PROTECCIÓN DE DATOS PERSONALES E INTEROPERABILIDAD EN LA ACCIÓN DEL ESTADO[1]

INTRODUCCIÓN

Es un hecho de nuestros tiempos que casi todos los gobiernos han implementado planes y programas para digitalizar sus procesos y documentos. Ello permitiría, de acuerdo a lo declarado por las propias administraciones, racionalizar el uso de los recursos públicos, otorgar una prestación eficiente de servicios a la ciudadanía, combatir la corrupción y otorgar mayores grados de transparencia a la gestión pública, todos objetivos que contribuirían a estimular la participación ciudadana.

Dentro del marco de esos planes y programas, la mayoría de las naciones han aprobado normativa sobre firma electrónica, comunicaciones electrónicas y mensajes de datos, sin lo cual esta digitalización no podría gozar de "equivalencia funcional", esto es, que sus procesos y documentos no puedan ser discriminados por su sola naturaleza, pues reúnen y cumplen la misma función que su símil no digital. La generación y aplicación de estas normas es fundamental en el desarrollo del gobierno electrónico, pues éste debe asegurar al ciudadano condiciones mínimas de operación en línea, tales como: la autenticidad (que sepa que la persona o el ente es en efecto quien manifiesta ser) integridad (que la información enviada o recibida se mantenga inalterada), y no repudio, entre otras.

Del mismo, si se considera que las actividades cotidianas se desarrollan principalmente a través de Internet, la construcción de una infraestructura para que la información producida por el Estado y que afecta o pueda afectar a los ciudadanos esté disponible, satisfaciendo de esa forma el derecho de acceso y transparencia desde y hacia los entes públicos, ha sido también una preocupación. En Chile, se ha recogido en alguna medida esta preocupación en la Ley de Acceso a la Información Pública[2], que exige que esta información[3] esté disponible y accesible para todos, disponiendo sobre su publicación por los órganos públicos (transparencia activa), así como sobre el

---

[1] Elaborado por Romina Garrido Iglesias, abogada investigadora de la Biblioteca del Congreso Nacional de Chile. Coautora del sitio Web http://protecciondedatospersonales.cl/ ; y Patricia Reyes Olmedo, abogada Jefe del Área de Recursos Legales de la Biblioteca del Congreso Nacional de Chile

[2] Ley N° 20.285 sobre acceso a la información pública, publicada en el Diario Oficial de 20 de agosto de 2008, entró en vigencia el día 20 de abril de 2009. http://www.leychile.cl/Navegar?idNorma=276363

[3] De acuerdo con la Ley N° 20.285 la información publica comprende todos los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo y esencial, y los procedimientos que se utilicen para su dictación. Asimismo, la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento.

resguardo del derecho de los ciudadanos para acceder a ella (transparencia pasiva). Un tema no menor en este ámbito está referido a la normalización de la documentación administrativa, toda vez que ésta no sólo afecta la seguridad en el uso, almacenamiento y distribución de los documentos, sino que contribuye a facilitar su intercambio entre servicios públicos, y entre éstos y el resto de la sociedad. Así visto, identificar los nuevos recursos digitales para su estructuración, acceso y referencia es un desafío en proceso en casi todos los países.

Al respecto, es preciso considerar que la producción de la documentación que integra el sistema de información pública, no es un hecho aislado *per se*, pese a que la generación de la misma se produce por cada organismo independientemente y es almacenada en las bases de datos propias, es necesario en determinados supuestos, que exista una interrelación entre la documentación digital que se refieren a las mismas materias o encuentran su fundamento en otro documento jurídico digital. Surgen entonces supuestos indispensables: disponibilidad, acceso e integración de esta información, para hacer tangible el derecho de acceso a la información.

