

Derecho de acceso a la información pública y protección de datos personales

*The Right to Access to Public Information and Information
Privacy*

JESSICA MATUS ARENAS

Abogada, Consejera Instituto Chileno de Derecho y Tecnología, Chile

RESUMEN El presente trabajo indaga en el problema del equilibrio entre la Ley de Transparencia y Acceso a la Información Pública y la Ley de Protección de Datos, considerando que los organismos públicos están obligados legalmente a entregar información salvo las hipótesis de excepción a las reglas de publicidad, especialmente cuando ésta pudiera afectar los derechos de las personas, especialmente cuando se trata de aspectos de su vida privada. En el artículo se describe el estado actual de la discusión en Chile, el rol que le ha correspondido desempeñar al Consejo para la Transparencia desde su creación, analizando sistemáticamente su copiosa jurisprudencia, las principales iniciativas legislativas relacionadas y la armonización necesaria que debe existir entre ambos derechos en aparente conflicto. Finalmente, se presentan algunas orientaciones prácticas y recomendaciones que dan cuenta de la necesidad de contar con un órgano regulador independiente en nuestro país que tenga facultades efectivas de sanción y fiscalización.

PALABRAS CLAVE Protección de datos, privacidad, acceso a la información pública, armonización de derechos en conflicto, Consejo para la Transparencia.

ABSTRACT This work explores the balance issues existing between the Transparency and Access to Public Information Act and the Data Protection Act, taking into consideration that public institutions are legally required to provide the information, except when legally exempted by law, particularly when this disclosure could affect the rights of individuals, and namely their privacy. This article discusses the current status of this debate in Chile, the role that carried out by the Transparency Council since its creation, making an analytical study of the abundant body of decisions issued by the Council; the main related legislative initiatives; and the necessary accommodation that must exist among these apparently conflicting rights. Finally, this work proposes practical guidelines and recommendations that reflect the need for an independent regulatory agency in our country, with effective punitive and enforcement authority.

KEYWORDS Data protection, privacy, access to public information, harmonization of conflicting rights, Transparency Council.

Hasta el año 2008, al solicitar información a un órgano público los ciudadanos debían sujetarse a las reglas propias de cada institución y a su discrecionalidad al momento de decidir si otorgarle o no acceso a la información requerida. El legislador realizó varios intentos para transparentar el ejercicio de la función pública, que se veía entorpecida por resoluciones, decisiones y decretos que declaraban reservado o secreto ciertos actos de la administración pública. Por otro lado, existía un gran desconocimiento ciudadano acerca de lo que se tenía derecho a conocer sobre el funcionamiento del sector público.

Con la publicación de la Ley 20.285 de Transparencia y Acceso a la Información Pública (en adelante, «Ley de Transparencia»), el Estado materializó el principio constitucional de la transparencia de la función pública. Junto a ello se reconoció el derecho de acceso a la información pública, el cual establece los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información, siendo una de ellas la protección de los datos personales.

La Ley 19.628 sobre Protección de la Vida Privada (en adelante, «Ley de Datos Personales») y la Ley de Transparencia, establecen un marco general para el tratamiento de datos que se verifique en el sector público, considerando que esos datos están contenidos en actos o documentos de

carácter público sobre los cuales existe una legítima aspiración de acceso y disponibilidad por y para los ciudadanos.

En este sentido, ambas leyes son contrapesos de una misma situación, que consiste en cómo se deben tratar estos datos, cuáles son los derechos de los titulares y las limitaciones al derecho de acceso cuando la información solicitada contiene datos personales de terceras personas.

Cabe recordar que durante la tramitación de la Ley de Transparencia se señaló expresamente que «no es admisible entender que, a través de la transparencia, se pueda llegar al conocimiento de las características físicas o morales de las personas o de las autoridades de turno [...] o a hechos o circunstancias de su vida privada o íntima, 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 de los funcionarios públicos».¹

Así, el Estado es uno de los principales tenedores de información personal, siendo ésta necesaria para cumplir eficientemente con la implementación de políticas públicas, la entrega de determinados beneficios o por razones de planificación, gestión y orden público, por mencionar algunas. En el ejercicio de sus funciones los órganos del Estado almacenan y registran hechos en documentos y bases de datos, efectuando tratamiento de datos personales, incluyendo datos personales sensibles.

Cabe destacar que es la propia Ley de Datos Personales, en su artículo 20, la que faculta a todo organismo público a efectuar cualquier tratamiento de datos personales, sin autorización del titular, dentro de la órbita de su competencia, para lo cual no se requiere de texto específico que autorice el tratamiento de datos personales; sólo se necesita que éste se inserte dentro de la esfera de las atribuciones y competencias que tiene asignada por ley. También exige que las bases de datos en poder de dichos organismos públicos, aunque sin sanción en caso de incumplimiento, deban inscribirse en el Registro de Bancos de Datos que lleva

1. Trámite Comisión Mixta: Senado Discusión en Sala. Legislatura 355, Sesión 84, 16 de enero de 2008. Discusión Informe Comisión Mixta: «En consecuencia, aparte de la transparencia que se incorpora en el proyecto, hay medidas para proteger la vida privada, lo cual nos parece fundamental para que no se entienda que aquella puede llegar al punto de afectar la privacidad de la gente».

el Servicio de Registro Civil e Identificación, observándose al año 2011, conforme a un estudio realizado por la Fundación Pro Acceso, que sólo el 43,2% de ellos había dado cumplimiento ha dicho mandato. En 2012, se manifiesta un aumento, alcanzando un 64%.²

El estudio efectuado en 2011 revela que el cumplimiento de la ley no es homogéneo por parte de la administración. Por ejemplo, existen falencias respecto a la seguridad de la información, dado que un 14,4% de los organismos identifica las políticas de privacidad como la medida de seguridad para resguardar el debido secreto de la información que maneja, confundiendo el objeto que persiguen en esta materia; un 17% de los órganos públicos no contaba con un responsable encargado de velar por el tratamiento de datos personales al interior de su institución en el 2011. Se reveló, asimismo, que al año 2012, un 36% de los organismos que reconocía poseer bases de datos no contaba con un encargado del tratamiento de los datos personales. Por último, en el año 2011, un 48% de los servicios manifestó haber realizado transferencia o cesión de datos a un ente público o privado durante el último año, porcentaje que se reduce a un 35% de transferencias a otros organismos públicos y a un 16% a privados, en el año 2012.

Frente a este panorama, y dotado el Consejo para la Transparencia (en adelante, el «Consejo») de la atribución de velar por el cumplimiento de la Ley de Datos Personales, ha dado los primeros pasos incorporando algunas recomendaciones en el Instructivo núm. 4 sobre Transparencia Activa, en el Instructivo General núm. 10 sobre el Procedimiento Administrativo de Acceso a la Información, y luego dictando en concreto las denominadas «Recomendaciones sobre protección de datos personales por parte de los órganos de la Administración del Estado», con el propósito de contribuir a elevar los estándares de protección de los datos personales en poder de dichos órganos y asegurar los derechos que la ley reconoce a los titulares de los mismos.

