

Consideraciones y recomendaciones en materia de tratamiento de datos personales por organismos públicos

Rodrigo Gutiérrez

• Este documento fue presentado en el seminario técnico “Protección de datos personales”, organizado por Expansiva y la Facultad de Derecho de la Universidad de Chile, realizado el 1 de agosto de 2008.

Introducción

El desarrollo de la sociedad de la información y el conocimiento ha conllevado el tratamiento de datos personales para múltiples usos y diversas finalidades. El desarrollo del mercado y las necesidades de las empresas de ser más competitivas han motivado a éstas a conocer mejor a sus clientes, y para ello han destinado importantes recursos a la conformación de registros con los datos de millones de personas. Así, en los diversos sectores de la economía, y en particular en la industria de servicios, el uso de registros y bases de datos es cada vez más frecuente. El sector público no ha estado ajeno a este fenómeno y ha elaborado diversos registros con datos personales para cumplir más eficientemente con la implementación de políticas públicas y la entrega de determinados beneficios sociales.

El sector público no ha estado ajeno a este fenómeno y ha elaborado diversos registros con datos personales para cumplir más eficientemente con la implementación de políticas públicas y la entrega de determinados beneficios sociales.

Sin embargo, es necesario reconocer que el tratamiento de datos personales es un tema complejo y con múltiples aristas, por cuanto su uso indebido puede significar perjuicios en contra de los titulares de dichos datos. Es por ello que en buena parte de los países este tema se encuentra regulado. Chile no es la excepción, en virtud de la ley 19.628, sobre tratamiento de datos personales y protección de la vida privada.

Los gobiernos requieren para la implementación eficaz y eficiente de sus políticas públicas conocer con precisión a los destinatarios de las mismas. La entrega focalizada de determinados beneficios sociales se hará de mejor manera si es posible conocer con mayor exactitud a los grupos de la población que pretende alcanzar el objetivo de la política pública. Es por ello que los organismos públicos, inspirados en criterios de eficacia y eficiencia, y con apoyo de los medios tecnológicos disponibles, han conformado registros o bases de datos personales de diversos grupos de la población, en función de necesidades que emanan, a su vez, de distintos objetivos de política pública.

Habiendo situado el tratamiento de datos personales¹ como una activi-

(1) En Chile, la letra f) del artículo 2 de la 19.628 señala que los datos personales son aquellos “relativos a cualquier información concerniente a personas naturales, identificadas o identificables”. Asimismo, la letra o) del mismo artículo señala que se entenderá por tratamiento a “cualquier operación o complejo de operaciones o

dad de naturaleza instrumental al servicio de la mejor implementación de las políticas públicas, este artículo pretende aportar con una sistematización de las principales problemáticas concretas a las que se puede ver expuesto un directivo público en el ejercicio de sus funciones, a la luz de la legislación actualmente vigente en Chile sobre datos personales.

En tal sentido, y sin afán de ser exhaustivo, en este artículo se realiza una breve presentación y análisis de algunos de los principales problemas a los cuales pudiera verse enfrentado un directivo público, efectuando diversas consideraciones y proponiendo recomendaciones que podrían ser de utilidad. En consecuencia, este documento se inscribe en el ámbito de la gestión pública, y como tal está pensado para directivos públicos y funcionarios responsables de diseñar, implementar y gestionar políticas públicas.

Finalmente, cabe precisar que no se pretende realizar una crítica de la legislación vigente², lo cual podría ser tema de otro estudio, sino más bien tratar de abordar las diversas problemáticas o “restricciones” que la norma actual impone a la gestión de los directivos públicos. En tal sentido, este trabajo se inspira en criterios de realidad y oportunidad, identificando y discutiendo esas problemáticas desde la perspectiva de un directivo público. El impacto en la gestión pública de futuros cambios normativos en la materia podrá ser motivo de nuevos estudios.

El problema de la competencia legal

El directivo público debe tener presente que el tratamiento de datos personales por parte de organismos públicos no es una actividad que pueda

(...) es necesario que el organismo público enmarque su accionar dentro de su competencia y de las normas existentes en materia de protección de datos personales.

llevarse a cabo en forma descontextualizada de las restricciones que impone la ley.