El concepto de **interoperabilidad** recoge estos supuestos y está orientado a posibilitar que los sistemas de las Administraciones Públicas trabajen juntos de forma satisfactoria y productiva, esto es, que funcionen de manera mancomunada e integrada para lograr un fin definido, independientemente de la tecnología o la aplicación que se utilice, o de qué proveedor ha suministrado el sistema que contiene la información. Se concreta de esta manera el derecho de acceso a la información pública, posibilitando la navegación transparente de los ciudadanos a través de los portales públicos y/o la interrelación entre los servicios públicos para un mejor y más eficiente servicio. Es decir, acceso desde una plataforma común a distintos documentos electrónicos relacionados, aunque éstos se encuentren en distintas bases de datos. Para ello, se requiere acciones concretas del Estado destinadas a establecer estándares de almacenamiento e incorporar tecnologías a los procesos en las organizaciones públicas.

En este marco de la interoperabilidad es preciso considerar que los organismos públicos poseen y procesan información personal de los ciudadanos, situación que debe orientar acciones concretas del Estado destinadas a proteger la difusión, la seguridad informática y el tratamiento y procesamiento adecuado de los **datos personales**. Si bien en Chile existen algunas directrices o normas técnicas que

pasaremos analizar brevemente, en la práctica estos resguardos son insuficientes, y lo que es aún más preocupante no hay conciencia real de la necesidad de los mismos.

DOCUMENTACIÓN ELECTRÓNICA E INTEROPERABILIDAD

En el contexto internacional contemplamos hoy en día un panorama singular, un creciente número de tecnologías digitales al alcance de la ciudadanía y la transformación de la Web en espacio común de información de un número cada vez más significativo de usuarios, lo que permite la conexión transversal entre éstos de datos, recursos, información e ideas, y también el surgimiento de nuevas formas sociales basadas en la participación y la interactividad entre usuarios y proveedores de información. Es, esta interoperatividad un concepto clave para el desarrollo técnico del gobierno electrónico.

Efectivamente, en los últimos años, se ha desarrollado sustancialmente la implementación de servicios de la administración electrónica basados en la interoperabilidad y en el intercambio de recursos, entendiendo éstos como un paso crucial para la consecución de una verdadera administración electrónica en la que la información se pueda compartir fácilmente y en la que los esfuerzos sean únicos y no duplicados.

Para la puesta en marcha de un marco común para compartir e intercambiar datos e información en todos los niveles, se han sugerido, a nivel mundial, una serie de medidas horizontales, que consisten en servicios de infraestructura, así como servicios estratégicos y de apoyo, y que incluyen, entre otras:

- Desarrollo de aplicaciones basadas en lenguajes estándares, tales como XML, relacionados con el apoyo al intercambio de datos en redes.
- Generación de modelos funcionales y no funcionales para la gestión de registros electrónicos en las administraciones públicas.
- Establecimiento de normas para la generación de metadatos para la información del sector público.
- Creación de una política de formatos abiertos, con miras al intercambio de recursos

Queda claro de esta forma que la interoperabilidad entre sistemas, documentos y procesos adquiere importancia, y se revela como la forma de facilitar el acceso compartido a la información y su reutilización, la interactividad y el mejoramiento de los

procesos administrativos. La implementación de este tipo de servicios no sólo los hará más eficaces y disminuirá su costo final, sino que permitirá el uso de la documentación administrativa y el suministro de servicios e información a múltiples canales multimediales.

MARCO JURÍDICO DE LA INTEROPERABILIDAD EN CHILE

Desde hace varios años, Chile está enfocado en lograr un Estado más simple y eficiente, y una de las vías elegidas es el desarrollo del Gobierno Electrónico en el país, que tiene sus orígenes en el primer Comité interministerial de modernización de la gestión pública en 1998, y que hoy día está a cargo de un comité estable denominado "Estrategia para el desarrollo digital[4]", instalado en febrero de 2007.

En su primera fase incentivó la incorporación de Tecnologías de la Información y Comunicaciones (TICs) en los órganos del Estado, con el objetivo de mejorar la gestión interna, y también la interacción con los proveedores y los ciudadanos. Posteriormente, su foco estuvo en estandarizar e integrar su documentación electrónica, para mejorar los servicios de información ofrecidos a la sociedad, incrementar la eficiencia, eficacia, la transparencia del sector público y la participación ciudadana[5]

En efecto, hace 3 años, según la evaluación de la ONU el nivel de madurez del Gobierno Electrónico en Chile estaba en una etapa de "Presencia Interactiva"6[, siendo la estandarización e integración de la documentación electrónica uno de los principales problemas a abordar. Basado en este diagnóstico, en las experiencias internacionales y en las tecnologías disponibles, el Gobierno chileno tomó en el año 2004 la decisión de introducir XML (eXtensible Markup Language)[7] como la norma para representar y permitir el intercambio de su documentación electrónica.

