

Protección de Datos Personales: No basta con tener papeles



Matías Troncoso Zúñiga, Abogado de la Dirección Jurídica de la Universidad Católica del Maule.

La promulgación de la Ley N°21.719, que moderniza la protección de la vida privada en Chile, marca un punto de inflexión para el ecosistema público y privado del país. Después de años de funcionamiento con un marco normativo rezagado frente a la rápida evolución de la tecnología, el país da un paso firme hacia la modernización mediante la creación de una Agencia de Protección de Datos Personales, dotada de herramientas reales para orientar y fiscalizar, lo que sitúa a la legislación chilena a la altura de los mejores estándares internacionales. El gran valor de esta normativa no reside únicamente en su capacidad sancionatoria, sino en el profundo cambio de enfoque que propone: el tránsito de una cultura de cumplimiento meramente formal, donde bastaba con tener un documento de “términos y condiciones” hacia un modelo basado en la “responsabilidad proactiva”. Este principio invita a comprender que la privacidad debe garantizarse desde el diseño mismo de cualquier proyecto. A medida que la euforia legislativa decanta, los sectores público y privado se enfrentan a una realidad ineludible: el verdadero reto no fue aprobar la ley, sino lograr su implementación. Al analizar el panorama actual, emergen tres brechas críticas que amenazan con convertir la entrada en vigencia de esta norma en un problemático despertar para las organizaciones. El primer gran obstáculo es la infraestructura. Durante décadas, las empresas e instituciones acumularon datos como si fueran un recurso inagotable y

sin costo; hoy, esa acumulación constituye un pasivo de alto riesgo. La nueva normativa exige garantizar derechos complejos, como la “portabilidad” (entregar al titular sus datos en un formato estructurado) y la “supresión” (el derecho a ser borrado). El problema radica en que la mayoría de las organizaciones desconoce exactamente que datos posee, donde están alojados o quien tiene acceso a ellos, debido a que los sistemas heredados no fueron diseñados con la privacidad en mente. La segunda brecha se encuentra fuera de las fronteras de la propia organización. En la economía actual, ninguna entidad procesa datos en solitario, dada la dependencia de servicios en la nube, agencias de marketing y proveedores de software. La ley establece un régimen estricto de responsabilidad sobre quienes actúan como “encargados” del tratamiento de datos. El desafío en este punto es monumental: ya no basta con que una empresa sea segura; debe garantizar que todo su ecosistema de proveedores también lo sea. Finalmente, la brecha más profunda es la cultural. Todavía existe la falsa creencia en los directorios y



gerencias generales de que la protección de datos es un “problema de TI” o un mero “trámite legal”. La adecuación a la Ley N°21.719 no se soluciona adquiriendo un antivirus o redactando una nueva política de privacidad web. Exige una gobernanza real, encabezada por un Delegado de Protección de Datos que no opere como una figura decorativa, sino como un profesional con independencia, presupuesto y capacidad de veto sobre proyectos que pongan en riesgo la privacidad ciudadana. La entrada en plena vigencia de esta ley pondrá a prueba la resiliencia de los sectores público y privado. El desafío está trazado: el mercado debe dejar de ver la privacidad como un obstáculo legal o un mero costo de cumplimiento, para comenzar a entenderla como un sello de calidad, una ventaja competitiva y, por, sobre todo, como la máxima expresión de responsabilidad. ●