Los desafíos para instituciones públicas con la entrada en vigor de la nueva Ley de Protección de Datos Personales

Verónica Achá Álvarez

Master of Science in Public Policy and Management por la Carnegie Mellon University. Jefa de División de Información Social, en el Ministerio de Desarrollo Social y Familia.

@veronicaacha
linkedin.com/in/vacha/

Resumen / Durante años, la protección de los datos personales en el sector público ha estado bajo la supervisión del Consejo para la Transparencia, que instaló criterios y estándares relevantes. Ahora, los nuevos requisitos que entrarán en vigor en diciembre de 2026 plantean desafíos significativos, especialmente considerando que la implementación de la Ley de Transformación Digital también se realizó de forma gradual, segmentando a los órganos del Estado y otorgando plazos diferenciados según sus capacidades.

En este contexto, las instituciones que ya han avanzado en proyectos de gobernanza de datos estarán mejor preparadas para cumplir con las nuevas obligaciones, a diferencia de aquellas que aún no han ordenado sus prácticas de tratamiento de datos. Contar con normativas internas facilita la transición, pero para quienes no han iniciado este camino el desafío será complejo.

Advertencia necesaria

Inicio este artículo declarando que soy hija de Beauchef. Mi formación de base es la ingeniería civil en computación y, si bien he trabajado los últimos 13 años en el Ministerio de Desarrollo Social y Familia, administrando tal vez uno de los registros de datos personales y sensibles más completos del sector público sobre la población que vive en Chile, mi acercamiento ha sido desde la ingeniería. Sin embargo, escribo desde los años de experiencia que tengo trabajando con leyes y su aplicación al tratamiento de los datos personales, camino que he recorrido en un trabajo colaborativo con importantes profesionales del mundo jurídico, tanto en el Ministerio como fuera de él, así como desde el empeño y desafío personal de formarme en la materia, para realizar un trabajo profesional.

No partimos de cero

Por años ha existido en los círculos dedicados al trabajo con datos personales, la convicción de la necesidad de una actualización urgente a la normativa vigente en el país. Y si bien en 2018 se incorporó a la Constitución el derecho a la protección de los datos personales como parte del catálogo de derechos fundamentales [1], todavía era insuficiente frente a una ley anclada a la realidad de 1999, en cuanto a la protección a la vida privada, sin la posibilidad real de ejercer los derechos de las personas frente a abusos sobre ellos.

Sin embargo, desde el punto de vista de la sociedad, las instituciones públicas no estaban en igual nivel de libertad para sus acciones respecto del tratamiento de estos datos, porque como regla general, el derecho administrativo regula la organización y funcionamiento de la administración pública, estableciendo normas para su actuación en el día a día, y principios sobre sus actuaciones, ponen cota y control a ellas.

Sin ir más lejos, como ejemplos, por principio de legalidad, la actuación de los órganos públicos sólo puede realizarse conforme a la ley, y de proporcionalidad, la acción estatal debe ser proporcional a los fines que busca alcanzar.

Así, la ley N° 19.628 vigente [2], contiene un apartado breve donde se fijan parámetros para el tratamiento de datos por parte de los organismos públicos.

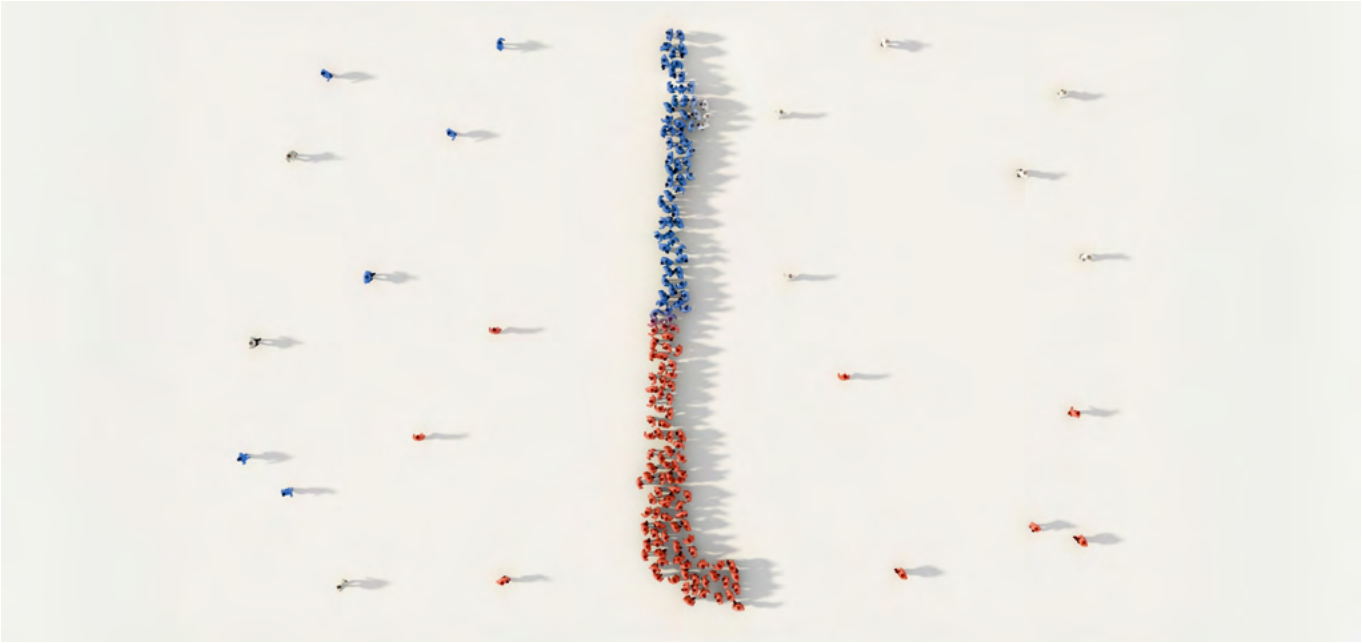
Como segundo elemento de control, no existente para el sector privado, en la ley N° 20.285 se estableció que el Consejo para la Transparencia (CPLT) tendría entre sus funciones y atribuciones "[v]elar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" [3]. De tal forma, el CPLT ha cumplido por años un rol semejante al que se espera cumpla la Agencia de Protección de Datos, definiendo lineamientos y estándares, sólo que ahora para todos los sujetos obligados y ya no sólo para las instituciones públicas.