No obstante, en sede legal y reglamentaria, no se han presentado avances. La discusión acerca del tratamiento de datos personales por parte de organismos públicos y privados tendrá lugar durante este año,

2. «Protección de Datos Personales en el Servicio Público», disponible en <[http://www.proacceso.cl/files/Estudio Datos Personales 202011.pdf](http://www.proacceso.cl/files/Estudio_Datos_Personales_202011.pdf)>.

en el que viene a representar el segundo intento legislativo³ en la materia, evidenciando un retraso respecto a sus pares latinoamericanos.

ESTADO ACTUAL DE LA PROTECCIÓN DE DATOS Y EL ACCESO A LA INFORMACIÓN

CARENCIA DE UN ÓRGANO ENCARGADO DE LA PROTECCIÓN DE DATOS

La Ley de Datos Personales no contempló la creación de un organismo público encargado de velar por el cumplimiento de sus disposiciones. Se limitó a establecer determinados principios en cuanto al tratamiento de datos personales por parte de organismos públicos y privados, y entregó a la justicia ordinaria el conocimiento de los conflictos que se suscitaban.

Con la dictación de la Ley de Transparencia, se creó un organismo autónomo —el Consejo para la Transparencia—, encargado de promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información. Además, se le entrega la atribución de velar por el debido cumplimiento de la Ley de Datos Personales respecto de los órganos de la Administración del Estado, no otorgándosele facultades de sanción alguna en este caso.

PROTECCIÓN DE DATOS PERSONALES EN LA LEY DE TRANSPARENCIA

En primer término, la Ley de Transparencia entrega la atribución al Consejo de velar por el cumplimiento de la Ley de Datos Personales, sin concederle facultad de sanción, como ya se indicó.

En materia de derecho de acceso a información, la ley dispone como causal de denegación de una solicitud (reserva o secreto) la afectación de los derechos de las personas, particularmente tratándose de la esfera de su vida privada (artículo 21.º núm. 2).

Por otra parte, en materia de transparencia activa, la ley exige la publicación de variada información pública, tal como la dotación de per-

3. Boletín 8143-03, proyecto elaborado por el Ministerio de Economía y presentado en 2012, el cual desechó el anterior proyecto de ley (Boletín 6120-07) del año 2009, que entregaba al Consejo para la Transparencia las facultades de protección de datos respecto de organismos públicos y privados.

sonal, ya sea de planta, contrata y honorarios, con las correspondientes remuneraciones; las contrataciones de suministros con indicación de los contratistas e identificación de los socios y accionistas principales de las sociedades o empresas prestadoras, en su caso; las transferencias de fondos públicos que efectúen, incluyendo todo aporte económico entregado a personas jurídicas o naturales, directamente o mediante concursos.

ROL DEL CPTL EN MATERIA DE PROTECCIÓN DE DATOS

Se puede observar que el rol del Consejo en protección de datos abarca tres ámbitos claramente definidos: la dictación de instrucciones en materia de transparencia, la resolución de los casos sometidos a su conocimiento y la dictación de recomendaciones específicas.

En relación a la dictación de instrucciones sobre transparencia, en las que se refiere a datos personales, podemos destacar que en el texto refundido de las Instrucciones Generales sobre Transparencia Activa (núms. 4, 7 y 9)⁴ el Consejo ha dispuesto en lo relativo a la protección de datos personales que:

- Frente a los actos y resoluciones que tengan efectos sobre terceros, los Órganos de la Administración del Estado deben abstenerse de publicar datos personales que tengan carácter reservado conforme a lo establecido en los artículos 7.º, 10.º, 20.º y siguientes de la Ley de Datos Personales. Asimismo, cuando se trate de actos administrativos sancionatorios,⁵ conforme al artículo 21.º de dicha normativa, deben abstenerse de publicar 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 reso-

4. Publicada en el Compendio de Normativa Chilena sobre Transparencia, Acceso a Información y Protección de Datos Personales en junio de 2012, disponible en <http://www.consejotransparencia.cl/consejo/site/artic/20120719/asocfile/20120719140710/refundido_ig4_7_9.pdf>.

5. Se reconduce al acápite 6.3 de las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado.

luciones 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.

- Respecto al diseño, montos asignados y criterio de acceso a los programas de subsidios y otros beneficios que entregue el respectivo órgano, además de las nóminas de beneficiarios de los programas sociales en ejecución, la Instrucción dispone que no se individualizarán los beneficiarios cuando ello suponga la revelación de datos sensibles, esto es, de datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. En estos casos deberá informarse el número total de beneficiarios y las razones fundadas de la exclusión de la nómina. Asimismo, en la publicación de nóminas de beneficiarios de programas sociales en ejecución debe indicarse el nombre completo de los beneficiarios, la fecha de otorgamiento del beneficio y la identificación del acto por el cual se le otorgó, excluyendo determinados datos como, por ejemplo, domicilio, teléfono y correo electrónico del beneficiario, por no ser estrictamente necesarios para individualizarlo.

Mediante la Instrucción General núm. 10, sobre el Procedimiento Administrativo de Acceso a la Información (2012),⁶ el Consejo dispone:

- En materia de formatos de presentación y requisitos de las solicitudes de acceso a la información, la identificación del solicitante exige la acreditación de la representación del requirente cuando se

6. Disponible en <http://www.consejotransparencia.cl/consejo/site/artic/20120719/asocfile/20120719141231/refundido_ig10.pdf>. Este texto refunde la Instrucción General núm. 10 del Consejo para la Transparencia sobre el procedimiento administrativo de acceso a la información (publicada en el *Diario Oficial* de 17 de diciembre de 2012), con el Acuerdo del Consejo para la Transparencia que la complementa en lo relativo a su fiscalización (publicado en el *Diario Oficial* de 17 de febrero de 2012).

soliciten datos personales de la persona representada. Dicho poder debe constar en escritura pública o documento privado suscrito ante notario.

