GERENCIA
Tecnologías y estrategias para la transformación digital

Fecha: 30/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $730.404 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $829.080 Difusión: 0
Vpe portada: $829.080 Ocupación: 88,1%

ESPECIAL **Protección de Datos Personales**

La ilusión de borrar un dato: ¿es realmente posible eliminar un dato personal?

La entrada en vigencia de la Ley de Protección de Datos Personales en Chile instala un desafío técnico y regulatorio de alta complejidad: hacer efectivo el derecho de eliminación de datos en entornos digitales donde la información no desaparece fácilmente. Esta columna analiza las brechas entre el marco legal y su aplicación práctica, revisando experiencias internacionales y abordando los desafíos operativos, tecnológicos y de gobernanza que enfrentan las organizaciones.

Oliver Ortiz, Senior Manager en Deloitte Legal.

René Martínez, Director de Cyber en Deloitte.

Con la entrada en vigencia de la Ley 21.719 sobre Protección de Datos Personales (LPDP), Chile enfrenta un desafío que hasta ahora era ajeno a su práctica regulatoria: dar cumplimiento efectivo al derecho de eliminación de datos personales. La pregunta que surge es: cuando un titular pide que borren sus datos, ¿desaparecen realmente? ¿Qué ocurre con las copias de respaldo, y los logs de auditoría, o incluso modelos de Inteligencia Artificial (IA) que absorbieron esa información? La LPDP reconoce el derecho, pero no indica cómo debe realizarse técnicamente.

Si bien pareciera ser un elemento nuevo en el ecosistema, la verdad es que Europa lleva ya casi una década lidiando con esta problemática. Así, el Reglamento General de Protección de Datos (RGPD) consagra en su artículo 17 el "derecho de supresión"(1), también conocido como "el derecho al olvido" con una formulación aparentemente categórica: el interesado puede obtener "sin dilación indebida" la eliminación de sus datos. Una redacción muy similar sigue el Art. 7 de la LPDP en Chile. Sin embargo, el mismo artículo establece excepciones en su inciso final, por lo que es evidente que el propio legislador (tanto en Europa como en Chile) asumió que la supresión no es un concepto absoluto.

El estándar europeo

Al estudiar la realidad del Viejo Continente, si bien ninguna autoridad de datos personales ha exigido un borrado instantáneo y absoluto de backups, todas coinciden en que lo imprescindible es que el responsable (la empresa u organización que trata los datos) sea plenamente transparente con el titular. En otras palabras, este último debe estar plenamente informado de qué pasará efectivamente con sus datos personales. Por ejemplo:

- La autoridad británica Information Comissioner's Office (ICO) ha desarrollado un estándar más pragmático, acuñando el concepto de "beyond use" (fuera de uso)(2), aceptando que los datos permanezcan en backups, siempre que el responsable no los utilice para decisiones sobre el titular, no los comparta con terceros, y se protejan con medidas de seguridad adecuadas, comprometiéndose a eliminarlo permanente "cuando sea técnicamente posible".
- Por su parte, la Commission Nationale de l'Informatique et des Libertés (CNIL) de Francia, ha sido más explícita, indicando que las organizaciones "no están siempre obligadas a eliminar backups para cumplir una solicitud de supresión", pero sí deben informar al titular que sus datos permanecerán en copias de respaldo durante un plazo definido, si es el caso(3).
- En España(4), la normativa de datos personales establece que cuando proceda la supresión, el responsable debe primero bloquear los datos (con el objeto de impedir su tratamiento y visualización), excepto para ponerlos a disposición de jueces, tribunales o autoridades de protección de datos. Una vez transcurrido el plazo de prescripción, se debe proceder a la destrucción física. En otras palabras, cuando existe una obligación legal de conservación, la información no se borra sino que transita a un estatus controlado con acceso restringido(5).