En efecto, los organismos públicos, en la medida en que conformen bases de datos personales, siempre deben velar por que se cautelen los derechos de los titulares de los datos

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”.

(2) Las críticas a la legislación vigente son bastante conocidas. Éstas dicen relación con mecanismos de reclamación poco eficientes, sanciones de difícil aplicación y ausencia de una autoridad central de control.

y por que la transmisión de los mismos se ajuste a las normas legales. En dicho espíritu, independientemente de las condiciones según las cuales se genere el tratamiento y sin importar cuál sea la naturaleza de éste, es necesario que el organismo público enmarque su accionar dentro de su competencia y de las normas existentes en materia de protección de datos personales.

El artículo 20 de la ley 19.628 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. En esas condiciones, no necesitará el consentimiento del titular”. Éste es el precepto fundamental y el pilar sobre el cual se sustenta toda la discusión en materia de tratamiento de datos personales por parte de organismos públicos.

En función de lo establecido en ese artículo, cualquier organismo público podrá efectuar todo tratamiento de datos personales sin autorización del titular dentro de la órbita de su competencia, para lo cual no se requiere que exista texto expreso 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.

Precisamente, lo anterior no significa que un directivo público deba suponer que un organismo público está autorizado a realizar cualquier tipo de tratamiento. Por el contrario, requiere tener clara conciencia de que existen principios que inspiran el estatuto de protección de datos personales y preocuparse de que se respeten debidamente. Éstos son: a) principio de legalidad, en la medida en que el tratamiento se enmarca dentro de la órbita de competencia de la institución; b) principio de finalidad, tomando en consideración que se debe velar por que el tratamiento efectuado se circunscriba al fin por el cual fue capturado el dato; y c) principio de responsabilidad, el cual supone que se debe asumir el rol que le corresponde como responsable del registro o banco de datos personales.

Teniendo presentes las consideraciones señaladas, el directivo público estará preparado para enfrentar diversos cuestionamientos, tales como “la institución no tiene las facultades para efectuar el tratamiento de dichos datos”, o bien, “¿es necesario tener texto expreso en nuestra ley orgánica (del organismo respectivo) que autorice el tratamiento de los datos?”, o, alternativamente, “es posible efectuar el tratamiento de estos datos personales en virtud de los principios generales aplicables a los organismos públicos (velar por el bien común)”.

La recomendación para el directivo público, entonces, es que verifique si el tratamiento de determinados datos personales se ajusta o no al ámbito de las competencias del organismo respectivo, lo cual podrá requerir, eventualmente, que deba interpretarse el rango de acción de sus atribuciones y funciones. Respecto de esta tarea, el directivo público debe tener presente que la asesoría jurídica que reciba puede tener sesgos. En un extremo estarán quienes hagan una interpretación extensiva de la norma, sugiriendo que las facultades que emanan del estatuto jurídico del organismo son lo suficien-

Se trata de lograr que el tratamiento de los datos cumpla con su rol instrumental al servicio de la política pública, pero con pleno respeto de los derechos de los titulares de los datos.

temente amplias como para permitir el tratamiento de los datos. En el otro extremo, en cambio, estarán los que tengan posiciones garantistas y visualicen diversos impedimentos para que el organismo pueda efectuar el tratamiento de datos sin el consenti-

miento del titular. Así, el directivo deberá encontrar el adecuado equilibrio entre estos intereses en juego. Se trata de lograr que el tratamiento de los datos cumpla con su rol instrumental al servicio de la política pública, pero con pleno respeto de los derechos de los titulares de los datos.

Como fuere, desde una perspectiva jurídica, la actuación del organismo público deberá darse con apego a la legalidad, por lo que la tarea de buscar una correcta interpretación de la ley que justifique la conformación de la base de datos personales es, sin lugar a dudas, un paso fundamental para avanzar con pilares sólidos en la implementación material de la política pública para la cual dicha base de datos personales servirá instrumentalmente.

