ESTRATEGIAS EMERGENTES PARA EL DESARROLLO DE LA PROTECCIÓN DE DATOS EN CHILE

I. ESTADO ACTUAL DE LA PROTECCIÓN DE DATOS EN CHILE.

Nuestro país cuenta, desde el año 1999, con la Ley N° 19.628, de Protección de la Vida Privada, que regula expresamente el tratamiento de los datos personales. No obstante constituir un indudable avance en su oportunidad, al contener una regulación mínima en la materia, con el transcurso de los años y el desarrollo de la protección de datos a nivel mundial, se han revelado una serie de fallas e imperfecciones en una legislación que, en definitiva, parece insuficiente para la efectiva protección de los datos y la intimidad de las personas.

La frecuente comunicación o transmisión de los datos contenidos en un número significativo y creciente de bases de datos personales, ha puesto de manifiesto las carencias legislativas y de control. En múltiples ocasiones la prensa chilena ha dado cuenta de ello, destacando, por ejemplo, la filtración en Internet de los datos de 6 millones de chilenos, ocurrido en el año 2008; la publicación de datos de menores en la Red; y la transferencia de información relativa a estados de salud de las personas entre ISAPRES (seguros privados de salud insertos en la seguridad social chilena) y farmacias durante el 2009, por mencionar sólo algunas.

Por otra parte, una adecuada protección de datos incide en las condiciones y perspectivas de desarrollo del promisorio "*Cluster*" de Servicios Globales en nuestro país. Un adecuado marco normativo eficazmente supervisado se revela como un factor clave de la competitividad de una industria que ha emergido con gran fuerza y potencial. Si bien las exportaciones de servicios globales ya se empinan a cifras que rozan los 1.000 millones de dólares, algunas empresas globales han expresado su preocupación por la insuficiente protección jurídica de las bases de datos personales. Por ello, esta materia requiere de urgente revisión desde la doble óptica del resguardo de un derecho personal como de la promoción de condiciones que favorezcan la competitividad y seguridad de una industria promisoria.

Atendido lo expuesto, es un deber prioritario fortalecer la protección de datos personales en nuestro país, definir las condiciones sobre las cuales terceros pueden hacer uso de los datos que conciernen a una persona y garantizar el derecho que a ésta asiste para controlar quién, cómo, dónde y con qué objeto se recogen y tratan sus datos. En definitiva, importa avanzar derechamente en lo que se conoce como derecho de autodeterminación informativa o, en general, derecho a la protección de datos.

Nuestro texto legal posee, al respecto, diversas carencias. Entre ellas destacan:

1. Inexistencia de un Registro Nacional de las bases de datos particulares existentes. Cabe hacer presente que, si bien la ley establece la obligación de los

órganos públicos a registrar sus bases de datos en el Servicio del Registro Civil, el incumplimiento de este deber carece de sanción en ella.

2. Inexistencia de un catálogo de infracciones a la ley y sus respectivas sanciones. Ya que actualmente sólo se dispone de un proceso indemnizatorio en que deben acreditarse los perjuicios.
3. Inexistencia de un órgano de control, de carácter público, encargado de la fiscalización, promoción y aplicación de la ley de protección de los datos, que posea, además, facultades para actuar respecto de organismos públicos como privados .
4. Opacidad en algunos conceptos que la ley contempla, tales como "fuentes de acceso público" y "encargado del tratamiento".

II. IMPORTANCIA DE LA REFORMA LEGISLATIVA: LOS SERVICIOS GLOBALES Y LOS FLUJOS TRANSFONTERIZOS DE DATOS.

Dentro del proceso de globalización económica, la industria de los Servicios Globales, o también conocida como *offshoring,* crece a tasas del 40% anual, alcanzando un volumen de mercado de US$ 40 billones adicionales por año entre el 2007-2010[1].

Chile, reconocido como una localización emergente con una gran oportunidad de desarrollar una estrategia de especialización internacional en servicios de alto valor, estableció y priorizó este sector productivo en la Política de Clústers impulsada por el Gobierno chileno.

