1. Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica

o de cualquier otro tipo.

Por tanto, los elementos básicos de la definición son:

i. Debe tratarse de información relativa a una persona, siendo indiferente la naturaleza del dato, antecedente o hecho de que se trate.

ii. Debe tratarse de información que permita identificar al titular. Se entiende para estos efectos por identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (por ejemplo: RUT o RUN, número de cuenta corriente bancaria, domicilio, número telefónico, etc.). No se considerará identificable si es necesario realizar actividades desproporcionadas o en plazos excesivos. En este último caso el elemento determinante será el tipo de esfuerzo que se realiza para lograr la identificación de una persona.

iii. El titular sólo puede ser una persona natural. Quedan comprendidos dentro de esta definición, independiente del soporte en que se encuentren, datos tales como: nombre, edad, sexo, rol único tributario o

rol único nacional, estado civil, profesión, domicilio, números telefónicos, dirección postal, etc.

3.2. Datos sensibles, 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. Estos datos deberán ser especialmente protegidos adoptando las medidas de seguridad que corresponda.

3.3. Registro o banco de datos, 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. Por ejemplo, se pueden mencionar: los registros de personal de una institución, los de datos de clientes, los de datos de beneficiarios de subsidios, los de proveedores, un documento o tabla excel en el que se incluya distintos nombres y direcciones de participantes de un evento, un conjunto de currículos en formato digital insertos en una carpeta catalogados por

nombre, etc.

Por tanto, los registros de datos podrán clasificarse en:

i. Registro automatizado: todo conjunto organizado de datos de carácter personal que para su tratamiento han sido o están sujetos al uso de la informática y que, por ende, requieren de una herramienta tecnológica específica, como por ejemplo un procesador de texto o de cálculo, para su acceso, recuperación o tratamiento.

ii. Registro no automatizado: todo conjunto de datos de carácter personal organizado de forma manual, contenido en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, y estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales. Será en este caso fundamental para su clasificación atender al criterio de estructuración a través del cual se puede acceder al dato, como podría ser el nombre, RUT o RUN, la fecha de nacimiento, etc.

3.4. Responsable del registro o banco de datos, el organismo público, de los definidos en el numeral 2 de estas Recomendaciones, a quien compete las

decisiones relacionadas con el tratamiento de los datos de carácter personal. Por tanto, lo que caracteriza al responsable es su capacidad de decisión respecto de la finalidad, contenido y uso del tratamiento de los datos.

3.5. 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. Estas operaciones pueden ser realizadas directamente por el responsable del registro o, también, por el encargado del tratamiento.

A modo ejemplar se entienden incorporadas dentro del concepto de tratamiento las siguientes acciones:

i. Almacenar, que consiste en la conservación o custodia de datos en un registro o banco de datos;

ii. Disociar, referido a todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Por

ejemplo, mediante la tacha de ciertos datos que permitan la anonimización de la información, como los nombres, RUT o RUN de los currículos, mediante la supresión de los datos de las personas encuestadas y la entrega sólo de las respuestas otorgadas, etc.;

iii. Comunicar, transmitir o ceder, es decir, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas. Sin perjuicio de ello, el acceso a los datos por un encargado del tratamiento no se considerará cesión;

iv. Bloquear, que consiste la suspensión temporal de cualquier operación de tratamiento de los datos almacenados;

v. Modificar, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

vi. Eliminar o cancelar, esto es, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello, lo que conlleva el cese del tratamiento en forma definitiva.

3.6. Mandatario (también denominado encargado del tratamiento),

aquella persona natural o jurídica que realiza un tratamiento de datos por encargo o mandato del responsable de la base de datos, al que le serán aplicables las reglas generales en la materia. El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos, y el mandatario estará obligado a respetar esas estipulaciones en el cumplimiento de su encargo.

3.7. Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes. Es decir, su consulta debe poder ser realizada por cualquier persona, como por ejemplo, los contenidos en diarios o en medios de comunicación social.

3.8. Dato caduco, el que 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.

3.9. Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

Por ejemplo, tendrán este carácter las respuestas dadas en las encuestas, en la medida que a su respecto se hayan suprimido los datos de las personas encuestadas y no exista posibilidad de definir su identidad.