Por último, es recomendable que el estudio de factibilidad jurídica que se lleve a cabo sea debidamente documentado para efectos de tener plena certeza de la legalidad de la actuación del organismo público, ya sea por razones de transparencia o para responder requerimientos de terceros o de los organismos de control.

El problema de la decisión de la estrategia tecnológica de implementación

Llegado el momento de implementar la base de datos personales, el directivo público probablemente se verá enfrentado a la decisión respecto de la estrategia tecnológica a seguir para su puesta en operación.

En efecto, a menudo en los organismos públicos, así como en cualquier

organización, se deberá resolver si la modalidad que se adoptará será *in-housing* u *outsourcing*. En el primer caso, se deberá adquirir los componentes de hardware y software necesarios para la operación, los que deberán ser complementados con las correspondientes capacidades de administración y soporte internos. En el segundo caso, el énfasis estará puesto en los requisitos de niveles de servicio y seguridad que deberán exigirse a los potenciales proveedores.

Desde una perspectiva jurídica, cualquiera sea la opción a tomar, el directivo debe tener siempre presente que el organismo público será el responsable a todo evento de los registros que almacenen datos personales, por lo que deberá adoptar todas las precauciones y resguardos que sean necesarios, con independencia de las responsabilidades que emanen o surjan por medios contractuales.

En este tipo de situaciones, más allá del análisis estratégico que realice el directivo público y las diversas consideraciones técnicas que pudieran tenerse en cuenta, ellas no lo eximirán de enfrentar cuestionamientos tales como “no existen en la institución los recursos humanos y técnicos para gestionar eficientemente y en forma segura los datos”, o, alternativamente, “no es recomendable que la administración de los datos quede encargada a terceros ajenos a la institución”, o “no debemos permitir por ningún motivo que los datos salgan físicamente de la institución”.

No existe una “receta” aplicable para enfrentar esta decisión. La recomendación es que se utilicen criterios técnicos y objetivos, debidamente ponderados con criterios estratégicos aplicables al manejo de información sensible. Corresponderá evaluar cada situación en función del análisis que se haga tanto de variables internas de la institución como de variables de su entorno.

Enfrentado al análisis, la opción del *outsourcing* es la que, según las preferencias de muchos directivos y asesores, revestiría un mayor riesgo, al menos en apariencia. Sin embargo, es probable que muchas veces dicha preferencia responda más bien a criterios subjetivos que objetivos, por cuanto el hecho de que los datos se guarden *in-housing* no significa necesariamente que se encuentren más seguros. En ambos casos debiera respetarse la política de seguridad informática que posea la entidad,³ con independencia de la

(3) Para todos los efectos, esta política debiera ceñirse a las recomendaciones u obligaciones establecidas en el decreto 83, norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

modalidad de implementación. Lo que se pretende es que el almacenamiento de los datos sea seguro, la recuperación sea eficiente y la disponibilidad sea permanente.

Si finalmente el directivo público optara por el *outsourcing*, y dado que ello no implicará en ningún caso que el organismo público traslade o delegue la responsabilidad al proveedor tecnológico adjudicatario del contrato, es recomendable que el organismo público utilice todas las herramientas contractuales disponibles para reducir el riesgo de vulneración de los datos personales. Lo anterior supone el establecimiento de cláusulas robustas que, por una parte, procuren que el proveedor reduzca el riesgo de vulneración de las medidas de seguridad que hayan sido adoptadas para proteger los datos, ello mediante el uso de los incentivos adecuados (como multas o premios que sean de fácil determinación mediante criterios objetivos), y, por otra, permitan perseguir de forma eficaz y eficiente las responsabilidades por incumplimiento de las obligaciones por parte del proveedor (que sea posible hacer efectivo el cobro de indemnizaciones).

Se trata, en definitiva, de evitar situaciones en que terceros no autorizados accedan a los datos, así como el eventual uso indebido de los mismos que este hecho implicaría.