Hasta aquí entonces, un concepto

GERENCIA
Tecnologías y estrategias para la transformación digital

Fecha: 30/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $684.569 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $829.080 Difusión: 0
Vpe portada: $829.080 Ocupación: 82,57%

queda claro: el dato no muere. Pero puede - y debe - ser gobernado con la seriedad con que protegemos cualquier otro derecho fundamental.

La "operacionalización" de la privacidad

Dado lo anterior, resultará fundamental revisar la "operacionalización" de la privacidad para todos los derechos ARSO+P, entendiendo que técnica y operativamente se deben generar diversos cambios en donde, en relación con la eliminación de datos personales (o supresión) debemos tener las siguientes consideraciones:

a) Identificar todos los datos, estructurados y no estructurados, es decir los que están en sistemas y aquellos que están distribuidos en archivos de diferentes formatos que tienen relación con el titular del derecho que se quiere ejecutar.

b) Se deben determinar aquellos datos personales que no se pueden eliminar dado que existen normativas o regulación vigente que lo impide y por lo mismo las organizaciones cuentan con el consentimiento implícito para determinadas actividades de tratamiento.

c) Para aquellos datos personales que pueden ser eliminados, se debe gestionar su eliminación ya sea manual, semi o automáticamente en los sistemas y repositorios en donde aplique. La experiencia práctica indica que esta eliminación no es escalable manualmente por lo que se requiere de procesos automatizados que se encarguen de esto.

d) Se debe asegurar generar y almacenar la evidencia necesaria para cumplimiento normativo y eventuales auditorías de la Agencia de protección de datos personales (Agencia).

e) Se debe medir y gestionar internamente el SLA de cumplimiento normativo de cada solicitud de eliminación de datos personales, para efectos de evitar multas por no cumplimiento de los plazos establecidos.

f) Se debe entregar al solicitante una confirmación de lo realizado.

Un concepto queda claro: el dato no muere. Pero puede - y debe - ser gobernado con la seriedad con que protegemos cualquier otro derecho fundamental.

Pero hasta este punto hemos eliminado solamente los datos que están actualmente en productivo. Las preguntas que quedan por responder son:

- ¿Qué ocurre con los datos personales que existen en los backups o respaldos?
- ¿Qué ocurre con las solicitudes de eliminación ejecutadas luego de la ejecución de un DRP por interrupciones de operación que requieren la recuperación desde backups?

Para ambas situaciones se debe contar con un mecanismo que identifique proactivamente aquella información que haya sido restaurada en productivo por cualquiera de las situaciones anteriores u otras propias del negocio. De esta forma es posible volver a eliminar la información personal restaurada, reaplicando las solicitudes de supresión (ARSO+P) que sean identificadas, lo que se puede efectuar con una solución de privacidad que resuelva la problemática o bien con herramientas internas y/o procedimientos manuales. Como podemos apreciar, el desafío de la privacidad y protección de datos personales no es sólo normativo, sino que modifica muchos procesos operativos y tecnológicos de las organizaciones. Quedará en la Agencia el realizar las recomendaciones de criterios y parámetros técnicos que permita a las organizaciones tener certeza de estar en cumplimiento de la LPDP. G

(1) Unión Europea, Reglamento general de protección de datos Contenido, articulo 17, abril 5, 2016, Artículo 17 UE Reglamento general de protección de datos. Privacy/Privazy according to plan. / (2) Information Commissioner's Office (ICO), "Right to erasure", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/ / (3)Commission Nationale de l'Informatique et des Libertés (CNIL), junio 11, 2020, "Sheet n°13: Prepare for the exercise of people's rights", https://www.cnil.fr/en/sheet-ndeg13-prepare-exercise-peoples-rights) / (4) Ley Orgánica N° 3/2018, OE-A-2018-16673, Boletin Oficial del Estado (España), articulo 32, diciembre 6, 2018, https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673) / (5) Agencia Española de Protección de Datos (AEPD), Informe Jurídico 00148/2019, https://www.aepd.es/documento/2019-0148.pdf)