4. PRINCIPIOS ORIENTADORES DE LA PROTECCIÓN DE DATOS

Los principios orientadores de la protección de datos que informan su tratamiento por parte de los organismos de la Administración del Estado son los siguientes: licitud, calidad, información, seguridad y confidencialidad.

4.1. Principio de licitud. De conformidad con el artículo 4° de la Ley N° 19.628, sólo es posible tratar datos de carácter personal cuando exista autorización legal, ya sea de la propia Ley N° 19.628 o de otras normas de igual rango.

De acuerdo a la referida Ley, cuando los órganos de la Administración del Estado efectúen tratamientos de datos personales no será necesario el consentimiento del titular de los datos, respecto de las materias de su competencia y con sujeción a las reglas que la ley establece. Sin perjuicio de lo anterior, se considerará una buena práctica informar a la persona el propósito del almacenamiento y su posible comuni-

cación al público.

Por el contrario, en las materias fuera de la competencia de dichos órganos, éstos no podrán efectuar tratamientos ni siquiera recabando el consentimiento del titular.

4.2. Principio de calidad de los datos.

Este principio consiste en que los datos tratados deben ser exactos, adecuados, pertinentes y no excesivos, y deberá ser observado durante la recogida y posterior tratamiento de los datos. Concurren, por tanto, tres principios rectores:

a. Principio de veracidad. De conformidad con el inciso segundo del artículo 9° de la Ley N° 19.628, los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular. Por consiguiente, el organismo o servicio público responsable de la base de datos deberá, sin necesidad de requerimiento del titular de los mismos: eliminar los datos caducos y aquellos que estén fuera de su competencia; bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuáles no corresponda su cancelación; y modificar los datos inexactos, equívocos o incompletos. Lo anterior es sin perjuicio de lo establecido en el punto 5.10. de las

presentes Recomendaciones.

b. Principio de finalidad. Según lo dispone el inciso primero del artículo 9° de la Ley N° 19.628, los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. La referida finalidad en el caso de órganos de la Administración del Estado estará determinada en función de las materias propias de su competencia. Por ejemplo, un órgano que tenga competencia para otorgar subsidios podrá tratar los datos personales de los postulantes y de los beneficiarios que digan relación con los requisitos necesarios para la obtención de dicho beneficio con ese único objetivo.

c. Principio de proporcionalidad. Este principio implica que sólo pueden recabarse aquellos datos que sean necesarios para conseguir los fines que justifican su recolección. Por tanto, se entenderá que se cumple con el principio de proporcionalidad cuando: el o los datos que se recolecten, así como su posterior tratamiento, sean adecuados o apropiados a la finalidad que lo motiva; sean pertinentes o conducentes para conseguir la referida finalidad y no excesivos en relación a dicha finalidad para la cual se han obtenido, en el sentido que no exista otra medida más moderada para la consecución de tal propósito con

igual eficacia. Por ejemplo, para cumplir con este principio en el otorgamiento de una beca para estudios sólo se podrán recolectar datos relativos a la identificación del solicitante, sus antecedentes curriculares y demás necesarios para verificar la concurrencia de los requisitos establecidos para postular, en la medida que éstos se encuentren relacionados con la naturaleza del beneficio. En aplicación de este principio, los órganos o servicios públicos deberán optar, de entre los diversos tratamientos que le permitan conseguir los fines pretendidos dentro del ámbito de sus competencias, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos.

4.3. Principio de información.

De acuerdo a lo dispuesto en los artículos 3°, 4° y 20 de la Ley N° 19.628, y aunque los organismos públicos estén facultados para efectuar tratamientos de datos de carácter personal sin consentimiento del titular de los mismos respecto de materias de su competencia, se recomienda que éstos, previamente a la recolección de los datos, informen a su titular acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con el tratamiento de la información, de la posible comunicación a terceros y de

los derechos que pueden ser ejercidos por ellos.

4.4. Principio de seguridad. Conforme a lo establecido en el artículo 11 de la Ley N° 19.628, 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. Por tanto, se recomienda a los órganos de la Administración del Estado que, a fin de dar cumplimiento a lo anterior, apliquen medidas de seguridad, técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

4.5. Principio de confidencialidad o secreto. Según lo prescribe el artículo 7° de la Ley N° 19.628, las personas que trabajan en el tratamiento de datos personales o tengan acceso a éstos de otra forma (como aquellos funcionarios públicos autorizados para el acceso a bancos de datos de los organismos respectivos), 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 el banco de datos, obligación que no cesa por haber terminado sus actividades en

ese campo.