En materia legislativa, directamente relacionada con la materia que nos aboca, aparece en el año 2002, la ley de Firma Electrónica[8], que regula los documentos electrónicos y sus efectos legales y la utilización en ellos de firma electrónica. En ella

[4] Estrategia digital es el responsable de diseñar y ejecutar una política pública que permita desarrollar acciones en pos de un uso más profundo e intensivo de las tecnologías de información y comunicaciones por parte de los ciudadanos, empresas y el propio Estado.
[5] Decreto N° 81, 2004, Ministerio Secretaria General de la Presidencia.
[6]De acuerdo al mismo ranking, pero del 2005, el gobierno electrónico chileno avanzó a la etapa de "Presencia Transaccional", esto es, donde el Estado ofrece transacciones completas y seguras tales como: obtención de visas y pasaportes, certificados de nacimiento y defunción, pago de multas y impuestos, etc. Ver en http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf
[7] Revisar al respecto, World Wide Web Consortium (W3C). Extensible Markup Language (XML) 1.0. (Fourth Edition). W3C Recommendation. Agosto, 2006. http://www.w3.org/TR/REC-xml/
[8] Ley 19.799

se reconoce que los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica (por tanto documentación electrónica), serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel. Por su parte, por el reglamento de la ley[9], del mismo año, se crea el Comité de Normas para el Documento Electrónico, cuya función principal refiere a asesorar al Presidente de la República con respecto a la fijación de normas técnicas que deberán seguir los órganos de la Administración del Estado para garantizar la compatibilidad de los distintos tipos de documentos electrónicos.

Otra regulación importante es la Ley de Procedimientos Administrativos[10], que esencialmente establece que los servicios públicos no pueden solicitar a un ciudadano que hace un trámite, ningún documento que otra dependencia debe tener, por ejemplo la cédula de identidad al solicitar la licencia de conducir. En los hechos, esto significa que los órganos gubernamentales deben poder intercambiar y/o validar la información entre ellos.

Ya a fines del año 2004, se dictó una norma sobre Eficiencia de Comunicaciones Electrónicas[11], que reguló este tipo de comunicación entre las dependencias gubernamentales y los ciudadanos.

Al mismo tiempo, y producto del trabajo del Comité de Normas para el Documento Electrónico, en diciembre del 2004, se dictó el Decreto 81, que contiene la norma técnica, aplicable a los órganos de la administración del Estado, para la interoperabilidad de los documentos electrónicos, adoptando el estándar XML. Esta norma representa para muchos, el gran paso dentro de los esfuerzos de la modernización gubernamental, pues varias iniciativas presentes en la Agenda Digital del Gobierno apuntaban en esa dirección y dependían de esta interoperabilidad. Así se puede observar en los considerandos de la norma expresamente como objetivos para el uso del documento electrónico por los órganos de la administración, desde el punto de vista político y administrativo: facilitar el acceso a la información gubernamental, aumentar la productividad y reducir costos, agilizar la comunicación entre los ciudadanos y las dependencias del Gobierno, y facilitar la interacción entre los organismos públicos; y desde un punto de vista técnico: fácil clasificación, almacenamiento y búsqueda de documentos electrónicos, interoperabilidad entre los

[9] Decreto 181. 2002. Ministerio de Economía.
[10] Ley N° 19.880 sobre Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado.
[11] Decreto 77. 2004. Ministerio Secretaria General de la Presidencia

documentos de organismos con diferentes plataformas de hardware, software y sistemas operativos, y fácil desarrollo de aplicaciones genéricas para el procesamiento de documentos.