El problema de la captura u obtención de los datos

Una vez resuelto el problema de disponer de los medios tecnológicos para el almacenamiento y tratamiento de los datos, surge la dificultad elemental de cómo obtenerlos. Evidentemente, las posibilidades son diversas y dependerá de las condiciones particulares de cada caso.

En efecto, una opción es que los datos se obtengan directamente de los titulares, lo cual eventualmente podría ser muy costoso. Peor aun, pudiese ser que esta opción no sea viable, por cuanto sea necesario primero tener los datos para poder ubicar a los titulares de los mismos.

Otras alternativas son acceder a fuentes de acceso público, asumiendo los consiguientes riesgos asociados a problemas de calidad de los datos; o bien hacer uso de bases de datos comerciales, considerando los costos respectivos.

Ligado al problema de obtener los datos está el de verificar la calidad de los mismos y, junto con ello, la necesidad de generar instancias automatizadas de validación para cumplir con este objetivo. Al respecto, es de conocimiento generalizado en el sector público que el Servicio de Registro

Civil e Identificación ofrece servicios que permiten efectuar consultas y validaciones de datos personales, previo establecimiento de un convenio que especifica las condiciones de la transferencia de los datos y los costos del servicio en que deberá incurrir el organismo público. Sin embargo, diversas razones, entre otras el costo del servicio, han llevado a muchos organismos a explorar instancias alternativas para validar datos, entre ellas, otros organismos públicos.

La necesidad de los organismos públicos de contar con datos y validarlos con fuentes confiables y autorizadas ha sido el fundamento para constituir la Plataforma de Servicios Integrada del Estado, instancia que serviría para satisfacer estas necesidades, reduciendo buena parte de los costos de transacción originados en los requerimientos de coordinación entre organismos públicos para efectos de implementar materialmente los medios tecnológicos para la transferencia de datos. Sin embargo, como en el caso anterior, por diversas razones, esta iniciativa se presenta con cierto retraso en relación con las necesidades que surgen desde los distintos servicios públicos, en la medida en que éstos avanzan en la implementación de sus respectivos proyectos.

La necesidad de los organismos públicos de contar con datos y validarlos con fuentes confiables y autorizadas ha sido el fundamento para constituir la Plataforma de Servicios Integrada del Estado.

De este modo, se configura un escenario en que el directivo público, en ausencia de instancias centrales de coordinación y cooperación, deberá decidir por recurrir a otras alternativas, como convenios de colaboración con otras entidades, contribuyendo así al fortalecimiento de las mismas y, consecuentemente, debilitando a aquellas que debiesen ser las más idóneas para cumplir con esos fines.

En estos casos, el directivo público se enfrenta a interrogantes tales como “¿validaré mis datos contra el Registro Civil o contra el (determinado organismo) que también los posee y es son igualmente confiables?”, o “¿dispondremos como institución de los recursos para pagar los servicios del Registro Civil?”, y, si estuvieran los recursos, “¿estamos dispuestos a desembolsarlos?”. Por otro lado, es probable que el directivo deba enfrentar requerimientos para establecer convenios de colaboración que permitan el intercambio recíproco de datos con otros organismos. En estos casos, las interrogantes podrían ser: “¿será beneficioso para nuestra institución suscribir

estos convenios?” o “¿es legal el intercambio de datos que se nos propone (el problema de la competencia legal)?”.

Por cierto, siempre está presente la posibilidad de prescindir de la implementación de mecanismos de validación de los datos, con el consiguiente riesgo de problemas de calidad de los mismos.

Finalmente, la recomendación que cabe realizar al directivo público en este ámbito es que decida con criterios técnicos y estratégicos, ponderando los costos y beneficios de las distintas alternativas, teniendo presente que lo que se pretende es contar con datos válidos y confiables a costos razonables.

El problema del “apetito” posterior por los datos

Una vez implementada la base de datos personales y estando en condición de servir a la política pública que la originó, surge en ocasiones otra problemática que el directivo público debe resolver. Ésta dice relación con nuevos usos que se pretende dar a los datos, ya sea por parte de la propia entidad o por un tercero, que puede ser otro organismo público o bien un privado.