Se trata de uno los *clusters* con mayor potencial de crecimiento de acuerdo con el Consejo Nacional de Innovación para la Competitividad[2] (organismo público-privado que actúa como asesor permanente del Presidente de la República), y genera un impacto cercano a los 10.000 empleos y US. 420 millones en flujos de capital.

Carlos Álvarez, Vicepresidente Ejecutivo de CORFO, (Agencia de Desarrollo Productivo chilena) ha destacado la importancia que tienen los servicios globales en el desarrollo económico del país: "Este año los servicios globales han exportado cerca de US$ 850 millones, y se espera que el próximo año superen los US$ 1.000 millones".

En este contexto, la Protección de Datos se vislumbra como un factor clave de competitividad para desplegar todo el potencial del *Clúster* de Servicios Globales en

[1] Presentación "Industria de Servicios Globales -Oportunidades para Chile-", del Consejo Estratégico del Clúster de Servicios Globales, CORFO. Abril de 2009.
[2] El objetivo de este organismo es asesorar a la autoridad en la identificación y formulación de políticas referidas a la innovación y la competitividad, incluyendo los campos de la ciencia, la formación de recursos humanos y el desarrollo, transferencia y difusión de tecnologías.

nuestro país, convirtiéndose en la credencial más importante para consolidar este tipo de desarrollo y crecimiento económicos**.**

III. HACIA EL CUMPLIMIENTO DE ESTÁNDARES INTERNACIONALES. EL "NIVEL DE PROTECCIÓN ADECUADO"

En materia de Protección de Datos, se han establecido internacionalmente determinados estándares: las Directrices para la regulación de los archivos de datos personales informatizados, aprobadas en el año 1990 por las Naciones Unidas; el Convenio 108 del Consejo de Europa; las Directrices de la OCDE, relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales; y la **Directiva Europea 46/95/CE**, que, sin duda, resulta una de las más relevantes por cuanto en ella se consagra que, frente a transmisiones internacionales de datos personales, el país receptor de dichos datos debe tener un "nivel de protección adecuado" en la materia.

Esta Directiva, además de garantizar el principio de la libre circulación de los datos entre los Estados miembros, nace con el objeto de garantizar el derecho a la intimidad en el tratamiento de los datos personales de las personas físicas.

Cumplir con el estándar europeo implica que una transferencia de datos personales fuera del ámbito comunitario sólo puede efectuarse cuando exista un **"nivel de protección adecuado"** en el país receptor.

Si bien se trata de un concepto ambiguo, el Grupo de Trabajo creado por el artículo 29 de la Directiva –G29-, mediante sus Documentos de Trabajo, ha permitido precisar el alcance de tal expresión, tarea favorecida por las Decisiones del Consejo de Europa al respecto.

La expresión "protección adecuada" se refiere, en primer término, a que **los terceros países deben garantizar el conjunto de principios básicos de protección de datos contenido en la Directiva Europea, y garantizar dichos principios de una manera efectiva**, por ello, no basta la sola legislación que plasme estos principios, sino que se establezcan los medios idóneos para ejercitar estos derechos, esto es:

1. Que exista un órgano de control responsable de la protección de datos no sólo autónomo sino independiente, con un campo de aplicación amplio, esto es, público y privado, con facultades de fiscalización y sancionadoras,
2. Un catálogo de infracciones y sanciones que sean disuasivas para los responsables de bancos de datos,
3. Acciones administrativas y/o judiciales,
4. Medidas de seguridad adecuadas,
5. Promoción de los derechos de los titulares de datos y de las obligaciones respecto de los bancos de datos,

6. Disponer de sistemas de responsabilidad y reparación para los afectados cuando no se de cumplimiento a las normas establecidas.

Al ser considerado actualmente Chile como un país con un nivel no adecuado de protección en materia de datos personales, ha debido someterse al mecanismo de las cláusulas tipo en los respectivos contratos que se suscriben con empresas españolas, con el fin de alcanzar las autorizaciones que correspondan por la Agencia Española de Protección de Datos cuando se pretenden realizar transferencias internacionales de los mismos (servicios globales). Es este el obligado camino que nuestro país deberá seguir mientras no se estatuya una legislación que le permita solicitar a la Comisión Europea la declaración de adecuación de la protección.