Características del documento electrónico

Concordante con lo expuesto, en el Decreto 81 se establecen las características mínimas obligatorias de interoperatividad que deben cumplir los documentos electrónicos en su generación, envío, recepción, procesamiento y almacenamiento, tanto en los órganos de la Administración del Estado, como en las relaciones de la ciudadanía y el sector privado con dichos órganos, y las demás cuya aplicación se recomienda. En definitiva, obliga a las organizaciones públicas a adoptar documentación electrónica, y establece a XML como el formato estándar a ser usado para ello.

Debemos hacer presente sin embargo, que aunque XML surgió como el principal candidato por reunir los requisitos deseados, fueron consideradas también en el proceso otras propuestas, por ejemplo PDF. Finalmente, XML y su familia de tecnologías fueron escogidas debido a la flexibilidad para especificar formatos, por su escalabilidad, por el hecho de ser un estándar abierto de facto, su independencia de plataformas y aplicaciones, su soporte técnico y comercial, y su arquitectura compatible con las extensiones futuras del sistema de información global. En una perspectiva más técnica, las tecnologías de XML propuesta son XML v.1, XML Schema para los esquemas, XForms, XML Signatura para firmas y/o cifrados, UTF-8 y un servicio de traducción para UNICODE, XSL y XHTML para la visualización de documentos electrónicos y Servicios Web a modo de recomendación.

Características mínimas generales

La norma también establece que cada documento electrónico debe cumplir a lo menos con las siguientes características generales:

1. Tener flexibilidad y extensibilidad
2. Poseer un sistema de multiplataforma
3. Ser permanente en el tiempo
4. Ser interoperable

Se señala además, que en caso de desear tener una representación impresa de un documento electrónico con firma avanzada, deberá contener además mecanismos

para verificar la integridad y autenticidad de los mismos. Asimismo, cada documento debe contener los siguientes metadatos: los esquemas usados, los metadatos documentando el uso y significando de los esquemas usados, metadatos semánticos para facilitar la localización, metadatos para permitir seguir la vida del documento, y referencias a un diccionario de metadatos. Igualmente debe soportar firma y cifrado, permitir presentaciones visuales alternativas para diferentes medios y, tal como señaláramos, mecanismos para verificar la integridad y autenticidad de las visualizaciones de las versiones de los documentos firmados.

Seguridad de las comunicaciones electrónicas y documentos electrónicos

En esta materia, en Chile una norma técnica (Decreto 83 de 12 de enero de 2005) establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos, que se generen, intercambien, transporten y almacenen en o entre los diferentes organismos de la Administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos de los órganos de la Administración del Estado. La norma busca garantizar un estándar mínimo de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

Esta norma se cumplirá en dos etapas, de conformidad a dos niveles: un nivel básico y un nivel avanzado de seguridad para el documento electrónico.

En términos generales, la seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento: confidencialidad, integridad, factibilidad de autenticación, y disponibilidad. La norma señala las acciones a ejecutar por los organismos públicos de manera permanente para dichos atributos.

Nivel básico de seguridad

Este nivel tiene por objeto que se garanticen las condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben,

procesan y almacenan entre los órganos de la Administración del Estado; facilitar la adopción de requerimientos de seguridad más estrictos por parte de aquellos organismos y en aquellos tópicos que se estimen necesarios, y facilitar el Nivel avanzado de seguridad para el documento electrónico, en aquellos organismos cuyo desarrollo institucional lo requiera.

Al respecto la norma obliga la implementación de diversos tópicos, tales como el establecimiento de una política de seguridad en la organización, un encargado de la seguridad de los documentos electrónicos, clasificación de grado de protección de los documentos y su procedimiento de manipulación seguridad física, seguridad del personal, controles de acceso, etc.
De acuerdo con la norma este nivel debería implementarse a más tardar el año 2004.

Nivel avanzado de seguridad

Para este nivel, se exigen la adopción de la norma, ISO NCh-ISO 27002 declarada norma oficial de la república en septiembre de 2009, en reemplazo de la Norma NCh2777 de 2003. Este nivel de la norma debería haberse implementado a más tardar en el año 2009.