Ya se ha señalado que frente a estas situaciones se debe tener presente que el organismo público es responsable de los datos, y que cualquier acción en el sentido de dar curso a las pretensiones antes referidas debe hacerse de igual modo con apego a la legalidad y al fin por el cual el dato fue capturado. Al respecto, el directivo público debe saber que, para el caso de los organismos públicos, la ley 19.628 ha permitido el tratamiento de datos personales sin el consentimiento previo e informado por parte de los titulares de los mismos, lo cual conlleva el deber ético de ser especialmente cauteloso en su resguardo.⁴

En este escenario, es posible que el directivo se enfrente a cuestionamientos como éste: “¿es posible que compartamos nuestras bases de datos con centros académicos para que ellos puedan realizar estudios?”, o bien a afirmaciones como la siguiente: “debemos implementar un mecanismo de transferencia de nuestros datos o un mecanismo de consulta para que otras instituciones puedan acceder a ellos para (sus respectivos fines)”.

Es necesario determinar el alcance que tendría la facultad legal del

(4) Es fundamental que los organismos públicos no hagan mal uso de la facultad concedida en el artículo 20 de la ley 19.628, aun cuando los fines que se persigan sean visualizados como positivos. Sin embargo, algunos organismos públicos, sustentándose en criterios generales de bien común, terminan vendiendo la información perteneciente a sus bases de datos personales, desviándola de la finalidad por la cual fue capturada.

organismo, en tanto pueda dar otros usos a dichos datos o bien transferirlos a terceros.

En tales situaciones, las alternativas que se le pueden presentar al directivo son variadas. Una posibilidad es negarse a transferir los datos, si la finalidad para la cual éstos se solicitan no es compatible con aquella que originó su captura. Otra opción es proporcionarlos tomando los resguardos correspondientes, tales como, por ejemplo, velar por que el tercero que los recibe enmarque su tratamiento dentro de sus competencias, en caso de que también fuera un organismo público, o bien que éste manifieste expresamente el uso que le dará a los mismos en caso de que se tratara de un privado. También puede darse como alternativa que la transferencia de los datos sea parcial, evitando la entrega de aquellos que permitan la identificación de los titulares, permitiendo, en consecuencia, sólo el tratamiento estadístico de la información.

Cualquiera sea el caso, es recomendable que el directivo cuide que la transferencia de datos se realice en el contexto de un acuerdo debidamente documentado, o protocolo, que señale las obligaciones que las partes adquieren en función del mismo, y en el cual se incluyan cláusulas cuyo sentido sea velar por que nunca se vulneren los derechos de los titulares de los datos.

El problema indeseable: el acceso indebido a los datos por parte de terceros

No obstante se hayan tomado las medidas necesarias para resguardar los datos, y con independencia de la estrategia tecnológica de implementación que se haya decidido seguir, las bases de datos no están exentas de la acción de terceros, quienes con distintas motivaciones (de buena o mala fe) pueden vulnerar los mecanismos de seguridad que se hayan dispuesto para proteger los datos.

En efecto, si se hace de público conocimiento una situación de acceso no autorizado a los datos, se haya realizado o no uso indebido de los mismos, este hecho configurará de forma casi inevitable un material atractivo para las pautas informativas de los medios de comunicación, lo cual conllevará una evaluación negativa por parte de la opinión pública.

La pérdida de confianza de los ciudadanos traerá consigo el descrédito de la función pública y, eventualmente, afectará la percepción de valor público pretendida por la política pública a la cual los datos, ahora vulnerados, servían instrumentalmente.

En este caso, el directivo público se enfrentará a cuestionamientos tales como “¿por qué no se tomaron las precauciones necesarias para resguardar los datos de las personas?”, o “¿cuáles son los riesgos que deberán enfrentar las personas titulares de los datos como consecuencia de este evento?”, o bien a respuestas con carácter reivindicativo por parte de los afectados, como, por ejemplo, “se tomarán todas las acciones legales que estén a nuestro alcance en contra del organismo público responsable”.