5. DERECHOS DE LOS TITULARES DE DATOS PERSONALES.

Los titulares de datos personales, conforme a lo establecido en el artículo 12 de la Ley N° 19.628, pueden ejercer respecto de los órganos de la Administración del Estado, los derechos que se describen en este numeral, teniendo presente las características de independencia, gratuidad y sencillez y las recomendaciones que en cada caso se señalan a continuación.

5.1. Derecho a acceder a sus propios datos. Toda persona tiene derecho a exigir del órgano o servicio que sea responsable de un banco 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 este caso la información será entregada en forma absolutamente gratuita, no siendo posible ni siquiera cobrar los costos directos de reproducción de esa información.

Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular podrá requerir información a cualquiera de ellos.

Cuando en el ejercicio del derecho de acceso a la información pública establecido en la Ley de Transparencia, se soliciten antecedentes que, obrando en poder de la Administración, contengan datos personales de los que es titular el solicitante, se aplicará el procedimiento establecido en dicha Ley, incluyendo la posibilidad de recurrir de amparo ante este Consejo. No obstante ello, en lo relativo a la gratuidad del acceso, se observará lo dispuesto en la Ley N° 19.628.

5.2. Derecho de rectificación o modificación. Toda persona tiene derecho a exigir que los datos que sean erróneos, inexactos, equívocos o incompletos, se modifiquen, siempre que se acredite debidamente cualquiera de dichas circunstancias y se indique con claridad la corrección solicitada. Lo anterior, es sin perjuicio de la rectificación o modificación de oficio por parte del órgano o servicio público, en aplicación directa del principio de calidad de los datos.

5.3. Derecho de cancelación o eliminación. Toda persona tiene derecho a exigir que se eliminen aquellos datos cuyo almacenamiento carece de fundamento legal o se encuentran caducos, salvo que concurra alguna excepción legal, como las señaladas en el numeral 5.10. de las

presentes Recomendaciones.

En el caso de los numerales 5.2. y 5.3., la rectificación y cancelación serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular copia del registro alterado en la parte pertinente. No estarán autorizados a cobrar los órganos o servicios públicos los costos directos de reproducción por la entrega de dicha información. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que hayan transcurrido, a lo menos, seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente por el titular del dato o debidamente representado.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el órgano responsable del banco deberá avisarles a la brevedad posible la operación efectuada. Si no fuere posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos. De todo ello, se recomienda informar, oportunamente y por escrito, al

titular del dato.

5.4. Derecho al bloqueo de datos. Es el derecho a exigir la suspensión temporal de cualquier operación de tratamiento de los datos almacenados (letra b) del artículo 2° de la Ley N° 19.628). Procede cuando el titular ha proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones informativas y no desee continuar figurando en el registro respectivo de modo temporal o definitivo, o cuando la exactitud de los datos personales no pueda ser establecida o cuya vigencia sea dudosa y respecto a los cuales no corresponda la cancelación. Lo anterior, sin perjuicio de lo establecido en el numeral 5.10. de las presentes Recomendaciones.

5.5. Procedimiento y formulario para el ejercicio de los derechos.

Para facilitar el ejercicio de los derechos señalados en los numerales precedentes, los órganos o servicios públicos podrán disponer de procedimientos y formularios simplificados que faciliten el ejercicio de los derechos señalados en los numerales precedentes. Se recomienda que dichos formularios estén disponibles en cada una de las Oficinas de Información, como también en sus respectivas páginas web. En los referidos formularios se exigirá:

a) El nombre y apellidos del titular de los datos. Lo anterior se acreditará mediante fotocopia de la cédula de identidad o pasaporte. Además, regirá la misma exigencia en caso de actuar mediante apoderado a su respecto.

b) La dirección del solicitante a efectos de notificación.

c) El derecho que se ejerce y una descripción simple de los hechos en que se funda.

d) La fecha y la firma del solicitante, estampada por cualquier medio habilitado.

e) Los documentos acreditativos de la solicitud, en caso de ser procedente.

