

CÓMO IMPACTA LA LEY A LOS SECTORES QUE TIENEN A LOS DATOS AL CENTRO

Cumplir con ley sin perder la viabilidad del negocio es el reto para las empresas que hacen uso intensivo de información personal. Consentimiento explícito de los dueños de los datos es solo uno de los conceptos que entran en juego en diciembre.

POR FRANCISCA ORELLANA

La nueva Ley de Protección de Datos Personales transformará por completo la forma en que algunos sectores económicos utilizan la información personal como centro de su negocio, lo que implica una transformación relevante en su estrategia para seguir siendo competitivos.

La norma entrega un nuevo marco y estándar para la privacidad y seguridad de los datos personales y su implementación plantea desafíos legales, tecnológicos y operativos para cumplir con ella sin perder la viabilidad del negocio.

El director de KPMG Law de KPMG Chile, Edmundo Varas, explica que actualmente los datos personales son utilizados en diversos ámbitos, como procesos laborales, desarrollo educacional, analítica urbana, gestión de políticas públicas, prevención de fraudes, análisis de proveedores y otros, tanto en el sector público como privado.

"Hay sectores como banca, seguros, servicios financieros, telecomunicaciones, salud, retail y economía digital que se verán fuertemente afectados, ya que realizan tratamiento de datos a gran escala, manejan datos sensibles y utilizan mecanismos de decisiones automatizadas o perfilamiento", dice Varas, mientras advierte que existe una infinidad de sectores que aún no han evaluado adecuadamente cómo la ley los podría impactar.

Ricardo Seguel, docente de la Facultad de Ingeniería de la U.

Adolfo Ibáñez y senior advisor en Technology Unit, menciona que la nueva ley impacta en los derechos ARCO —las facultades de acceso, rectificación, cancelación/supresión y oposición, que permiten a las personas controlar sus datos personales— y "empodera las personas a demandar a las instituciones públicas o privadas de forma transversal por el uso no autorizado de su información en campañas de publicidad o en cómo están custodiando su información privada".

En ese marco, ahora, las empresas deberán contar con el consentimiento "explícito de cómo y qué datos utilizar o compartir para actividades de publicidad, mejoras de procesos internos e incluso en entrenamiento de modelos de IA y GenAI", agrega.

El director de la Asociación Gremial de Profesionales en Protección de Datos Personales, Diego Morandé, indica que las empresas deberán implementar, por ejemplo, registros de actividades de tratamiento (RAT) y, en muchos casos, realizar estudios de impacto en protección de

datos, especialmente cuando tratan información sensible, hacen perfilamiento o usan tecnologías de alto riesgo. "Esto implica rediseñar procesos, contratos, sistemas y modelos de negocio que históricamente se construyeron sin estándares formales de rendición de cuentas en protección de datos y privacidad", precisa.

Para lograrlo, añade Seguel, las organizaciones "deberán implementar varios pasos administrativos de forma automática para poder responder en tiempo y forma a las personas y a la Agencia de Protección de Datos".

Más derechos

Las empresas están poco a poco ajustando sus procesos a la nueva normativa y buscando tener el consentimiento explícito de las personas para poder utilizar su información.

En la industria financiera, por ejemplo, un estudio de EY indica que, a febrero de este año, solo un 36% de las instituciones ya tenía identificados y clasificados los datos personales sensibles, mientras que el 50% se encontraba en desarrollo y solo el 29% de los encuestados había implementado la obtención del consentimiento explícito del titular antes de tratar sus datos personales.

Morandé agrega que, con la

ley, las estrategias de marketing, fidelización y analítica de clientes deberán ajustarse a nuevas bases de licitud y a principios como minimización y responsabilidad proactiva, lo que cambia la forma de capturar y explotar datos. "Las empresas que no inviertan en capacidades internas enfrentarán mayores riesgos sancionatorios, mayores costos de corrección y una clara desventaja competitiva frente a quienes integren la protección de datos como un activo estratégico. El desafío más importante se encuentra en la concientización y evangelización de estos temas", dice.

En ese objetivo, detalla Seguel, la brecha digital en las instituciones públicas y en las pymes es la mayor tarea pendiente en Chile.

Varas agrega que el ordenar las bases de datos, establecer medidas tecnológicas para captar, utilizar y proteger los mismos, así como diseñar reglas que permitan aprovechar de manera segura el dato con respecto a los grupos de interés con que se relaciona la empresa, no debe considerarse un costo, sino una inversión. "Preparará a la empresa para acceder, analizar y emplear datos de manera segura y eficiente para respaldar decisiones estratégicas y optimizar los resultados del negocio", concluye el ejecutivo.

SOLO
36%
 DE LAS
 INSTITUCIONES
 FINANCIERAS
 TENÍA IDENTIFICADOS
 Y CLASIFICADOS LOS
 DATOS PERSONALES
 SENSIBLES, SEGÚN
 UN ESTUDIO DE EY A
 FEBRERO PASADO.