Por tanto, si bien la entrada en vigencia de un nuevo y más alto estándar de control sobre el tratamiento de los datos personales no resulta indiferente, no parte desde cero en cuanto a la necesidad de contar con mecanismos de gestión y control. En lo que sí somos todos los trabajadores de los datos más conscientes del cambio, es que la creación de una Agencia de Protección de Datos, con potestad fiscalizadora para hacer cumplir las disposiciones de la ley, nos lleva a un estándar que hasta ahora no habíamos conocido.

Pero qué tan preparados estamos

Tal vez una de las primeras distinciones que sugiero tener, para entender el impacto de la entrada en vigor de la ley sobre protección de los datos personales, esté dada por la gradualidad establecida para la implementación de la ley de Transformación Digital [4]. En ese caso, se estableció una hoja de ruta —que en los hechos fue ajustándose en el tiempo por el peso de la realidad— dividiendo a los Órganos de la Administración del Estado en tres grupos [5]:

a. *Grupo A.* Conformado por los ministerios; los servicios públicos creados para el cumplimiento de la función administrativa, que no se encuentren en los grupos B y C; la Contraloría General de la República; las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública; y las delegaciones presidenciales regionales y provinciales.
b. *Grupo B.* Compuesto por los gobiernos regionales; y un primer conjunto de municipios.
c. *Grupo C.* Integrado por los municipios restantes, no incluidos en el grupo B.



El Consejo para la Transparencia ha cumplido por años un rol semejante al que se espera [ahora] cumpla la Agencia de Protección de Datos.

Esta segmentación y distribución temporal para su implementación tomó en consideración las importantes diferencias organizacionales y de capacidades existentes en el Estado, estableciendo los plazos más cortos y las obligaciones más exigentes para el primer grupo. Como tal, resulta una buena aproximación para avizorar el desafío que significa la implementación de los cambios legales respecto del tratamiento de los datos personales.

Aunque debiera resultar evidente, el tratamiento de datos personales es algo que ocurre en todas las instituciones del Estado. En el más simple y general de los casos, a lo menos las instituciones deben administrar la información de las y los funcionarios que trabajan en ella, en todas las calidades contractuales, con todos los datos de su trayectoria de trabajo y los procesos diarios, como la marca de la asistencia, los mensuales, como el pago de las remuneraciones, y los anuales, como las evaluaciones de desempeño, entre otras. Así mismo, les corresponde administrar los datos de las personas que postulan para acceder a cargos, junto a toda la documentación personal que incorporan en los procesos. Por tanto, si debemos definir, por ejemplo, a quiénes capacitar sobre las nuevas obligaciones, esto debe ocurrir a todo lo largo y ancho de toda la institución, en todos los órganos del Estado.

En cuanto a las instituciones que tienen responsabilidad sobre bancos de datos personales, ellas traen consigo las definiciones y mandatos que el CPLT fue entregando a lo largo de los años, respecto de cómo enfrentar requerimientos a la luz de peticiones por transparencia activa. Y en esa línea, los criterios también fueron ajustándose y cambiando con el tiempo. Ese aprendizaje resulta importante a la hora de la implementación de un estándar más exigente, que conlleva una entidad fiscalizadora y capacidad de persecución más concreta que la disponible hasta ahora.