- En cuanto a la prohibición de exigir en la solicitud el cumplimiento de requisitos no contemplados en la Ley de Transparencia ni en su reglamento, los órganos deben abstenerse de requerir en los formularios de solicitud o en las solicitudes de acceso, como campo obligatorio, para efectos de registrarse en el sistema electrónico de solicitudes, permitir la presentación de las mismas o dar curso a una solicitud de acceso como requisito de admisibilidad, datos como número de cédula de identidad y/o rol único tributario, teléfono fijo o móvil, género, sexo, nivel educacional, estado civil y pertenencia a alguna institución. La especificación de la ciudad y la región correspondientes al domicilio sólo se podrá exigir cuando el requirente opte por ser notificado por correo postal. Establece, asimismo, que se podrá solicitar a los usuarios que faciliten otros datos personales distintos a los exigidos en el artículo 12 de la Ley de Transparencia, únicamente con fines estadísticos y de forma voluntaria, debiendo el órgano informar estas circunstancias.
- En cuanto al análisis de la eventual afectación de derechos de terceros, procedimiento de notificación y ejercicio del derecho de oposición, la Instrucción dispone que tratándose de datos sensibles en ausencia de oposición se entenderá que el tercero no accede a la publicidad, debiendo aplicar el órgano público, de ser precedente, el principio de divisibilidad respecto de los documentos que los contengan. Excepcionalmente, de concurrir alguno de los supuestos establecidos en la letra c del artículo 21 núm. 1 de la Ley de Transparencia, podrá el órgano requerido omitir la notificación a que alude el párrafo primero de este apartado y denegar la solicitud por afectar el debido cumplimiento de las funciones del órgano.
- Respecto de la revisión de la información y redacción de la respuesta, se considera como buena práctica que los órganos publiquen en la sección «Transparencia activa» los actos administrativos por los cuales se acceda a las solicitudes de acceso a la información,

clasificándolos por materia y fecha, salvo cuando se trate de información que hubiese sido entregada exclusivamente en atención a la persona del peticionario, caso en el cual deberá abstenerse de publicar la respuesta correspondiente, por ejemplo, cuando lo solicitado sean datos personales sensibles y el solicitante es el titular de esos datos.

- En materia de entrega efectiva de la información solicitada, señala que no se podrá condicionar la entrega a que el solicitante otorgue su autorización para el tratamiento de sus datos personales con finalidades distintas a las de efectuar la tramitación del procedimiento administrativo de acceso a la información, como puede ser el envío de un boletín informativo del servicio.
- Específicamente en lo que se refiere a la entrega de información que contenga datos personales y el peticionario indique ser su titular, sólo procederá la entrega presencial y quien la efectúe deberá verificar que la información sea retirada por quien efectivamente tenga dicha calidad o por su apoderado, conforme a lo dispuesto en el artículo 22.º de la ley 19.880. En este caso, los solicitantes que concurran al respectivo órgano público a retirar la información requerida deberán acreditar su identidad mediante la exhibición de la cédula expedida por el Servicio de Registro Civil e Identificación, y quienes actúen como sus apoderados deberán además demostrar haberseles otorgado el respectivo poder, por escritura pública o instrumento privado suscrito ante notario. En forma excepcional, procederá la entrega por medios electrónicos cuando el titular utilice firma electrónica avanzada, conforme a lo dispuesto en la Ley 19.799. Por su parte, cuando se soliciten documentos y otros formatos en los que se contemplen datos personales de terceros y no hayan sido requeridos, se procederá a tachar los mencionados antecedentes, debiendo consignar en el formato respectivo que el tachado se procedió a efectuar en virtud de lo dispuesto en la Ley de Datos Personales.
- Cuando la información solicitada contenga datos sensibles de un tercero y se haya procedido a notificarlo, sin manifestarse consentimiento expreso por su parte, el órgano tachará aquellos datos en

virtud del principio de divisibilidad, debiendo consignar en el formato respectivo que ello se debe a la aplicación de la Ley de Datos Personales, y entregará la restante información.

Las recomendaciones del Consejo relativas a la Protección de Datos Personales por parte de los Órganos de la Administración del Estado,⁷ proponen una serie de buenas prácticas complementarias de las normas obligatorias contenidas en la Ley de Datos Personales, las que, en su carácter de recomendaciones, tienen 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, dicho instrumento recoge en su texto las obligaciones que dispone la ley y las complementa con orientaciones que facilitan su cumplimiento homogéneo por parte de la administración.

Las recomendaciones sugieren que las distintas autoridades de los órganos designen a un funcionario para desempeñarse como encargado de protección de datos y constituya un contacto efectivo en la materia con el Consejo para la Transparencia.

La resolución de casos resulta ser el rol más interesante del Consejo a la hora de valorar y ponderar ambos derechos en juego, dado que muchas veces las solicitudes de información recaen sobre documentos o antecedentes que contienen datos personales de terceros. El principio de máxima divulgación contenido en la normativa sobre transparencia y el de finalidad, en el caso de las normas sobre datos personales, ha tornado difícil el equilibrio de ambos derechos.

El Consejo tiene la facultad de resolver cuestiones de relevancia jurídica sometidas a su conocimiento, en la oportunidad y mediante la forma establecida en su propia ley. La particularidad de esta facultad radica en que el Consejo actúa conociendo y fallando, al mismo tiempo, un determinado caso. Es interesante ver cómo las otras potestades del Consejo delimitan los extremos de la legalidad en el tratamiento de la información de manera formal. En efecto, en la medida que proliferan instrucciones

7. Disponible en <http://www.consejotransparencia.cl/consejo/site/artic/20110914/asocfile/20110914100108/propuesta_de_recomendacion_pd_vf_09sept2011_publicacion_do.pdf>.

y recomendaciones, se crean criterios de corrección de comportamiento, de interpretación normativa y de previsibilidad en cuanto a lo que será derecho válido frente a determinadas circunstancias.

Es relevante destacar que las resoluciones del Consejo están delimitando constantemente los extremos de derechos constitucionales. No es menor que los principios en virtud de los cuales funda sus decisiones tienen un trato directo en el proceso interpretativo.

OBLIGACIONES DE LOS ORGANISMOS PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS

Conforme a la Ley de Datos Personales, los organismos públicos 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 consentimiento del titular bajo estas condiciones. *A contrario sensu*, si los organismos públicos tratasen datos fuera del ámbito de su competencia, requeriría el consentimiento del titular de los datos.

En este contexto, los órganos públicos deben respetar las reglas dispuestas en la ley, que no son otras que el deber de informar al titular acerca de la identidad del responsable de la base de datos, de la finalidad perseguida con el tratamiento de ellos, de la posible comunicación a terceros, de los derechos que pueden ejercerse por los titulares, entre otras.

Los organismos públicos deben cumplir con los principios de información, calidad de los datos y seguridad. Además, la ley les exige inscribir los ficheros o bases de datos que tienen a su cargo en un registro, que para estos efectos lleva el Servicio del Registro Civil e Identificación.

DECISIONES DEL CONSEJO PARA LA TRANSPARENCIA

El Consejo, a través de sus decisiones, ha declarado generalmente la reserva de la información cuando ésta contiene datos personales, no obstante, en determinados casos ha aplicado los denominados test de daño y de interés público, ordenando la entrega en consecuencia bajo dichos criterios.

El test de daño o principio de proporcionalidad⁸ consiste en el balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación; en el presente caso proteger la vida privada de una persona determinada. Tratándose de un derecho de rango constitucional, la reserva o secreto debe respetar el principio de proporcionalidad que supone analizar: a) si la medida es eficaz, b) si no existe un medio más moderado para la consecución eficaz del propósito buscado (en este caso, cautelar el secreto) y, por último, c) si de la medida a adoptar (en este caso, el secreto absoluto) derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Este test ha sido aplicado en general en materia de sumarios administrativos.