SOLUCIONES DE INTEROPERABILIDAD Y PROTECCIÓN DE DATOS

Enfrentados a los nuevos desafíos y necesidades de acceso a la información, junto al hecho del avance tecnológico que permite facilitar la trasparencia y el acceso, no podemos dejar de desconocer que en la práctica mucha de la documentación detentada (producida, intercambiada, almacenada, etc.) por el Estado contiene información personal de los ciudadanos. Es más, el Estado, como tal, en el ejercicio de sus funciones, trata por este hecho datos personales. Se hace necesario, en este contexto, el deber de los servicios de clasificar el grado de protección de los documentos y establecer los procedimientos de manipulación**,** en razón del contenido de la información que se almacena y se trata. A consecuencia de dicha clasificación, y al tratarse de datos de propiedad de terceras personas manipulados por el Estado, se hace más exigente la adopción de medidas de seguridad sobre los documentos que los contienen. La protección de los documentos, no se justifica en sí misma, sino en virtud de la protección de su contenido.

Al respecto, las normas internacionales de protección de datos clasifican los datos en función de su mayor o menor grado de sensibilidad, siendo los requisitos legales y de medidas de seguridad informáticas más estrictas en función de dicho grado.

De este modo, dentro de la información que los organismos públicos detentan es posible distinguir **datos públicos**, es decir aquellos que suelen ser conocidos por diversas personas tales como el nombre, apellido, sexo, edad generalmente disponibles en archivos y registros al alcance de todos; y **datos privados** que refieren a aspectos de la vida privada de la persona y que sólo deberían darse a conocer bajo el consentimiento de su titular o en circunstancias reguladas por la ley, pensemos por ejemplo en el historial médico de un paciente en un hospital público. La adopción de medidas en resguardo de la seguridad de los datos personales que almacena, obligación de confidencialidad y reserva se transforman en deberes del Estado, lo que se superpone a cualquier solicitud de acceso a la documentación que no sea hecha por el titular de los datos.

Situación en Chile

A modo de ejemplo, un proyecto país que muestra el desarrollo de diversos sistemas interoperando entre sí es el programa inaugurado en el mes de julio de 2009**, "Un Rut, un trámite[12]"**, el cual simplifica ciertos trámites para acceder a beneficios y servicios del Estado.

Con esto, 35 trámites que antes requerían de una serie de documentos y certificados, podrían realizarse en un paso, mediante una Plataforma Integrada de servicios del Estado. El objetivo de programas como éste es que "el ciudadano no tenga que recopilar antecedentes y documentos de distintas oficinas públicas a la hora de solicitar a un beneficio, realizar un trámite, o simplemente acceder a su información personal manejada por el Estado"[13]. Actualmente esta plataforma integra cinco servicios públicos el SII, el Registro Civil, Instituto de Previsión Social, Tesorería General de la República y el Ministerio de Vivienda y Urbanismo[14].

---

[12]Un rut, un trámite: Simplifican trámites para acceder a beneficios y servicios del Estado [http://www.estrategiadigital.gob.cl/node/413]

[13] Hugo Lavados Ex Ministro de Economía en EMOL [http://www.emol.com/noticias/tecnologia/detalle/detallenoticias.asp?idnoticia=368075]

[14] A modo de ejemplo, cuando una persona vaya a solicitar un subsidio habitacional o una pensión asistencial, ya no necesitará recopilar documentación como certificados de nacimiento cargas familiares y otra información que ya está en poder del Estado, puesto que los organismos podrían verificar en línea los datos que el solicitante declara.
http://www.desarrollodigital.cl/gobierno_electronico/index.php?accion=detalle&idAreaPublicacion=1&idContenido=175

La promesa es facilitar la trasparencia y acceso a la información, asegurando el pleno respeto a los derechos de los titulares de los datos personales contenidos en esa información. La protección de datos personales, como garantía de control sobre la información propia es un tema que no podemos obviar al implementar estos servicios. Toda solución de interoperabilidad de información pública que contenga datos personales, debe respetar los principios orientadores de la protección de datos.