5.6. Ejercicio independiente. Cada uno de los derechos señalados en los numerales 5.1. a 5.4. podrá ser ejercido en forma independiente, es decir, no puede exigirse el ejercicio de ninguno de ellos como condición o requisito previo para el ejercicio del otro. A modo ejemplar, no podrá exigirse ejercer el derecho de acceso en forma previa ni concurrente al ejercicio del derecho de rectificación.

5.7. Ejercicio a través de apoderado. Los derechos señalados en los numerales 5.1. a 5.4. podrán ser ejercidos perso-

nalmente o mediante apoderado. En este último caso, el apoderado tendrá las mismas facultades que el titular del dato, salvo manifestación expresa en contrario.

El poder deberá constar en escritura pública o documento privado suscrito ante notario y el apoderado deberá acreditar al ejercer el derecho, mediante la correspondiente documentación, la identidad del titular del dato y la calidad de apoderado.

5.8. Ejercicio de los derechos ante el mandatario (también denominado encargado del tratamiento). En caso de que el organismo de la Administración del Estado hubiese encargado el tratamiento de los datos a un tercero, los titulares de éstos podrán ejercer sus derechos directamente ante él o ante el órgano o servicio, a su elección. En el contrato respectivo deberá establecerse la forma en que se dará respuesta en estos casos, buscando en todo momento responder en forma oportuna y adecuada al titular del dato.

5.9. Prohibición de limitación. Los derechos señalados en los numerales 5.1. a 5.4. no podrán ser limitados por medio de ningún acto o convención.

5.10. Límites al ejercicio de los derechos. No obstante lo dispuesto en los

numerales precedentes, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando:

i. Ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo de la Administración del Estado requerido,

ii. Afecte la reserva o secreto establecidos en disposiciones legales, las que, de acuerdo al artículo 8º de la Constitución Política de la República, deberán tener rango de ley de quórum calificado. En especial, cuando se configure algunas de las causales establecidas en el artículo 21 de la Ley de Transparencia,

iii. Afecte la seguridad de la nación,

iv. Afecte el interés nacional o

v. Hubiesen sido almacenados por mandato legal. En este caso el mandato legal deberá ser expreso y autorizar al órgano o servicio para hacer tratamiento de datos respecto de un determinado banco de datos, como por ejemplo, los registros de datos de nacimiento que tiene en su poder el Servicio de Registro Civil e Identificación. La procedencia de la modificación, cancelación o bloqueo de los datos en esos casos estará sometida y tendrá el alcance que

establezca la normativa respectiva.

5.11. Obligación de evacuar respuesta. El órgano o servicio público estará obligado a evacuar respuesta a la solicitud efectuada por el titular de los datos, en el plazo señalado en el numeral 5.12., aunque no disponga de los datos de carácter personal de la persona que ejerció el derecho.

5.12. Plazo de respuesta y efectos de la falta de pronunciamiento en tiempo o de la denegación. Si el órgano o servicio responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, solicitando amparo a los derechos consagrados en este numeral, de acuerdo al procedimiento establecido en el inciso segundo del artículo 16 de la Ley N° 19.628.

En caso que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará

informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. El procedimiento ante la Corte Suprema se someterá a las normas establecidas en los incisos tercero y siguientes del artículo 16 de la Ley N° 19.628.

6. OBLIGACIONES ESPECÍFICAS DE LOS ORGANISMOS DE LA ADMINISTRACIÓN DEL ESTADO

6.1. Condiciones de licitud en el tratamiento de los datos. Los organismos de la Administración del Estado pueden realizar tratamiento de datos personales, sólo y exclusivamente respecto de las materias de su competencia y con sujeción a las reglas que la ley establece, no requiriendo para estos efectos el consentimiento del titular. Asimismo, deberán tener en consideración las presentes Recomendaciones que velan por el adecuado cumplimiento de la Ley N° 19.628.

Los órganos públicos no podrán efectuar tratamientos de datos personales en materias ajenas a su competencia, ni siquiera recabando el consentimiento del titular.