IV. LA NUEVA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS: EL DESAFÍO PENDIENTE.

Conforme a lo señalado, y con el propósito de cumplir los estándares internacionales en materia de Protección de Datos, nuestro país inició en el año 2008 un proceso de modificación a la legislación existente, que data de 1999: la Ley N° 19.628, de Protección de la Vida Privada. Proyecto de ley que también modifica la Ley N° 20.285, de Acceso a la Información Pública, que entró en vigencia en el mes de abril de 2009.

Dicho Proyecto ingresó al Congreso el **1° de octubre de 2008**, mediante Mensaje de S.E. la Presidenta de la República, Boletín N° 6120-07, introduciendo las modificaciones necesarias para dar cumplimiento al estándar internacional europeo.

Básicamente, nuestro proyecto contempla lo siguiente:

a) Se otorgan al **Consejo para la Transparencia** (órgano público autónomo encargado del acceso a la información pública) las facultades de protección de datos, respecto de organismos públicos y de carácter privado. El Consejo pasa a denominarse **"Consejo para la Transparencia y Protección de Datos Personales"**.

b) Se reconoce explícitamente el derecho de los titulares a controlar sus datos, y se fortalecen los derechos de información, de rectificación y cancelación de los datos.

c) Se establece un Sistema Único Nacional de Registro de los bancos de datos personales, a cargo del Consejo.

d) Se amplía el margen de sujetos protegidos a las personas jurídicas.

e) Se regula el flujo transfronterizo de datos.

f) Se aclaran conceptos claves como "fuente accesible al público" y "encargado del tratamiento" de los datos, en armonía con el estándar europeo en la materia.

g) Se regula detalladamente un catálogo de infracciones y sanciones, en el que se distinguen tres niveles: leve, grave y gravísima, con sanciones consistentes en multas o cancelación del registro.

h) Se regula un procedimiento sancionatorio, que puede iniciarse de oficio o por denuncia. Tal procedimiento garantiza la bilateralidad de la audiencia y el derecho a defensa del acusado o denunciado. El órgano ante el cual se sigue este procedimiento es el Consejo para la Transparencia (autoridad controladora), quien aplicará la sanción. En contra de la resolución que imponga la sanción, se podrá presentar reposición ante el mismo Consejo y en contra de la resolución que se pronuncie sobre esta última podrá recurrirse de ilegalidad ante la Corte de Apelaciones, en los mismos términos que se regular en el artículo 28 de la Ley de Acceso a la Información Pública.

Dentro de las **nuevas potestades** que se otorgan al Consejo para la Transparencia podemos mencionar las que se pasan a exponer:

1. Mantener un Registro Único Nacional de las Bases de Datos, y requerir la inscripción de los bancos de datos, que no estén registrados, en el Registro Único Nacional.

2. Fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estime pertinente.

3. Inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley.

4. Dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos.

5. Conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos, señalados en la ley N° 19.628 y en otras normas sobre protección de datos personales, sin perjuicio de las facultades de otras autoridades públicas.

6. Sancionar a los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos.

7. Requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro, cuando no se ajuste a sus disposiciones.

8. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y promover el respeto de los mismos.

9. Ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos.

10. Desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

11. Entregar una cuenta anual sobre la actividad desarrollada en torno a la protección de datos personales.

V. RECORRIDO DEL CONSEJO PARA LA TRANSPARENCIA EN MATERIA DE PROTECCIÓN DE DATOS

Desde la entrada en vigencia de la Ley de Transparencia, el Consejo ha debido enfrentar la labor de conciliar y ponderar dos bienes jurídicos; por un lado, el derecho de acceso a la información y, por el otro, la protección de los datos personales solicitados. Lo anterior, en razón que el propio texto legal de la Ley de Transparencia le encomienda el velar por el adecuado cumplimiento de la Ley N°19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado.