En virtud del test de interés público, se debe determinar la existencia de 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 en cuanto a su vida privada, que serían vulnerados de publicarse la información requerida.

Algunas decisiones relevantes se encuentran en lo que sigue:⁹

MATERIA: ABUSO POR PARTE DEL ÓRGANO EN LA ENTREGA DE INFORMACIÓN SOLICITADA

Acta de elección sindical (C432-10)

- Se solicitó copia del acta de una elección sindical, pero el organismo proporcionó al petionario no sólo la citada acta sino también el detalle de la votación, donde constan los integrantes del sindicato que votaron favorablemente por el delegado electo y todos los partícipes en dicha elección, con indicación de su nombre, RUT, firma domicilio, nacionalidad, fecha de nacimiento y número de teléfono celular.

8. Decisión del Consejo A45-09, reproducido en decisiones posteriores.

9. El Consejo elaboró en el año 2011 un primer Informe sobre Jurisprudencia relevante en relación a la protección de datos personales. Disponible en <http://www.consejotransparencia.cl/consejo/site/artic/20110615/asocfile/20110615173431/informe_2_0.pdf>.

- El reclamante señala que con ello se vulneró el deber de resguardo del secreto electoral.
- El Consejo representa al organismo reclamado no haber tarjado los datos personales de contexto del delegado electo, tales como su RUT, domicilio, nacionalidad, fecha de nacimiento y número de teléfono celular, datos que se encuentran protegidos por la Ley de Datos Personales, infringiendo, así, el principio de divisibilidad.

Datos de alumnos menores de edad, calificaciones (C392-12)

- Se solicitan Planes de Educación Media Formación Diferenciada Humanística-Científica, de 3.º y 4.º, informadas en las actas de un colegio para el período lectivo 2011, como así también los docentes, que se informó que los impartieron, pero el Mineduc entrega copias de las actas digitales del registro de calificaciones finales y promoción de alumnos, que contienen datos personales de éstos, tales como los nombres, RUT, fecha de nacimiento y sus calificaciones, así como también el nombre completo y RUT de los profesores de dichos cursos.
- El Consejo indica que no han sido resguardados los datos conforme a la Ley de Datos Personales, especialmente tratándose de menores de edad, y cita la Convención de Derechos del Niño, en su artículo 16.1, que 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».
- Otros casos de datos personales de menores de edad en C80-10, C579-10, C816-10, C906-10. El Consejo en estos casos representa a los órganos no haber dado adecuada protección a los datos personales que debe cautelar, de conformidad al cuerpo normativo respectivo (C901-11 y C208-12).

MATERIA: DATOS PERSONALES Y TRANSPARENCIA ACTIVA

Contrato de sala cuna en Gobierno Transparente (C579-10)

- Reclamante indicó que el órgano 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 esta última.

- El Consejo estimó que siendo competente para pronunciarse sobre el cumplimiento de la Ley de Datos Personales, al establecer el artículo 8.º de la Ley de Transparencia que la acción de reclamación resulta procedente cuando el organismo «no informa lo prescrito» en el artículo 7.º de la ley, debe entenderse que el incumplimiento de la obligación de informar 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 Ley de Transparencia y las disposiciones aplicables de la Ley de Datos Personales.
- Conforme a lo anterior, en aplicación del artículo 47 de la Ley de Transparencia, el Consejo podrá sancionar a la autoridad que «injustificadamente» no divulgue la información requerida por el artículo 7.º, lo haga comunicando datos personales cuya comunicación no responde a la finalidad autorizada por el legislador, o divulgue información secreta o reservada.

MATERIA: DIVULGACIÓN DE DATOS POR APLICACIÓN DE TEST DE DAÑO

Copia sumario administrativo (617-09, 664-10)

- Se solicita copia del sumario administrativo instruido en contra de determinados funcionarios de una universidad pública.
- El Consejo estimó que si hubiesen existido derechos de los exfuncionarios que pudieren verse afectados, realizando un test de daño, el beneficio de conocer los resultados de un sumario iniciado 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.

MATERIA: DIVULGACIÓN DE DATOS POR APLICACIÓN DE TEST DE INTERÉS PÚBLICO

Patentes municipales (C610-10)

- Resolvió el Consejo 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.
- 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 respectiva para este solo 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.
- Entiende que 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: 1) el cumplimiento de los requisitos necesarios para el ejercicio de la actividad que se autoriza por medio de la patente; y 2) 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.
- Aplica entonces el test de interés público: la reserva de los datos personales que interesan al reclamante podría ceder en beneficio de su publicidad, por el manifiesto interés público que revisten.
- Otros casos de aplicación del test de interés público: C335-10, C626-10, A115-09 y A244-09.

MATERIA: CORREOS ELECTRÓNICOS

Contenido de los correos electrónicos de un funcionario público (C640-10 y C83-10)

- El Consejo ha estimado que no puede considerarse privada una carta enviada por un particular a un funcionario público, porque se trata de materias propias que mantiene el particular con la administración del Estado.
- Voto disidente del consejero Jorge Jaraquemada: «los correos electrónicos se encuentran protegidos por la garantía contenida en el artículo 19 núm.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».
- En el caso C1101-11, se solicitaron los correos electrónicos enviados y recibidos por el Ministro Secretario General de la Presidencia, desde y hacia su cuenta de correo institucional entregada por el Estado para el correcto desempeño de sus funciones. El Consejo acoge el amparo señalando que los correos electrónicos de funcionarios públicos, enviados o recibidos desde su casilla institucional y en ejercicio de funciones públicas —esto es, no los que tengan que ver con su vida privada o personal—, son públicos si no se acredita la concurrencia de una causal legal específica de secreto o reserva. El secreto o la reserva de la información dependen del contenido y no del continente. Sólo así son posibles el control y la participación ciudadana en el ejercicio de las funciones públicas y el adecuado ejercicio de la libertad de expresión (con voto disidente del consejero Jorge Jaraquemada). El organismo presentó ante la Corte de Apelaciones de Santiago un recurso de ilegalidad para luego interponer una acción de inaplicabilidad por inconstitucionalidad ante el Tribunal Constitucional (Rol 2246-12-INA), la que fue acogida.
- En el caso C406-11, en contra de la Subsecretaría del Interior, el

Consejo señala que en virtud del principio de divisibilidad, los correos electrónicos institucionales que versan sobre atribuciones y ejercicio de funciones de órganos públicos no son comunicaciones privadas, pero si éstos también contienen antecedentes relativos a la vida privada de sus emisores o receptores debe denegarse acceso exclusivamente en esta parte. Por lo que se acoge amparo y se ordena que se entregue copia de los correos sólo en aquella parte que hable de atribuciones o funciones públicas (con voto disidente del consejero Jorge Jaraquemada). El organismo presentó ante la Corte de Apelaciones de Santiago un recurso de ilegalidad para luego interponer una acción de inaplicabilidad por inconstitucionalidad ante el Tribunal Constitucional (rol 2153-11-INA), la que fue acogida.