6.2. Requerimientos para el tratamiento de datos. Los órganos o servicios públicos deben sujetarse para el tratamiento de los datos, según el artículo 20, a las reglas establecidas en la Ley N° 19.628, con la sola excepción de la exigencia relativa al consentimiento del titular. En consecuencia:

a) Se recomienda a los órganos de la Administración del Estado que informen al titular de los datos, según lo dispone el artículo 4° de la Ley N° 19.628, el propósito del almacenamiento de sus datos personales, es decir, la finalidad perseguida con el tratamiento de la información, y la posible comunicación a terceros. De la misma forma, se podrá informar al titular la denominación del órgano o servicio responsable del tratamiento de la base de datos y los derechos que le asisten para la protección de sus datos personales.

Se recomienda especialmente a los órganos o servicios públicos que dispongan de una política proactiva de difusión de información en esta materia a fin de dar cabal cumplimiento al deber de informar antes señalado. Por ejemplo, podrán contemplar estos antecedentes en la Política de Privacidad poniéndola a disposición permanente del público en los respectivos sitios web institucio-

nales, mediante afiches o la mención a tal política en los formularios en que se soliciten datos personales (formulario de registro), señalando dónde se encuentra ésta, entre otras.

b) Los órganos o servicios públicos deberán necesariamente, de conformidad al artículo 9° de la Ley N° 19.628, efectuar el tratamiento de los datos personales cumpliendo con las finalidades correspondientes a las materias de su competencia. Se recomienda que estas finalidades se encuentren explicitadas, a modo ejemplar, en la política de privacidad, formulario de registro, formulario papel u otro medio, para de esta manera informar adecuadamente a su titular.

c) En virtud del principio de calidad de los datos y de los artículos 6° y 9°, inciso segundo, de la Ley N° 19.628, los órganos o servicios públicos deberán de oficio y sin necesidad de requerimiento del titular de los datos: eliminar los datos caducos y aquéllos que se encuentren fuera de su competencia por carecer de fundamento legal; bloquear los datos cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; y modificar los datos inexactos, equívocos o incompletos.

d) Se recomienda asimismo que, en virtud del principio de seguridad y del artículo 11 de la Ley N° 19.628, los órganos o servicios públicos, desde el momento de la recolección, adopten todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar su alteración, pérdida, transmisión y acceso no autorizado, haciéndose responsable de los daños causados. En este sentido, los organismos públicos deberán aplicar diversos niveles de seguridad atendiendo al tipo de dato almacenado. A título ejemplar, respecto de aquellos datos definidos como sensibles, deberán adoptarse niveles de seguridad más altos que respecto de aquellos que no posean dicha calidad.

e) Los órganos o servicios públicos deberán exigir a sus funcionarios cumplir con la obligación de secreto o confidencialidad en relación a los datos que provengan o hayan sido recolectados de fuentes no accesibles al público, contemplada en el artículo 7° de la Ley N° 19.628, en especial respecto de los que trabajen en el tratamiento de datos personales o tengan acceso a éstos de cualquier otra forma, extendiéndose, igualmente, este deber a los demás datos o antecedentes relacionados con el banco de datos, como por ejemplo respecto de

las medidas de seguridad adoptadas a su respecto. Asimismo, la referida obligación del funcionario público no cesará por haber terminado sus obligaciones en ese campo, es decir, por dejar de desempeñarse en el tratamiento o acceso a dichos registros o en el Servicio mismo.

6.3. Tratamiento de datos personales relativos a delitos, infracciones administrativas o faltas disciplinarias.

Los órganos de la Administración del Estado, conforme a lo dispuesto en el artículo 21 de la Ley N° 19.628, que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Por consiguiente, los órganos deberán abstenerse de publicar en virtud del artículo 7°, letra g) de la Ley de Transparencia, referido a los actos y resoluciones que tengan efectos sobre terceros, los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena y aplicarán, de ser procedente, el principio de divisibilidad respecto de los actos o resoluciones que

los contengan.

Con todo, cuando el Consejo conozca de un reclamo por incumplimiento de los deberes de transparencia activa o de un amparo por denegación de acceso a la información, podrá autorizar la comunicación de este tipo de datos cuando así lo exija el interés público, en aplicación de la Ley de Transparencia.