El gobierno de Chile en este sentido, ha elaborado una Guía[15], que de manera detallada desarrolla cada uno de los requisitos técnicos y legales asociados a las distintas etapas que componen el sistema de gobierno electrónico y con ello la implementación de la interoperabilidad en los diversos sectores de la administración.
Uno de los pasos de esta guía, incorpora entre los diversos requisitos el ajuste a guías técnicas, entre las que se señala la Guía Modelo de Políticas de Privacidad[16] para la protección de los datos personales. Mantener adoptar y declarar una política de privacidad es obligatorio en el primer nivel de cumplimiento de la norma técnica para el desarrollo de sitios Web de servicios de los órganos de la administración del estado[17]. La inclusión de una política de privacidad, apunta a conferir certidumbre a la ciudadanía respecto del tratamiento de datos personales que se verificará en el sitio, así como los derechos de que se es titular y el modo en que puede ejercerlos, anticipando su conocimiento al uso mismo de los recursos disponible en línea[18].

Los contenidos de estas políticas de privacidad de los portales públicos que recogen y en definitiva hacen tratamiento de datos, no son otra cosa que el cumplimiento de la ley 19.628 sobre protección de la vida privada, que permiten o autorizan el tratamiento de datos por los entes públicos y la posibilidad de establecer procedimientos informatizados de transmisión de datos.

Estos pueden resumirse en:

a) Cuando los organismos del Estado tratan datos sólo deben hacerlo respecto a materias de su competencia, de esta manera no requieren consentimiento de su titular

[15] Consulta en [http://www.dipres.cl/572/articles-51683_egov_guia.pdf]
[16] Consulta en [http://www.estrategiadigital.gob.cl/files/guia_modelo_privacidad.pdf]
[17] DTO 100 de 12 de agosto 2006 SEGPRES [http://www.leychile.cl/Navegar?idNorma=252158]
[18] Guía Modelo de Políticas de Privacidad [http://www.estrategiadigital.gob.cl/files/guia_modelo_privacidad.pdf]

La ley chilena, señala que el tratamiento de datos personales por el Estado no obsta a la aplicación de la normativa general, esto es el **respeto de los principios orientadores de la protección de datos** plasmados en la Ley 19.628. Esta es por tanto nuestra base.

Respecto al consentimiento e información, el artículo 20 de la ley contiene una norma especial para entes públicos, que señala 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 (entiéndase el articulado de la ley 19.628) y en esas condiciones, no necesitará el consentimiento del titular.

Para el caso de los datos sensibles, definidos en la misma ley, no pueden ser objeto de tratamiento, salvo cuando la ley lo autorice, exista consentimiento del titular, o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. En tal caso, el Estado podrá efectuar operaciones de almacenamiento y registro. Al tratarse de una categoría especial de datos no puede comunicar estos datos a personas distintas de sus titulares y si lo hace en razón de un interés superior, debe existir información previa.

Si el órgano público trata datos en materias **fuera del ámbito de su competencia**, el titular de los datos debe autorizar dicho tratamiento y debe ser debidamente informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La ley señala que a persona que autoriza debe autorizar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito. Pese a esta afirmación de la ley las excepciones al consentimiento en el tratamiento de datos son tantas que finalmente se transforman en la regla general.

b) Cuando los organismos del Estado tratan datos tienen la obligación legal de registrar su base de datos en el registro civil[19].

Este registro ha sido reglamento a través del Decreto Nº 779 de agosto de 2000[20] del Ministerio de Justicia, el cumplimiento de sus disposiciones no obsta al cumplimiento de lo previsto en el Decreto Supremo N° 100 de 2006 (sobre sitios Web), del Ministerio Secretaría General de la Presidencia. El Registro de Bases de Datos es público y,

[19] Al respecto, en el mes de marzo de 2010 se cerró la consulta pública del Consejo para la transparencia que evaluaba el nivel de cumplimiento de esta obligación [http://www.consejotransparencia.cl/prontus_consejo/site/artic/20100506/pags/20100506130726.html]

[20] http://www.leychile.cl/Navegar?idNorma=177681

como tal, el Servicio de Registro Civil e Identificación lo ha hecho accesible en línea en su respectivo sitio Web. De ahí que el Decreto precise que, tratándose de los servicios que hacen tratamiento de datos desde sus sitios Web, alude al mencionado registro y aún se establezca un vínculo hacia aquella parte del mismo que le contempla[21].

c) Las transferencias electrónicas de datos personales, entre organismos públicos, deben cautelar los derechos de los titulares y guardar concordancia con las tareas y finalidades de los organismos participantes.