- En el caso C1482-11, en contra de la Subsecretaría de Transportes, en atención a la solicitud de correos electrónicos enviados y recibidos por las máximas autoridades y determinados funcionarios públicos, el Consejo acoge el amparo, ordenando entregar dicha información tarjando aquellos antecedentes acerca de la intimidad o la vida privada de su emisor o receptor que puedan contener los correos (con voto parcialmente disidente del consejero José Luis Santa María).
- Las decisiones señaladas precedentemente en los casos C1101-11, C406-11 y C1482-11, fueron recurridas de ilegalidad ante la Corte de Apelaciones de Santiago por las instituciones afectadas, bajo los roles núm. 2496-2012, 6704-2011, 5077-2012, respectivamente, existiendo sentencia favorable en los últimos dos casos. El fallo en el caso de la Segpres se encuentra pendiente a esta fecha.

Ficha clínica (persona fallecida) (C398-10, C322-10, C740-10)

- Una persona fallecida no es titular de datos personales, 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.

- El Consejo 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 calidades: a) ser heredero (a) del fallecido, de acuerdo a lo dispuesto en el art. 983 del Código Civil, o que se actúa en representación de uno o más herederos; b) tener una legitimación activa para ejercer otros derechos que supongan el acceso previo a la ficha clínica del difunto.

Listado de personas fallecidas por accidentes laborales (C64-10)

- 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 la vida privada.
- 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, pudiendo verse éstas afectadas en su propia honra.
- Respecto a si procede la notificación a todos ellos como terceros, se estimó que esto implicaría una distracción indebida de los funcionarios del órgano reclamado. Por otro lado 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.

Principio de finalidad, listado de cotizantes de una Isapre (C351-10, C418-10)

- Al tratarse de datos aportados directamente por las Isapres, y al no constituir información que deba mantenerse disponible al público, se descarta la aplicación del artículo 4.º inciso 5.º de la Ley de Datos Personales, por cuanto dichos datos no obran en poder del organismo reclamado por haber sido recolectados de fuentes accesibles al público. Así, aun 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.

Acceso a la base de datos de la Encuesta de Calidad de Vida y Salud (principio divisibilidad) (A190-09)

- Acoge el amparo y ordena entregar totalmente la base de datos, tarjando todos los datos personales y sensibles de los encuestados.

Acceso al padrón electoral del Servel (C407-09)

- Acoge el amparo y ordena entregar totalmente la base de datos, no pudiendo tarjarse los datos personales atendido que la Ley Orgánica Constitucional sobre el Sistema de Inscripciones Electorales y el Servicio Electoral señala que el «registro electoral» es público.
- Importante el voto disidente del consejero Juan Pablo Olmedo: los datos contenidos en el padrón «deben utilizarse sólo para los fines para los cuales se hubieren recolectado, salvo que provengan o se hayan recolectado 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 ahí consignados 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.

Información sobre fecha de entrada y salida del territorio nacional de una persona determinada entre ciertas fechas (control social) (A86-09)

- Se solicita información acerca de la fecha de salida del territorio nacional por un paso determinado de una persona específica, e ingreso al territorio nacional, entre ciertos meses.
- El organismo deniega la información por la obligación de guardar secreto respecto de los datos personales.
- El Consejo cita a la doctrina: «lo privado es el ámbito restringido de lo doméstico y lo familiar, de aquellos asuntos del sujeto, que

no necesariamente deben ser divulgados masivamente. Es el derecho fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público» y aplica la herramienta del *balancing test*, ponderando los derechos de acceso a la información del reclamante, con el de vida privada del tercero.

Elección sindical y nóminas (C532-II)

- Se solicita copia de las actas de constitución de determinados sindicatos interempresas, así como de sus estatutos y el listado de socios que concurrieron a su constitución.
- El Consejo señaló que la nómina de personas que concurrieron a la constitución de un sindicato, en tanto da cuenta de la afiliación sindical de una persona natural, constituye un registro o base de datos de carácter personal, por lo que se acogió parcialmente el amparo.

Condenados (CI414-II)

- Se solicitó todo documento que expliciten solicitudes de salidas esporádicas realizadas por internos durante los años que estuvieron reclusos en el Centro de Cumplimiento Penitenciario Punta Peuco, y todo documento referente a la aplicación de medidas disciplinarias que fueron cursadas a los reclusos durante esos años.
- El Consejo señaló que la información relativa a las medidas disciplinarias impuestas a un determinado interno ha de constar en la resolución que las aplica, sin embargo, la información relativa a las sanciones disciplinarias —de índole administrativa— impuestas por Gendarmería de Chile a un interno, en tanto se encuentran cumplidas, se subsumen en la hipótesis de secreto contemplada en el artículo 21 y respecto de su comunicación no concurre un interés público prevalente que justifique su comunicación, de manera que se rechaza su entrega, en cambio, a la comunicación de información relativa a las «salidas esporádicas» de los reclusos no le resulta aplicable.

- En C160-13 se solicitó a Gendarmería de Chile información sobre el recinto penitenciario en que se encuentran actualmente cumpliendo la condena respectiva y la fecha en que les será posible solicitar beneficios penitenciarios respecto de veintiséis personas que identifica con nombre, apellido, delito por el que fueron condenados y pena impuesta.
- El Consejo señaló que la información en cuestión si bien constituye datos personales, no se corresponde con la definición legal de «datos sensibles». En efecto, la esfera de publicidad que rodea la misma información impide que pueda ser considerada dentro de esta categoría. Resulta indicativo en este sentido la historia de la Ley de Datos Personales, cuyo texto original al referirse a la categoría en cuestión incluía la información referida a «condenas criminales» (Segundo Informe de la Comisión de Constitución del Senado); sin embargo, en la tramitación posterior dicha categoría fue eliminada como dato sensible, y así figura en el texto definitivo.

PRINCIPALES INICIATIVAS LEGISLATIVAS Y DE REGULACIÓN

Más allá del trabajo desarrollado por el Consejo en la materia, se encuentran actualmente en tramitación en el Congreso Nacional dos importantes iniciativas legislativas. La primera, una moción¹⁰ contenida en el Boletín 7686-07 que modifica la Ley de Transparencia e ingresada en junio de 2011, y la segunda en el Boletín 8143-03,¹¹ que modifica la Ley de Datos Personales, mensaje que fue presentado en el año 2012 por el Presidente Sebastián Piñera y elaborado por el Ministerio de Economía durante el año 2011.

La referida moción busca perfeccionar las debilidades o falencias que se pudieron detectar a dos años de vigencia de la Ley de Transparencia y reforzar la institucionalidad que regula el Consejo para la Transparencia. Dichos perfeccionamientos apuntan a mejorar el contenido de la información a que tiene acceso la ciudadanía a través de la transparencia activa, recogiendo algunas de las buenas prácticas que el Consejo ha

10. Presentada por los parlamentarios Jorge Burgos, Alberto Cardemil, Marcelo Díaz, Edmundo Eluchans, Felipe Harboe y Andrea Molina.