Se exceptuarán de la prohibición de comunicación, 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 serán aplicables los siguientes artículos de la Ley N° 19.628:

- a) El artículo 5° que regula el procedimiento automatizado de transmisión de datos,
- b) El artículo 7° que consagra el principio de secreto exigible a los funcionarios públicos,
- c) El artículo 11 que establece el principio de seguridad y
- d) El artículo 18 referido a la prohibición de comunicación de datos personales relativos

a obligaciones de carácter económico, financiero bancario o comercial cuando han transcurrido cinco años desde que la obligación se hizo exigible, después de haber sido pagada o haberse extinguido la obligación por otro modo legal, sin perjuicio de la comunicación a los Tribunales de Justicia de la información que requieran con motivo de juicios pendientes.

6.4. Inscripción de las bases de datos en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos. Los órganos de la Administración del Estado deberán inscribir todos los bancos de datos personales que obren en su poder en el Registro de los Bancos de Datos Personales a cargo de Organismos Públicos que lleva el Servicio de Registro Civil e Identificación, de acuerdo a lo establecido en el artículo 22 de la Ley N° 19.628, en el Decreto Supremo N° 779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos y en la Resolución (E) N° 1540, de 2010, del Servicio de Registro Civil e Identificación.

a) Características del registro. 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.

b) Requisitos de la inscripción. Conforme a la normativa aludida, el organismo público responsable del banco de datos para efectos de la inscripción, debe proporcionar, a lo menos:

i. El nombre del banco de datos personales, es decir, la denominación que el propio organismo le dé al banco de datos que inscriba y que sirva para su identificación;

ii. El organismo público responsable del banco de datos personales respectivo;

iii. El RUT correspondiente al organismo público;

iv. El fundamento jurídico de la existencia del banco de datos personales, es decir, se deben indicar las normas legales que sancionan en forma específica la existencia de un registro en particular, o las normas de carácter general, sectorial u orgánica que habiliten al organismo público para tratar los datos personales y almacenarlos en bancos de datos;

v. La finalidad del banco de datos;

vi. El o los tipos de datos almacenados en dicho banco, pudiendo corresponder, a modo ejemplar, a cualquiera de las siguientes categorías de datos: biométricos (como ADN, firma, fotografía, impresiones dactilares, etc), civiles (como datos de los padres, domicilio, fecha de nacimiento, lugar de nacimiento, nombres, apellidos, datos del cónyuge, estado civil, fecha de matrimonio, sexo, fecha de defunción, lugar de defunción, nacionalidad, RUN, etc), económicos y financieros (como cuentas bancarias, ingresos, tarjetas de crédito, deudas, RUT, etc), generales (calidad de conductor de vehículos motorizados, habilidades, membresía a organizaciones, etc), judiciales o legales (como condenas, infracciones de tránsito, consumo y tráfico de estupefacientes, violencia intrafamiliar, etc.), de salud (como enfermedades, discapacidad, intervenciones, alergias, etc.), sociales (nivel educacional, religión, profesión, ocupación u oficio, etnia, etc.) y otros datos referidos a cualquier otra información concerniente a personas naturales, identificadas o identificables, almacenada en la base de datos del organismo respectivo; y

vii. Una descripción del universo de personas que comprende.

c) Procedimiento de inscripción. El proce-

dimiento de inscripción de los bancos de datos personales a cargo de los órganos de la Administración del Estado se encuentra regulado en el Decreto Supremo N° 779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos y en las resoluciones que el Director Nacional estime pertinente dictar al efecto, en especial, la Resolución (E) N°1540, de 2010, que establece el procedimiento de inscripción de registros y/o bancos de datos personales a cargo de los organismos públicos o la que la reemplace.

d) Oportunidad de la inscripción. Los órganos o servicios públicos deberán inscribir la base de datos dentro del plazo de 15 días contados desde que se inicien las actividades del respectivo banco.

e) Correcciones de la inscripción. Cualquier corrección relativa a errores u omisiones de una inscripción deberá ser requerida por el propio organismo responsable de dicha inscripción en el Registro de Bancos de Datos Personales, siguiendo el mismo procedimiento establecido para la inscripción.

f) Modificaciones de la inscripción. Cualquier modificación de una inscripción

deberá ser requerida por el propio organismo responsable de la inscripción en el Registro de Bancos de Datos Personales, en el plazo de 15 días contados desde que se produzca cualquier cambio en la información proporcionada, de acuerdo a lo establecido en la letra b) del presente numeral.