De esta forma y de acuerdo a la experiencia recopilada, existen, al menos, dos razones fundamentales por las cuales el acceso a la información y la protección de datos personales son derechos llamados a complementarse e interrelacionarse en forma constante:

- En primer lugar, porque ejercer los derechos que envuelven la protección de datos personales supone normalmente ejercer el derecho de acceso a la información en contra de quien lleva la base de datos respectiva.
- En segundo, porque en muchos casos el derecho de acceso a la información recae en datos personales de terceros lo que genera un conflicto jurídico entre ambos y exige recurrir al procedimiento de ponderación de bienes jurídicos en aparente colisión..

a) El derecho a la privacidad y el derecho de acceso a la información como complementarios.

La naturaleza complementaria de ambos derechos se pone de relieve cuando una persona pide información sobre sus datos personales. En efecto, el derecho de toda persona a exigir de quien sea responsable de un banco o base de datos la información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito de almacenamiento y la individualización de las personas u organismos a los cuales son transmitidos regularmente, implica ejercer el derecho de acceso a sus datos personales.

En concreto este derecho se contempla en el nuevo inciso primero que se introduce al artículo 12 en el proyecto que modifica la Ley N°19.628 y en el actual inciso primero del artículo 12 de la mencionada ley. Normas en las que se evidencia el carácter complementario del derecho a la privacidad y el derecho de acceso a la información.

De esta forma, el inciso primero que se propone incorporar, establece que "Toda persona podrá **solicitar** al Registro Único Nacional de Bancos de Datos **información** sobre la existencia de tratamientos de datos de carácter personal que pudieran afectarle, sus finalidades y todos los antecedentes necesarios para la identificación del responsable del tratamiento."

Por su parte, el actual inciso primero establece que "Toda persona tiene **derecho a exigir** a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, **información** sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente."

Como se aprecia, el derecho a la vida privada, en su aspecto positivo, está directamente relacionado con el derecho de acceso a la información. Es más, los derechos que pueden ejercer los titulares de los datos personales registrados en bancos de datos exigen, como requisito previo, ejercer el derecho de información y acceso a la misma; pues sin éste derecho esencial la protección de datos personales se volvería ilusoria, dejando sin contenido los derechos de rectificación, cancelación e indemnización.

Ahora bien, cuando dicho derecho se ejerce respecto de un organismo público, responsable del banco de datos, existirá coincidencia eventual entre el derecho de acceso a que alude la Ley N°20.285, de carácter general, y el derecho de acceso a los datos a que se refiere la Ley N°19.628, de carácter particular. Lo anterior, pues el artículo 10 de la Ley de Transparencia dispone que "Toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece esta ley." Y agrega que "El acceso a la información comprende el derecho de acceder a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como a toda información elaborada con presupuesto público, cualquiera sea el formato o soporte en que se contenga, salvo las excepciones legales."

Ya el Consejo para la Transparencia ha tenido ocasión de pronunciarse en esta materia, conociendo de un amparo al derecho de acceso a la información (**Decisión Amparo N°A29-09**). En lo que interesa, el solicitante requería los resultados de su evaluación personal en el proceso de selección implementado para proveer el cargo de Jefe de Cobranzas y Quiebras de la Tesorería General de la República. La Dirección Nacional del Servicio Civil (DNSC) invocó la causal constitucional de afectación de los derechos de las personas, prevista también en el artículo 21 N°2 de la Ley de Transparencia, argumentando que el titular de los informes sicolaborales no sería el postulante a que se refieren, sino la autoridad que solicitó la asesoría profesional para efectuar dicha evaluación. Al resolver este amparo, el Consejo estableció que aunque el informe haya sido encargado por la DNSC el titular de los datos allí contenidos es la persona a que se refieren dichos datos, en este caso, el postulante requirente. A este respecto y haciendo aplicación expresa de la normativa relativa a la protección de datos, determinó que es claro el art. 2° ñ) de la Ley N°19.628, sobre protección de datos personales, que entiende por "titular de los datos" a "la persona natural a la que

se refieren los datos de carácter personal". En consecuencia, el requirente tiene derecho a conocer su evaluación personal, con excepción de las referencias de terceros. Como puede observarse, el derecho de acceso a la información contemplado en la Ley N°20.285 fue utilizado por el titular de los datos personales para acceder a información personal que obraba en poder del organismo público.