11. Disponible en <http://sil.congreso.cl/cgi-bin/sil_proyectos.pl?8143-03>.

contemplado en su Instrucción General; resolver una serie de indefiniciones legales con la finalidad de otorgar certeza jurídica a los solicitantes en materia de derecho de acceso y notificación a terceros, y en el procedimiento de reclamos y amparos; también supone mejoras respecto del reclamo de ilegalidad, plazos de reserva o secreto, y a las infracciones y sanciones establecidas en la ley.

Mediante indicaciones presentadas por el Ejecutivo al Boletín 7686-07, se incorpora lo siguiente respecto a datos personales:

- En la sección «Transparencia activa», los órganos deberán abstenerse de publicar en sus sitios electrónicos información que contenga datos personales amparados por la Ley de Datos Personales distintos a los exigidos en forma expresa en los incisos anteriores. En caso de contenerse en un documento este tipo de datos, se procederá a tachar dicha información, en virtud del principio de divisibilidad. No obstante, respecto de transferencia de recursos y nóminas de beneficiarios, la propuesta dispone la indicación del rol único tributario o rol único nacional que la persona tenga asignado.
- Cuando la información requerida contenga datos de carácter personal y el solicitante indique ser su titular, la entrega sólo podrá efectuarse a quien acredite efectivamente serlo o a su apoderado.
- Cuando no se hubiere deducido oposición por parte del tercero, entendiéndose que aquél accede a la publicidad de dicha información, el órgano respectivo siempre podrá ponderar si respecto de la información solicitada concurre alguna de las causales de secreto o reserva contempladas en el artículo 21, salvo que la información solicitada se refiera a sus datos personales, en cuyo caso se entenderá que el tercero no accede a la publicidad, debiendo aplicar el órgano público, de ser procedente, el principio de divisibilidad respecto de los documentos que los contengan.
- El incumplimiento injustificado de las normas sobre transparencia activa, de las demás normas de la ley y su reglamento, se sancionará con censura, multa de hasta un 50% de las remuneraciones o suspensión del empleo hasta por treinta días de la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado. En este caso, la normativa ya contiene disposiciones

relativas a la protección de datos, por tanto, su incumplimiento podrá ser sancionado por el Consejo.

Por su parte, el proyecto de ley que modifica la Ley de Datos Personales (Boletín 8143-03) busca «reforzar la idea del control sobre los datos de los cuales se es titular, esto es, favorecer la protección de los datos de carácter personal frente a toda intromisión de terceros, sean éstos públicos o privados, y, por tanto, establecer las condiciones bajo las cuales estos últimos podrán efectuar legítimamente el tratamiento de tales datos», considerando como contexto internacional la firma de Chile al Convenio de Adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE), dejando fuera la normativa y avances que en este ámbito jurídico la Unión Europea lidera.

La principal deficiencia de la iniciativa radica en que no crea un órgano de control independiente que vele por el cumplimiento de la Ley de Datos Personales, entregando ciertas funciones y responsabilidades al Servicio Nacional del Consumidor (en adelante, «Sernac»), en atención a las particularidades que la ley presenta y las atribuciones que esta institución posee.

En el mes de enero de 2013, el Ejecutivo formuló indicaciones al proyecto, definiéndose que el Ministerio de Economía, Fomento y Turismo deberá elaborar un informe, antes de cumplidos 4 años contados desde la publicación en el *Diario Oficial* de la ley, sobre el desempeño del Sernac, exclusivamente respecto al cumplimiento a sus funciones y prerrogativas establecidas en la ley, y se limita la vigencia de las facultades entregadas a esa repartición por un plazo de 5 años.

No obstante lo anterior, se destacan dos normas aplicables a los organismos públicos:

- Un nuevo artículo 4° A. «Excepciones al consentimiento previo», que permite a los organismos públicos tratar los datos sin consentimiento del titular a propósito de una investigación criminal o en el ejercicio de sus funciones y atribuciones autorizadas expresamente por ley, como asimismo si la interconexión, comunicación, transmisión o transferencia de datos personales se realiza entre organismos públicos, con el objeto de prestar servicios o conceder beneficios al titular que los solicita, en virtud de lo dispuesto en la letra c del artículo 17 de la Ley 19.880, por tanto, sólo en la medi-

da que el titular solicite la prestación de un servicio o la concesión de un beneficio determinado a un organismo público específico, su consentimiento no será necesario para la cesión de esos datos.

- La nueva redacción del artículo 20, relativo al tratamiento de datos personales por parte de organismos públicos, especifica que éste debe realizarse con sujeción a las reglas dispuestas en su propia ley orgánica o, en su defecto, a las normas especiales que establece la Ley de Datos Personales. Además, declara que pueden transferir y compartir datos personales con otros organismos públicos con el objeto de prestar servicios o conceder beneficios al titular que los solicita, evitándole a éste trámites adicionales para recolectar los datos personales que están en poder de otro organismo público, bajo los estándares establecidos en un reglamento. Permite, asimismo, la interconexión electrónica, otorgando derecho a los titulares de datos para que ejerzan su derecho de acceso u oposición ante cualquiera de los organismos públicos que compartan éstos o ante el administrador de la plataforma de servicios electrónicos del Estado, según sea el caso. Y, por último, establece principios a los que debe sujetarse el mencionado reglamento, tales como coordinación, gratuidad, no duplicación, unidad de acción y especificidad.

LA ARMONIZACIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES FRENTE AL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

El Estado, como detentador de una gran cantidad de información relativa a sus ciudadanos, tiene grandes desafíos al momento de ponderar los derechos de acceso a la información y de la protección de los datos respecto de la información que posee.

La relación entre ambos derechos es de permanente tensión, entre el objetivo de hacer pública determinada información gubernamental y la necesidad de proteger los datos personales que puedan estar contenidos en ella. Dicha tensión se produce dado que no existe un límite claro entre lo público y lo privado. Indudablemente la labor del organismo público es y será mantener un equilibrio en el ejercicio de ambos derechos.

En este contexto, resulta evidente que la Administración Pública ha

tenido avances y retrocesos en la materia. Si bien la labor que el Consejo ha realizado, mediante la dictación de sus recomendaciones de protección de datos y diversos dictámenes, ha permitido un progreso, los organismos públicos no han alcanzado el debido cumplimiento a la normativa de protección de datos. La falta de sensibilidad en esta materia se une al retraso normativo que Chile mantiene respecto a sus pares latinoamericanos y legislaciones europeas.

DATOS PERSONALES EN TRANSPARENCIA: UN LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN

Los órganos de la Administración del Estado son los primeros que se encuentran en situación de determinar si una solicitud de acceso afecta datos personales de terceros. La adopción de medidas de resguardo, el establecimiento de procedimientos de acceso a los datos, una política adecuada de tratamiento, de cesión, la obligación de confidencialidad y reserva son deberes de los organismos del Estado.

La regla general en materia de transparencia es que toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece la ley. Dicho derecho de 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.