6.5. Comunicación o transmisión de datos personales. Los organismos de la Administración del Estado sólo podrán establecer procedimientos de comunicación, transmisión o cesión de datos de carácter personal para fines que digan directa relación con sus competencias legales y las de los organismos participantes, aplicando los principios orientadores establecidos en el punto 4 de estas recomendaciones. Por su parte, el receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión, salvo que se trate de datos personales accesibles al público en general o se trasmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en tratados y convenios vigentes. Dicho procedimiento podrá contemplar las siguientes etapas: requerimiento expreso, admisibilidad del mismo y firma de un convenio de transmisión, las que se someterán a los lineamientos que se señalan a continuación.

El requerimiento de datos personales efectuado a un órgano o servicio público contendrá las siguientes especificaciones:

- a) La individualización del requirente, el que puede ser un organismo público o privado;
- b) El motivo y el propósito del requerimiento, con indicación expresa del tratamiento de datos que se busque efectuar y la finalidad del mismo, y
- c) El tipo de datos que se desea transmitir.

La admisibilidad del requerimiento será evaluada por el órgano o servicio responsable del banco de datos que lo recibe, verificando que la comunicación guarde relación con sus tareas o finalidades, es decir, que se encuentra dentro del ámbito de sus competencias, y estableciendo los requisitos necesarios para el resguardo de los derechos de protección de datos en el convenio respectivo. En esta etapa, los órganos públicos garantizarán la igualdad de trato en el acceso a esta información por parte de todas las entidades que efectúen el requerimiento correspondiente, y cumplan con los requisitos establecidos.

De la transmisión, la fecha, el motivo y propósito de la misma, los requisitos específicos para la protección de los datos personales transmitidos y la obligación del solicitante de utilizar los datos personales sólo para los fines que motivaron la transmisión se dejará constancia en un convenio de comunicación o transmisión suscrito por ambas partes, el que se entenderá aprobado una vez que se encuentre totalmente tramitado el o los correspondientes actos administrativos de aprobación, según se trate de uno o más órganos públicos. Por tanto, a lo menos deberá contener:

i. Identificación del órgano público que transmite los datos y del destinatario de los mismos,

ii. Identificación del banco de datos, según la denominación dada en la inscripción efectuada en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos,

iii. Las medidas de seguridad que deberán adoptar tanto el que transmite los datos como el destinatario de los mismos durante todo el procedimiento de transmisión y posterior tratamiento de los datos por éste último,

iv. La indicación de que el receptor de los datos tendrá la calidad de responsable del tratamiento, estando sometido a las mismas obligaciones, multas y responsabilidad de indemnizar en caso de tratamiento indebido de los datos, que el órgano público que efectuó la transmisión,

v. El procedimiento para efectuar el aviso a que se refiere el artículo 12, inciso final, de la Ley N° 19.628, en caso que se ejerza ante cualquiera de los responsables de la base de datos comunicada los derechos de modificación, cancelación o bloqueo, adoptando las medidas de trazabilidad que correspondan,

vi. El plazo que el destinatario conservará los datos transmitidos, y

vii. Los cursos de acción que deberá seguir el destinatario una vez que haya efectuado el tratamiento que motivó la transmisión, ya sea que se acuerde la destrucción o devolución del banco de datos al transmisor y de cualquier otro soporte donde consten los datos objetos de la comunicación.

Por ejemplo, si el organismo utiliza un servicio Web que permite la consulta directa entre los sistemas de información de las diversas entidades participantes o si dos

organismos públicos suscriben convenios de intercambio de datos personales deberán cumplir con lo dispuesto en el artículo 5° de la Ley N° 19.628 y observar las precedentes recomendaciones.

No serán aplicables las recomendaciones contenidas en este numeral a los convenios o contratos celebrados entre órganos o servicios públicos y particulares cuando este último tenga la calidad de encargado del tratamiento, esto es, actúa bajo las instrucciones del organismo responsable de la base de datos, quien tiene las facultades para decidir acerca de la base de datos misma. En ese caso, deberá estarse a las exigencias contempladas en el numeral 6.6. y siguientes.