En definitiva, como ha quedado expuesto, lo que encarga el Ordenamiento Jurídico al Consejo para la Transparencia es velar por el acceso universal a la información, tanto la de naturaleza privada (a la que sólo podrá tener acceso el titular para el ejercicio de sus derechos) como la de naturaleza pública (que reconoce un acceso universal con miras al control social del accionar público).

b) Derecho a la privacidad en la balanza con el derecho de acceso a la información (ponderación).

La naturaleza antagónica de ambos derechos surge cuando una solicitud de información contiene datos que son de carácter personal, lo que obliga al órgano público requerido a decidir si prevalece la protección de la vida privada o el interés público en dar a conocer la información solicitada.

Si efectuada la evaluación se define que existen derechos de terceros que puedan verse afectados, la Ley de Transparencia establece la obligación del órgano requerido de notificar al tercero, el que puede oponerse a la entrega de la información en forma escrita y con expresión de causa, y la posibilidad de invocar la causal de reserva del numeral 2 del artículo 21 de la Ley N°20.285. Luego, si el solicitante no estuviere de acuerdo, deducirá el reclamo correspondiente, y será, en definitiva, el Consejo para la Transparencia quien tendrá que decidir si prima el interés público en conocer la información o el interés personal que implicaría denegarla.

En esta labor de ponderación que el Consejo está llamado a realizar debe meditar con igual celo si es jurídicamente procedente dar a conocer la información que se haya solicitado, o bien, denegarla en razón de la protección de un dato de carácter personal.

Por consiguiente, de concentrarse ambas funciones —la de promover el acceso y velar por la protección de datos de carácter personal— en el Consejo, la labor de ponderación sería efectuada de una manera más eficiente y con criterios armónicos y uniformes.

Un caso práctico en que el Consejo ha ponderado ambos derechos se presentó a propósito de un amparo al derecho de acceso a la información interpuesto por una persona en contra de la Dirección Nacional del Servicio Civil por haberle negado el acceso a la información relativa al proceso de selección implementado para proveer el cargo de Subdirector de Estudios y Desarrollo del Servicio de Registro Civil e Identificación (**Decisión Amparo N°A35-09**). En lo relevante, respecto de los dos postulantes que no se opusieron a la entrega de su identidad ni informaron el traslado que les fue conferido, el Consejo estimó, en principio, que podría aplicarse el artículo 7° de la Ley N°19.628 declarando que sus identidades eran reservadas. Sin embargo, ello debía complementarse con el inciso final del art. 20 de la Ley de Transparencia, que

dispone que de no deducirse oposición por parte de la persona potencialmente afectada por la difusión de una determinada información dentro de los tres días desde que fue notificada de la solicitud "se entenderá que (…) accede a la publicidad de dicha información". Este último precepto, a juicio del Consejo, es el que debe preferirse en este caso tanto por su especialidad como por el interés público existente en conocer el funcionamiento del SADP dado que no se trata de la identidad de cualquier postulante; se trata de la de aquéllos que fueron propuestos a la autoridad por el respectivo Comité de Selección de directivos de segundo nivel jerárquico. Agrega que la conclusión anterior cambiaría tratándose del silencio de postulantes que no fueron incluidos en dicha nómina de candidatos. En efecto, en este segundo caso el Consejo estima que aplicando un test de daño o interés público prevalecería la reserva del dato personal sobre su publicidad, particularmente porque la difusión de tales identidades contribuiría escasamente a conocer el fundamento de la decisión adoptada. De allí que en esa hipótesis el Consejo, en caso de silencio, estima que debiera preferirse el art. 7° de la Ley N° 19.628 por sobre el inciso final del art. 20 de la Ley de Transparencia. Como puede verse, la resolución del amparo exigió al Consejo efectuar una ponderación caso a caso.

c) Otras decisiones del Consejo para la Transparencia en materia de protección de datos.