La pregunta que aquí surge es ¿cómo debe operar el órgano? Frente a la causal de reserva o secreto establecida en el artículo 21 núm. 2, esto es, cuando la publicidad, comunicación o conocimiento de la información pudiere afectar la esfera de la vida privada de las personas, el órgano se encuentra en el deber de comunicar a dichos terceros la solicitud de acceso, o también denegarla cuando afecta este derecho.¹² La posibilidad de denegar derechamente por parte del órgano una solicitud por afectar la vida privada de una persona reviste especial relevancia dado que si el

12. El artículo 7 núm. 2 del Reglamento de la Ley de Transparencia, entiende por derechos aquellos que el ordenamiento jurídico atribuye a las personas, en título de derecho y no de simple interés.

tercero no ejerce su derecho de oposición, se entiende que accede a la publicidad de dicha información.

Una segunda interrogante es cómo se compatibiliza el artículo 17 de la Ley de Transparencia con el contenido esencial del derecho a la protección de datos. En este caso, la entrega de información en sede de acceso a ella «se hará por parte del órgano requerido sin imponer condiciones de uso o restricciones a su empleo, salvo las expresamente estipuladas por la ley», 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 Ley de Datos Personales, lo que supone una afectación al núcleo central del derecho a la protección de datos, la autodeterminación informativa (decisiones C351-10, C418-10).

BASES PARA UNA INTERPRETACIÓN

La interpretación normativa del Consejo se ha fundado, en el proceso dialéctico de reserva versus publicidad, en base a los test de daño y test de interés público (como lo veremos en el punto 1 siguiente). Por su parte, el Supervisor Europeo de Protección de Datos ha propuesto el criterio interpretativo del principio de proporcionalidad (punto 2). También la doctrina consagra una especie de interpretación, denominada armónica (punto 3).

1) Si bien el Consejo ha aplicado los test de daño e interés público en la resolución de los casos de que ha tomado conocimiento, son también los órganos públicos los que se encuentran en posición de aplicarlos cuando la solicitud de acceso contiene información relativa a terceras personas que pudieran ver afectado su derecho a la vida privada. Éste es el método actualmente utilizado por el Consejo para la Transparencia, y que puede describirse de la siguiente manera:

- El test de daño establece la obligación de la autoridad de demostrar que la divulgación de un determinado documento o información puede producir un daño a un valor o un derecho jurídicamente protegido. Corresponde que la autoridad lleve a cabo una ponderación de los valores en conflicto, esto es, el derecho de acceso a la información pública frente a la seguridad nacional, el derecho al honor, la privacidad, la libertad de expresión, la libertad económica, etc.¹³

13. El Consejo ha señalado: «balance entre el interés de retener la información y el

- El test de interés público tiene por objeto determinar si existe un interés público que justifique la divulgación de la información que se solicita 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 opone a su entrega, por vulneración a su vida privada, la salud, la honra, derechos que resultarían vulnerados de publicarse la información requerida.¹⁴

2) La normativa chilena relativa a la protección de la vida privada se ha inspirado, principalmente, en las regulaciones de Europa continental. Por la máxima interpretativa de *ratio legis*, es necesario que no sólo el fundamento específico del tratamiento del material normativo en una cuestión contingente sea analizado bajo los parámetros que motivaron el establecimiento de la norma. Si durante la vigencia de una ley surgen necesidades de modificación o de inclusión de nuevos criterios interpretativos, es necesario, desde un punto de vista de la coherencia del ordenamiento jurídico, recurrir a los fundamentos por los cuales fue necesaria la regulación. Pues bien, en nuestro análisis es posible constatar que la protección de los derechos constitucionales que se resguardan con la normativa en cuestión tiene en su proceso de interpretación jurídica unos principios generales (expresados a través de los test de daños e interés público), como *ratio legis*, que no son suficientes para dar el debido resguardo que se pretendió. Bajo estas circunstancias resulta importante considerar lo establecido en el documento «Acceso público a documentos y protección de datos»,¹⁵ del Supervisor Europeo de Protección de Datos,¹⁶ en el que se consagra el

interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación» (Decisión A45-09, Carabineros de Chile. Listado de escoltas).

14. Algunas decisiones del Consejo en que aplica dicho test: concursos públicos generales (identidades y puntajes de las distintas evaluaciones); concursos de alta dirección pública (acceso a informes psicolaborales); datos de donantes y beneficiarios (C361-10, C678-10, C488-10, C758-10); revelación de sanciones administrativas ya cumplidas (C335-10, C339-10, C111-10, C664-10, C73-10).

15. Disponible en <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_summary_ES.pdf>.

16. «La publicación de datos ‘en bruto’ es contraria a la normativa de protección de datos de carácter personal, habrá que establecer criterios de publicación menos lesivos

principio de proporcionalidad. Dicho criterio consta de los siguientes dos elementos:

- Las excepciones al acceso del público no deben superar los límites de lo adecuado y necesario para alcanzar la finalidad deseada.
- Hay que preguntarse si es posible lograr el mismo resultado mediante otras medidas menos restrictivas, por ejemplo, concediendo un acceso parcial a los documentos.

3) Es ilustrativo recurrir a doctrinas de países que poseen legislaciones de fuente y contenidos similares a la nuestra. El autor uruguayo Carlos Delpiazzo (2009), partiendo de la necesaria interpretación armónica de los derechos, señala que el intérprete debe centrarse en pensar cada uno de los derechos en juego desde su contenido esencial, a efectos de determinar, no el «peso» concreto de los mismos para apreciar cuál es más importante o cuál debe rendirse, sino cuál de ellos comparece y cuál no en el caso concreto. En el caso en particular señala que el equilibrio entre el derecho de acceso a la información pública por una parte, y el derecho a la protección de datos personales, por la otra, aboga a favor de este último cuando existen datos personales en poder de la Administración susceptibles de ser accedidos no sólo por el titular sino por terceros. Las razones que respaldan esta afirmación se basan en la diversa naturaleza de la información en juego, en los bienes jurídicos a ponderar, en los fines y, en definitiva, en el núcleo esencial de cada uno de ambos derechos.

Esta interpretación da pie para reflexionar que no toda información que posee el Estado es pública, no comprende a la información de carácter privado o personal por imperio de la ley dictada en razón del interés general; respecto al bien jurídico tutelado, los datos que se encuentren en poder de la Administración no implican que pueda desatenderse su finalidad, esto es, el propósito para el cual fueron recolectados; cada derecho presenta su propia finalidad y cada una respeta el fin del otro, si esto no sucede el derecho que se extralimita se desvirtúa en su fin; y por último, el contenido esencial de cada derecho, donde el núcleo determinante del

que permitan conjugar el principio de publicidad y transparencia en la actividad administrativa con el derecho de las personas a la protección de datos de carácter personal», disponible en <<http://www.iurismatica.com/blog/transparencia-publicidad-y-la-proteccion-de-datos-de-caracter-personal>>.

derecho a la protección de datos es la dignidad humana. A mayor abundamiento, la reserva y la publicidad no son principios opuestos, si el intérprete considera que éstos se aplican a diferentes objetos, información privada e información pública.