6.6. Tratamiento de datos a través de un mandatario (también denominado encargado del tratamiento). Los órganos o servicios públicos, en conformidad a lo dispuesto en el artículo 8° de la Ley N° 19.628, podrán encargar el tratamiento de los datos a un tercero, que tendrá la calidad de mandatario.

El contrato de prestación de servicios de tratamiento que encargue el tratamiento de datos personales deberá ser otorgado por escrito y se recomienda hacer mención de:

a) Que el tratamiento se efectúa a cuenta y riesgo del organismo responsable del tratamiento,

b) Las condiciones de utilización de los datos,

c) Las medidas de seguridad que se deban adoptar y,

d) Las exigencias de confidencialidad de las personas que trabajen en el tratamiento y, en general, de la necesidad de dar cumplimiento a las obligaciones establecidas en la Ley N° 19.628 y de observar las presentes recomendaciones.

En estos casos no se entenderá que existe transmisión, comunicación o cesión de datos entre el responsable del tratamiento y el mandatario (o encargado).

6.7. Medidas de Seguridad de los bancos o registros de datos. En virtud del principio de seguridad y del artículo 11 de la Ley N° 19.628, se recomienda a los organismos de la Administración del Estado adoptar todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso

no autorizado de los mismos.

Para ello, los organismos públicos aplicarán diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de los datos sensibles deberán adoptarse niveles de seguridad más altos que en relación a aquellos que no poseen dicha calidad.

Los organismos públicos deberán adoptar todas las medidas de seguridad de sistemas para el resguardo de los bancos de datos personales que sean pertinentes a la naturaleza de los datos tratados, por lo que se recomienda, especialmente, adoptar las medidas de seguridad establecidas en el artículo 11 y siguientes del Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprobó la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, en lo relativo a establecer una política que fije las directrices generales orientadoras en materia de seguridad de bases de datos que se encuentran en su poder, que defina un encargado de seguridad al interior del servicio, mediante el correspondiente acto administrativo, y que a cada banco de datos se le asigne un responsable.

6.8. Obligaciones en caso tratamiento de datos para encuestas, estudios de mercado y sondeos de opinión.

De acuerdo a lo establecido en el artículo 3° de la Ley N° 19.628, cuando los órganos o servicios públicos recolecten datos personales a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que la ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas, debiendo sólo comunicarse los datos que tengan la calidad de estadísticos, es decir, los que en su origen, o como consecuencia de un tratamiento, no pueden ser asociados a un titular identificado o identificable, por haber sido aplicado a su respecto un procedimiento de disociación de datos.

Asimismo, el titular del dato puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Para ello se recomienda que el órgano o servicio informe al titular del dato, conjuntamente con los aspectos señalados y al momento

de realizarse la recopilación, que le asiste el derecho a oponerse, en cualquier tiempo, a la utilización de los mismos con los fines indicados.

6.9. Responsabilidad por las infracciones y derecho a indemnización. De conformidad al artículo 23 de la Ley N° 19.628, el órgano de la Administración del Estado 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 su caso, lo ordenado por el tribunal.

7. ENCARGADO O ENCARGADA DE PROTECCIÓN DE DATOS

Para facilitar el cumplimiento de las obligaciones establecidas en la Ley N° 19.628 y una mejor observancia de las presentes Recomendaciones, se sugiere que las distintas autoridades, jefaturas o jefes superiores de los órganos o servicios

de la Administración del Estado, designen a un funcionario o funcionaria de dicha repartición para desempeñarse como encargado o encargada de protección de datos y constituya un contacto efectivo en la materia con el Consejo para la Transparencia.

La designación y las comunicaciones que se establezcan para los efectos antedichos no alterarán, en caso alguno, la responsabilidad prevista en el artículo 23 de la Ley señalada anteriormente.

II.- Publicación. Publíquese el presente acuerdo en el Diario Oficial.”

Santiago, 5 de septiembre de 2011.

ENRIQUE RAJEVIC MOSLER
Director General (S)
Consejo para la Transparencia

PROTECCIÓN DE DATOS PERSONALES
UNIDAD NORMATIVA, DIRECCIÓN JURÍDICA CPLT / ABRIL 2011