- **Decisión Amparo N°A10-09** y **Decisión Amparo N°A126-09.** En ambos casos el Consejo debió pronunciarse sobre la aplicación de la Ley N°19.628, la resolución se motivo a propósito de un amparo al derecho de acceso a la información interpuesto por una persona en contra del Ministerio de Vivienda y Urbanismo, el primero, y del Fondo Nacional de Salud, el segundo, por haberle negado el acceso a las calificaciones de todo el personal y ex-funcionarios, desde 2003 a 2008, en formato Excel, conteniendo las siguientes columnas: **R.U.T.**, tipo de contrato, estamento, sexo, puntaje, lista de calificación y año. En lo que interesa, el Consejo resolvió que a pesar de interés público que tiene la entrega de las calificaciones funcionarias y los razonamientos deben matizarse tratándose del Rol Único Tributario (en adelante R.U.T.) de los funcionarios y ex funcionarios, también requerido por el solicitante. En efecto, el R.U.T. es un código numérico creado por el D.F.L. N°3/1969, M. Justicia (D.O. 15.02.1969), con el fin de identificar "…a todos los contribuyentes del país, de los diversos impuestos, y otras personas o entes que se señalan más adelante" (art. 1°, inc. 1°), tanto las personas jurídicas como las naturales. Se trata de un dato de carácter personal o dato personal, esto es, relativo "a cualquier información concerniente a personas naturales, identificadas o identificables", conforme el art. 2° f) de la Ley N°19.628, de 1999, sobre protección de la vida privada o protección de datos de carácter personal, cuyo tratamiento sólo puede efectuarse cuando dicha ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello (art. 4° Ley N°19.628). En tal carácter, quienes trabajen "en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligados a guardar

secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público" (art. 7° Ley N° 19.628), esto es, aquéllas de acceso no restringido o reservado a los solicitantes. Que, por último, el art. 20 de la Ley N°19.628 dispone que "El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En estas condiciones, no necesitará el consentimiento del titular". Atendido lo anterior puede afirmarse que el R.U.T. de los funcionarios es un dato personal obtenido de los propios interesados en acceder a la función pública (art. 13 del Estatuto Administrativo), y no directamente de un registro público, sólo para su tratamiento al interior del servicio público respectivo y no para su cesión a terceros, por lo que debiera ser secreto o reservado. No cabe duda que en este caso particular, el Consejo debió hacer un análisis y aplicar, derechamente, las normas contenidas en la Ley N°19.628.

- **Decisión Amparo N°A33-09**. En el particular el amparo fue interpuesto por una persona para solicitar copia de la red familiar del causante de la herencia, que había denunciado como vacante, en contra de la Subsecretaria de Bienes Nacionales. El Consejo, tras analizar el R.C. Ord. N° 4783, de 14.04.2009, del Servicio de Registro Civil e Identificación, que informa la **red familiar del causante**, advirtió que contenía datos personales de los integrantes de dicha red, concretamente su R.U.N. o R.U.T., su domicilio y los datos de algunas inscripciones de matrimonio y de nacimiento. Previo análisis de las normas contenidas en la Ley N°19.628, se resolvió que no puede decirse que el R.U.N. o el R.U.T. y el domicilio de los terceros que constan en la red familiar en poder de la Subsecretaría de Bienes Nacionales provengan o hayan sido recolectados de fuentes accesibles al público. En efecto, se trata de datos personales a los cuáles sólo puede accederse con la autorización de su titular o cuando la ley lo permite, por lo que en definitiva, decretó el acceso a la información tarjando el R.U.N. y el domicilio.
- **Decisión Amparo N°A53-09**. En este caso el solicitante presentó amparo al derecho de acceso a la información por haberle sido denegado el acceso a la copia de los expedientes relativos a las multas cursadas en su contra, por la Dirección del Trabajo. No obstante estimar el Consejo que la confidencialidad en este procedimiento de fiscalización sólo rige durante su tramitación, se señaló que se reconoce que cierta parte de la información contenida en los expedientes solicitados por el reclamante podrían contener datos personales de terceros —e incluso sensibles—, que deberían ser protegidos de acuerdo a los arts. 2°, 4°, 7°, 10 y 20 de la Ley N°19.628, de 1999, sobre protección de la vida privada o protección de datos de carácter personal. Hace hincapié en el hecho que 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, dispuso que, respecto de aquellos datos personales señalados, cabe entender que la publicidad,