Otro elemento que permite estimar el nivel de preparación de los servicios públicos frente a las obligaciones de la ley de protección de datos personales es la autoevaluación utilizando el marco de referencia de gestión de datos para los órganos de la Administración del Estado, que forma parte del Sistema de Transformación Digital administrado por la Secretaría de Gobierno Digital. Este instrumento, desarrollado específicamente para el sector público chileno, se basa en el modelo DAMA —un marco global de buenas prácticas para la gestión de datos elaborado por la Data Management Association— al que se incorporaron elementos relevantes para la realidad nacional. Define las áreas de práctica básicas que se espera que todas las instituciones alcancen en un plazo de tres años, entre 2026 y 2028.

Con su aplicación, cada servicio público cuenta con una autoevaluación de este modelo simplificado de gobierno de

datos que le permite identificar brechas para luego elaborar un plan de trabajo trianual, comprometido desde su máxima autoridad, para avanzar en aquellas prácticas que sean especialmente relevantes para su institución y en las que existan brechas por cubrir. Y, aunque este instrumento funciona sólo como un *proxy* para lo que será una gestión adecuada de datos y para las exigencias que impondrá la ley, la gobernanza de datos constituye el punto de partida indispensable para lograr un control apropiado de los datos personales y su protección.

Experiencias compartidas

Los años de tramitación de esta ley dieron oportunidad para conocer cuáles eran las líneas principales que se estaban trabajando, así como algunas preferencias normativas, por ejemplo, que inclinaban la balanza hacia un enfoque más europeo sobre protección de los datos personales. Pequeñas señales como ésta fueron suficientes para que, en instituciones públicas como nuestro ministerio, buscáramos elementos de valor que pudieran aportarnos a un incipiente trabajo en gobierno de datos.

Si bien la Ley sobre Protección de Datos Personales no establece una obligación de realizar gobernanza de datos, la experiencia de tratamiento de grandes bancos de datos enseña que sin un estándar de trabajo es imposible dar cumplimiento a ninguna exigencia. Por ello, el Ministerio de Desarrollo Social y Familia inició, en el año 2018, un trabajo sistemático para gobernar los datos personales y sensibles que le corresponde administrar y, para ello, escogimos el estándar DAMA. La experiencia de este trabajo inicial quedó reflejada en un documento que elaboró la (hoy) Secretaría de Gobierno Digital, con apoyo del Banco Interamericano de Desarrollo [6].

Ya en ese momento, aún sin una nueva normativa, nos desafiamos constantemente a evaluar si éramos capaces de responder a cualquier titular de un dato, qué datos tenemos sobre su persona, con quién lo habíamos compartido, bajo qué amparo legal lo tenemos y lo compartimos, entre otras materias. Tenemos respuestas fáciles y concretas para varias de esas preguntas, pero obtener algunas otras resultaba engorroso o imposible, y sabíamos que debíamos prepararnos para ello. Lo vimos como la necesidad de introducir cambios en formas de trabajo a distintos niveles, que tocan distintas partes de la institución, tanto a nivel funcional o de negocio, como a niveles técnicos y tecnológicos, es decir, era necesario establecer una nueva cultura de trabajo y de conocimiento y de forma de comportamiento institucional respecto del tratamiento de los datos personales.

Como parte de este trabajo, establecimos normativas ministeriales sobre el trabajo con datos personales, para ordenar la forma de trabajo en distintos niveles. Y, si bien no ha estado exento de dificultades, ha permitido entregar señales sobre cómo se trabaja con datos personales, qué significa la proporcionalidad, por qué no todos pueden acceder a los datos que el ministerio trata, qué obligaciones de protección y privacidad tenemos, no sólo como funcionarios públicos sino, específicamente, como funcionarios de este ministerio, entre otras muchas materias, que fuimos dejando reguladas y sobre las que hemos capacitado cada año, una y otra vez, porque los cambios organizacionales y de cultura no ocurren de la noche a la mañana.

Entre las prácticas que instalamos paulatinamente, aprovechando el marco de trabajo DAMA y las prácticas que parecían aplicables de la experiencia europea, estuvo la evaluación de impacto en la privacidad. Para ello, buscamos cursos gratuitos y elaboramos instrumentos propios que nos permitieron comenzar la evaluación de los proyectos tecnológicos ministeriales que usan datos personales, para determinar si en algún punto, significan un riesgo en la privacidad para los titulares de los datos que utilizan. Desde que partimos con esta práctica a la fecha se han evaluado un par de decenas de proyectos ministeriales, tras cuyos resultados se introdujeron ajustes de todo tipo, para hacerlos más seguros desde el punto de vista de la protección de los datos de las personas.

La evaluación de impacto en la privacidad es una de las obligaciones que trae la ley de protección de datos personales, específicamente en su artículo 15 ter y, claramente, nuestro ministerio califica en la obligatoriedad de su realización, por el tipo de tratamiento de datos que realiza.