Partiremos señalando que para el caso de transferencias electrónicas, que es lo que nos interesa en materia de interoperabilidad, la ley chilena no prevé uno de los dos roles vinculados técnicamente a la actividad de tratamiento de datos[22]: el encargado del tratamiento. Este último, no se encuentra previsto en la ley 19.628 pero si en un proyecto de ley que se encuentra en discusión en el Congreso. El encargado del tratamiento, señala el proyecto, es la persona, física o jurídica o la autoridad pública que sólo o conjuntamente con otros trate datos personales por cuenta del responsable del tratamiento. Este como tal tiene responsabilidades en la actividad de transferencia.
Las plataformas de servicios integradas, como “medios de traspaso" de información entre los organismos públicos, no concentran en sí las bases de datos siendo por tanto por definición, encargados del tratamiento de datos[23], transformándose en facilitadotes de la información entregada. Al no existir esta figura en la legislación se hace posible que estos últimos eludan el cumplimiento de sus obligaciones, y que no tengan responsabilidad concreta o efectiva asociada a la actividad.

La ley chilena si contempla al “responsable del registro o banco de datos personales”, como a quien le competen las decisiones relacionadas con el tratamiento de datos de carácter personal. El responsable, **podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes**.
Ello implica que el procedimiento automatizado puede establecerse siempre y cuando dicha automatización se haga en el desarrollo de sus funciones o competencias como ente público y entre los entes públicos y con el cuidado de los derechos de los titulares

[21] Guía Modelo de Políticas de Privacidad [http://www.estrategiadigital.gob.cl/files/guia_modelo_privacidad.pdf]

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

frente al tratamiento automatizado, es decir, acceso e información, posibilidad de modificación, bloqueo, eliminación de datos caducos o inexactos, etc.
La ley señala que el receptor de los datos solo puede utilizarlos los fines que motivaron la transmisión.

El responsable del tratamiento tiene la obligación de dejar constancia de:

a) La individualización del requirente;
b) El motivo y el propósito del requerimiento, y
c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento de transferencia electrónica de datos será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga, es decir del servicio solicitante.

CONCLUSIONES

A modo de dejar abierto este tema al debate y reflexión, creemos que no todo está resuelto en cuanto a la interoperabilidad frente a la protección de datos personales.

En mayor medida se enfrentan problemas tales como las responsabilidades difusas al no existir sanciones efectivas y directas, ni un órgano de control por sobre la actividad de aquellos que tratan datos en Chile. El ajuste a la legalidad forma parte de la buena voluntad de los organismos públicos que tratan datos, puesto que el derecho a la protección de datos y a la autodeterminación informativa no se encuentra afianzado en los ciudadanos.

Por otra parte, pese a que existen normas técnicas que regulan el establecimiento de estándares de almacenamiento, no existe uniforme incorporación de las tecnologías de la información a los procesos, generando en definitiva asimetrías en el ejercicio de los derechos de acceso a la información por un lado y habeas data por otro.

En tercer término, no está claramente delimitado la matriz de competencias de los organismos del Estado para tratar datos personales: Es necesario delimitar donde está la raíz que autoriza a cualquier organismo público para tratar datos personales, generar y mantener bases de datos ¿dónde deben estar explicitadas estas competencias? El Estado requiere competencia para eximirse de requerir datos a los administrados, datos que ya posee, los datos deben ser pertinentes al trámite realizado, debe poseer las competencias para haber capturado y almacenado, en definitiva para hacer tratamiento de datos.

Finalmente un tema relevante es la forma de garantizar niveles de seguridad adecuados tanto en el acceso a la información como en las transacciones cuando éstas involucren tratamiento de datos de acuerdo a su categorización a la luz de lo dispuesto en la ley 19.628 y en las normas técnicas que exigen implementar cierto nivel de seguridad. Para ello es necesaria la inversión de recursos públicos y sobre todo de ciudadanos concientes del valor de sus datos, que demanden la existencia de un estándar real de seguridad y protección.