Al momento de la ponderación debe considerarse que el dato no se hace público, se hace accesible por parte de los solicitantes, por tanto, un dato de carácter personal, incluso hecho público, sigue siendo un dato personal y goza de protección.¹⁷ Por otra parte, la accesibilidad debe ser compatible con la finalidad; para ello, cualquiera podrá acceder al dato pero no al banco de datos en su conjunto. Se debe también impedir la indexación automatizada del dato, delimitando el uso de tecnologías al respecto.

Cuando pensamos en el control social que mediante la transparencia y el derecho de acceso a la información pública ejercen los ciudadanos sobre la Administración, es dable entender que las leyes de esta naturaleza están dirigidas a establecer cómo se ejercen las funciones públicas. Si ciertos datos personales son confiados por particulares para la toma de decisiones, el derecho de acceso no necesariamente alcanzaría la totalidad de esos datos, sino sólo en la medida que esos datos sean necesarios para establecer si el proceder del Estado ha sido conforme a la ley.¹⁸

En consecuencia, constituye una obligación de las instituciones hacer un balance, antes de divulgar información, entre la transparencia y la lesión de derechos.

ORIENTACIONES PRÁCTICAS DEL SUPERVISOR EUROPEO DE LA PROTECCIÓN DE DATOS¹⁹

Con el objeto de evitar judicializaciones de cuestiones previsibles y de dar una mayor certeza jurídica respecto de los márgenes de publicidad de la información que poseen las administraciones, el Supervisor Europeo de la Protección de Datos ha dado algunas orientaciones prácticas. Esta facultad debe ejercitarse con suma cautela, ya que en definitiva pue-

17. Decisión A190-09, Acceso a la base de datos de la Encuesta de Calidad de Vida y Salud; Decisión C407-09, Acceso al padrón electoral del Servel.

18. Decisión A86-09, Fecha de entrada y salida del territorio nacional de una persona determinada en un período determinado.

19. Disponible en <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_summary_ES.pdf>.

de interferir de manera indebida en la configuración de ciertos derechos, cuestión que sólo es competencia de la ley. Sin embargo, es ilustrativo que frente a situaciones evidentes las administraciones tengan directrices para operar con mayor eficiencia para el resguardo de los intereses de las personas y de la misma administración.

Para dicha autoridad, la regla general en la materia es que las instituciones deben denegar el acceso a un documento cuya divulgación suponga un perjuicio para la protección de la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales. Ahora bien, para que esté en juego la intimidad del interesado debe existir un interés cualificado de una persona involucrada, es decir, el documento o soporte en que se encuentre la información tiene que contener detalles sobre una persona que por lo general se consideren personales o privados. El mero hecho de que un documento contenga datos personales de carácter general, como el nombre de una persona, no debería —normalmente—, impedir su divulgación.

Por lo general, la intimidad está en juego cuando el documento contiene datos sensibles, por ejemplo, sobre su salud; cuando se refiere al honor y la reputación de la persona; cuando pudiera dar una imagen falsa de la persona; cuando divulga hechos embarazosos; y cuando divulga información dada o recibida por la persona con carácter confidencial.

Para que se vea afectado sustancialmente el interesado, debe darse cierto grado de perjuicio objetivo a su intimidad; no debería denegarse al público el acceso a los datos si la divulgación de los mismos sólo afectara superficialmente al interesado. En bastantes situaciones, el acceso del público a un documento no afecta a la intimidad del interesado, como por ejemplo cuando dichos datos personales ya han sido divulgados anteriormente.

Al analizar en qué medida la legislación sobre protección de datos permite la divulgación, desempeñan un papel clave el principio del derecho a la información, en que la divulgación debe ser compatible con los fines y el principio de proporcionalidad.

Es posible que determinadas informaciones que de forma directa no identifican a un titular puedan ser consideradas datos de carácter personal cuando dicha identificación es posible sin suponer la misma un tiempo o esfuerzo desproporcionados. O lo que es lo mismo, el hecho de que el interesado no aparezca identificado en una base de datos por su

nombre y apellidos no supone que dicho registro no contenga datos de carácter personal cuando dicha identificación puede o podría tener lugar con posterioridad a la recogida de tales datos.²⁰

RECOMENDACIONES

- Revisión de la normativa chilena de protección de datos y discusión con participación ciudadana. Boletín 8143-03, actualmente en el Congreso Nacional. Se requiere la urgente creación de un órgano de control en materia de protección de datos con facultades fiscalizadoras y sancionadoras.
- Capacitación a los organismos públicos en materia de protección de datos.
- Revisión del D.S. 83, de 2004, del Ministerio Secretaría General de la Presidencia, que establece la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, para el debido cumplimiento de las políticas de seguridad de la información.
- Establecimiento de sanciones en caso de incumplimiento al deber de registro de bases de datos en poder de organismos públicos.
- Realización de auditorías de seguridad en protección de datos, para garantizar el cumplimiento de la legislación de protección de datos y las normas autoimpuestas por la organización en la materia, a la luz de las recomendaciones del Consejo, y la calidad del sistema de medidas y procedimientos que la organización ha implementado para lograr ese objetivo (su diseño, existencia y eficacia). Lo anterior implica catalogar los archivos relacionados con los datos personales, catalogar las amenazas que pueden afectar los archivos, determinar los objetivos de la organización en materia de protección de datos, realizar el análisis de los posibles riesgos sobre los datos personales, y analizar la adecuación de las

20. Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007, del Grupo de Autoridades de Protección de Datos (G29). Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>.

medidas técnicas y administrativas que la organización ha implementado. En España, en el ámbito de la Administración Electrónica se prevén auditorías al menos cada dos años. El resultado de la auditoría debe estar a disposición de la autoridad de privacidad, en el caso, la Agencia Española de Protección de Datos, el que se mantiene durante dos años.

- Revisión de la modificación a la Directiva Europea de protección de datos, que se lleva a cabo actualmente, y que se encuentra vigente desde 1995, con el objeto de conocer los avances que Europa ha dado en la materia.

REFERENCIAS

DELPIAZZO, Carlos (2009). «A la búsqueda del equilibrio entre privacidad y acceso». En *Protección de datos personales y acceso a la información pública*, Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República, Fundación de la Cultura Universitaria y AGESIC. Montevideo: FCU.

SOBRE LA AUTORA

JÉSSICA MATUS ARENAS es abogada. Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile. Coautora del libro *El deber de información y el consentimiento para la cesión de datos personales*. Su correo electrónico es <jecamatus@gmail.com>. El presente artículo es una versión mejorada y actualizada del informe elaborado para la Fundación Pro Acceso en el marco de mesas de trabajo en torno al derecho de acceso a la información pública y su relación con el derecho a la protección de datos, en agosto de 2012.

Este trabajo fue recibido el 8 de mayo de 2013 y aprobado el 14 de junio de 2013.