Volviendo la mirada hacia la Administración del Estado, muchas instituciones que son parte del Grupo A antes mencionado, y que administran bancos de datos, iniciaron proyectos de implementación de gobernanza de datos más o menos a la par de nuestro ministerio. Con muchos de ellos compartimos e intercambiamos experiencias durante estos años, aprendiendo de la forma en que realizamos el trabajo con los datos y del cómo establecimos un modelo de gobierno de datos, para avanzar en el cambio cultural y organizacional que significa lograr esa gobernanza.

De estos diálogos, evalúo que para las instituciones que iniciaron el trabajo de gobernar sus datos con anticipación, será más fácil dar cumplimiento a las obligaciones que se establecen en la normativa que entrará en vigor a contar de diciembre de 2026, en comparación con aquellas que no han iniciado ese camino. Porque el tratamiento de los datos gobernados es algo que se obtiene de manera progresiva a nivel institucional. No pasa por una instrucción o un lineamiento. Se requiere lograr un cambio de cultura de trabajo en torno a los datos personales.

Sin ir más lejos, instituciones como la nuestra, donde hemos trabajado con un foco en datos qué podríamos llamar "de negocio" y no tanto en los datos operacionales, tenemos que trabajar para involucrar a nuevos usuarios que, hasta hoy, no había sido necesario incluir tan vigorosamente, como los equipos de Desarrollo de las Personas y, en general, las personas de Administración y Finanzas, que administran los datos personales de las y los funcionarios y trabajadores de las instituciones.

Nos desafiamos constantemente a evaluar si éramos capaces de responder a cualquier titular de un dato qué datos tenemos sobre su persona, con quién lo habíamos compartido y bajo qué amparo legal lo tenemos y lo compartimos.

Conclusión

La entrada en vigor de la nueva ley de protección de datos personales representa, sin duda, un cambio profundo para las instituciones públicas, pero no un salto al vacío. El sector público arriba a este nuevo estándar con una trayectoria previa: años de regulaciones administrativas, principios de actuación que han marcado límites claros, y el rol fiscalizador que históricamente ejerció el Consejo para la Transparencia. Todo ello configura un punto de partida que, si bien es insuficiente frente a las exigencias actuales, dista de ser inexistente.

Sin embargo, el desafío real no está sólo en la actualización normativa, sino en la capacidad de cada institución para transformar esa base en un modelo maduro de gestión y protección de datos. La experiencia acumulada por instituciones que administran bancos de información y la adopción de marcos de trabajo como DAMA han demostrado que la única forma de responder adecuadamente a las nuevas obligaciones es mediante un cambio cultural sostenido y transversal.

En esa línea, herramientas como el marco de gestión de datos del Sistema de Transformación Digital permiten dimensionar brechas y orientar un trabajo planificado. Si bien es una autoevaluación y, como tal, tiene muchas limitaciones, hoy es el mejor *proxy* al estado de preparación de los servicios públicos respecto de la entrada en vigor de la Ley de Protección de Datos Personales.

Las instituciones que han iniciado el camino del gobierno de datos con anticipación —instalando prácticas, ajustando procesos, definiendo normativas internas y preparando equipos— enfrentarán este nuevo escenario con mayor madurez y capacidad de adaptación. Para aquellas que aún no han comenzado, el desafío será enorme, no sólo porque el tiempo apremia, sino porque la gobernanza de datos no se decreta: se construye día a día, en la operación cotidiana, en la toma de decisiones, en la convicción de que la protección de los datos personales es parte esencial del quehacer público, y eso toca demasiados puntos de la administración. Se requiere un proyecto para lograr gobernarlos, porque requiere un proceso de maduración institucional. **B**

Referencias

[1] Decreto 100 fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile, Capítulo III De los derechos y deberes constitucionales, artículo 19, número 4°, https://bcn.cl/2eph2.

[2] Ley N° 19.628 sobre protección de la vida privada, Del tratamiento de datos por los organismos públicos, https://bcn.cl/2eqfn.

[3] Ley N° 20.285 sobre acceso a la información pública, artículo 33, letra m), https://bcn.cl/25bya.

[4] Ley N° 21.180 transformación digital del Estado, https://bcn.cl/2eqqx.

[5] DFL 1 establece normas de aplicación del artículo 1 de la ley N° 21.180, de transformación digital del Estado, respecto de los procedimiento administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley, a los Órganos de la Administración del Estado que indica y materiales que les resultan aplicables, artículo 5°, https://bcn.cl/yW4svd.

[6] Gobierno de datos en Ministerio de Desarrollo Social y Familia, https://digital.gob.cl/biblioteca/estudios/gobierno-de-datos-en-ministerio-de-desarrollo-social-y-familia/.