comunicación o conocimiento de dicha información puede afectar derechos de terceros —en el caso en análisis de los trabajadores denunciantes o de los que han prestado declaración—, en particular tratándose de la esfera de su vida privada y sus derechos de carácter económico emanados de la relación laboral, configurándose de esta forma y respecto de aquellos datos la causal del artículo 21, numeral 2 de la Ley de Transparencia, causal que se encuentra reforzada por la especial función que el artículo 33, letra m), de la Ley de Transparencia, encomienda al Consejo, en orden a velar por el adecuado cumplimiento de la Ley N°19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado.

VI. CONCLUSIONES Y ESTRATEGIAS DE FUTURO

La ampliación de competencias para el Consejo para la Transparencia, que supondría la aprobación del proyecto de ley mencionado, amerita las siguientes observaciones:

a) El Consejo para la Transparencia es un organismo de reciente creación, únicamente encargado de velar por el acceso a la información pública. Por ello, la eventual asunción de nuevas y exigentes responsabilidades en materia de protección de datos requiere de un proceso de transición y reforma institucional de cierta envergadura. En tal sentido, un razonable plazo de vacancia legal permitirá preparar la entrada en vigencia de la ley con los debidos estándares de buen servicio. No será fácil ni espontánea la adecuación al nuevo marco legal de actores públicos y privados acostumbrados a otras prácticas. Con todo, es dable destacar la muy útil y reciente experiencia adquirida en la instalación del Consejo, la misma que ahora deberá replicarse para abordar los desafíos que supone el proyecto de ley sobre protección de datos.

b) Asimismo, se debe afrontar **una reforma institucional** que permita insertar y armonizar las funciones de protección de datos y derecho de acceso a información pública, concentrando en el Consejo Directivo (máximo órgano de decisión del Consejo para la Transparencia), la función de precisar la doctrina en ambos campos.

c) La entrega de nuevas atribuciones en materia de protección de datos suponen la necesaria **asignación de recursos** para hacer frente a estos desafíos, lo que, en definitiva, exige un compromiso del país y sus instituciones en el desarrollo de la nueva institucionalidad.

d) No obstante encontrarse en tramitación el proyecto a que se ha hecho referencia, el Consejo para la Transparencia, conforme a lo establecido en la Ley N° 20.285, de Acceso a la Información Pública, ya cuenta con una importante atribución; como es velar por el cumplimiento de la Ley N° 19.628, de protección de la vida privada (art. 33 letra m). Por tanto, al menos respecto de organismos públicos nuestra institución tiene facultades para pronunciarse en materia de protección de datos personales y generar estándares básicos de protección.

e) En el ámbito internacional, el Consejo para la Transparencia con el propósito de conocer la experiencia de otras instituciones que se encuentran abocadas a la protección de datos personales, como con la finalidad de integrarse a redes internacionales de autoridades en la materia, realizó una visita Oficial a la Agencia Española de Protección de Datos y a la Information Commissioner´s Office de Reino Unido (junio 2009), y participó en la Conferencia Internacional de Comisionados de la Información (septiembre 2009), la que tuvo lugar en Oslo.

En este mismo contexto, agredecemos la cordial invitación efectuada para ser parte de este VII Encuentro Iberoamericano de Protección de Datos y de la 31° Conferencia Internacional de Protección de Datos. Sin lugar a dudas, el camino que nos queda por recorrer se hará más llevadero si conocemos y aprendemos de las lecciones de implementación y del quehacer diario y cotidiano de cada uno de ustedes.

ALEJANDRO FERRERIO YAZIGI

CONSEJERO

CONSEJO PARA LA TRANSPARENCIA

CHILE