Con el propósito de que el directivo pueda estar mejor preparado frente a una situación como la descrita, es recomendable que tenga claridad de la importancia de adoptar medidas tanto preventivas como correctivas.

Desde un punto de vista preventivo, el directivo público deberá adoptar decisiones orientadas a minimizar el riesgo, tanto mediante control técnico (seguridad informática) como mediante control jurídico (cláusulas robustas en los contratos).

Desde una perspectiva correctiva, en cambio, será fundamental que el directivo lleve a cabo acciones tendientes a mitigar los eventuales perjuicios. En efecto, deberá hacer exigibles las responsabilidades –administrativas, civiles e incluso penales–, ya sea de funcionarios públicos o de terceros que hubieren participado, reclamando las indemnizaciones de los daños morales o patrimoniales que se hubiesen ocasionado. Asimismo, deberá también hacer efectivas aquellas cláusulas de los contratos que, habiendo previsto situaciones de este tipo, hubieran determinado multas de beneficio fiscal.

Finalmente, el directivo deberá en lo posible revertir la pérdida de confianza por parte de los usuarios, reposicionando la imagen de la función pública mediante las acciones comunicacionales que sean recomendables según sea el caso.

Conclusiones

Dadas la ascendente demanda por una mayor eficacia y eficiencia en la aplicación de las políticas públicas y la necesidad de focalización de las mismas sobre determinados grupos objetivos de la población, el tratamiento de datos personales por parte de los organismos públicos es una necesidad creciente y una realidad cada vez más habitual.

En ese contexto, es importante que en los organismos públicos exista claridad de la relevancia que conlleva esta actividad, por cuanto existe regulación especializada que los obliga a actuar en consistencia con los princi-

prios de legalidad, finalidad y responsabilidad.

Es rol de los directivos públicos asegurar que esta claridad sea transversal a los distintos estamentos de los organismos que dirigen. No es suficiente que la evaluación y verificación del cumplimiento de los principios antes señalados sea patrimonio de las áreas jurídicas o fiscalías de las instituciones. Debe necesariamente alcanzar a las áreas encargadas de la implementación de las políticas y de aquéllas responsables de proporcionar y administrar los medios tecnológicos que permitan la implementación y uso de las bases de datos personales.

Es fundamental que los directivos públicos actúen con rigurosidad cuando se vean enfrentados a decisiones que involucren el tratamiento de datos personales, por cuanto se trata de resguardar un bien tan preciado como la intimidad de las personas.

Finalmente, el desafío para los directivos públicos consiste en conciliar equilibradamente la necesidad de tratar datos personales con la obligación de proteger los derechos de sus titulares, utilizando criterios de eficiencia y legalidad.

Autor



Rodrigo Gutiérrez Castro

Ingeniero civil industrial por la Universidad Técnica Federico Santa María y magíster en gerencia y políticas públicas por la Universidad Adolfo Ibáñez. Jefe de Planificación y Desarrollo de la Superintendencia de Seguridad Social.

© 2009 Expansiva UDP

La serie **en foco** recoge las investigaciones del Instituto de Políticas Públicas Expansiva UDP las que tienen por objeto promover un debate amplio y riguroso sobre los temas de la sociedad actual, con el fin de hacer propuestas que contribuyan a mejorar las políticas públicas del país.

Este documento forma parte de un proyecto del Instituto en conjunto con la Escuela de Derecho de la Universidad de Chile, el que tuvo como objetivo analizar el marco legal necesario para el funcionamiento de los actuales sistemas de tratamiento de datos personales, además de trazar ciertas directrices sobre las soluciones urgentes que el país tiene que adoptar en materia de derechos fundamentales.

El documento forma parte del libro “Chile y la Protección de Datos Personales: ¿Están en Crisis nuestros derechos fundamentales?” publicado por la Serie de Políticas Públicas de Ediciones Universidad Diego Portales.

Se autoriza su reproducción total o parcial siempre que su fuente sea citada.