Minuta de Exposición: Desafíos Prácticos en la Supresión de Datos Personales en Chile

1. Antecedentes generales

La Red chilena de mujeres en Datos Inteligencia Artificial y Ciberseguridad (**REDIAC)**, es una corporación sin fines de lucro constituida en 2025, cuyo objeto es fomentar la inclusión, participación y desarrollo profesional de mujeres en el campo de la ciberseguridad, Protección de Datos Personales e Inteligencia Artificial.

Conforme a sus Estatutos, en el desarrollo de sus actividades **REDIAC** podrá, entre otras materias, colaborar con y participar en instituciones públicas y privadas para mejorar los estándares de Protección de Datos, Inteligencia Artificial y seguridad cibernética en Chile.

Esta minuta ha sido preparada por las socias de **REDIAC**, Paloma Herrera Carpintero, Constanza Hess Arteaga, María Luisa Acuña Quiñones y Katherine Barcia Schott.

2. Introducción

- **Contexto Normativo:** La entrada en vigencia de la ley 21.719 marca un antes y un después en la gestión de los datos personales en Chile. Más allá del marco normativo, el desafío está en la capacidad operacional y presupuestaria de las empresas para implementar medidas técnicas que les permitan cumplir con la norma.
- **Relevancia Práctica:** La eliminación de los datos se ha convertido en un punto crítico del cumplimiento: una frontera entre la protección efectiva de los derechos de las personas, la imposibilidad material de cumplir con algunas obligaciones y la necesidad práctica de mantener información útil para operar, auditar y defenderse. En la realidad chilena, muchas organizaciones están obligadas a borrar datos que ni siquiera saben exactamente dónde están, ni cuánto necesitan conservar para poder seguir funcionando o defenderse.
- **Objetivo de la Exposición:** Esta exposición abordará los desafíos prácticos en la eliminación de los datos personales, con foco en lo que realmente ocurre en las organizaciones chilenas al intentar cumplir la ley.

3. Fundamento Legal de la Supresión de Datos Personales

La obligación de eliminar o suprimir datos personales no es nueva, ya en el artículo 6to de la ley N° 19.628 establece que los datos deben ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. La Ley N° 21.719

moderniza este marco, se adapta al estándar del Reglamento Europeo y refuerza la exigencia en diferentes niveles:

- **Ley N° 21.719, Artículo 3° (Principio de Proporcionalidad):** Los datos personales pueden ser conservados sólo por el período de tiempo necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados. El cumplimiento de este principio implica una reacción proactiva de parte de las empresas, que no deben esperar al ejercicio del derecho de supresión por parte de un titular, sino por el contrario, generar un calendario de eliminación y disponibilizar las medidas técnicas y organizativas para ejecutarlo de forma sistemática.
- **Ley N° 21.719, Artículo 7° (Derecho de Supresión):** El titular tiene derecho a solicitar la eliminación de sus datos en diversos escenarios, incluyendo cuando no sean necesarios para los fines originalmente pactados, por revocación del consentimiento, tratamiento ilícito o caducidad. Frente a este requerimiento las organizaciones podrán (i) negar el requerimiento por existir una base de licitud que permita continuar con el tratamiento o (ii) ejecutar la eliminación en el menor plazo posible, cuestión que sólo podrán hacer si cuentan con la tecnología necesaria para eliminar datos en todos sus ambientes, tanto productivos como de respaldo, incluyendo repositorios de datos de los terceros que intervienen en el tratamiento.
- **Ley N°21.719, Artículo 11 (Procedimiento ante el responsable de datos):** Cuando se formule una solicitud de rectificación, supresión u oposición, el titular tendrá derecho a solicitar y obtener del responsable el bloqueo temporal de sus datos o del tratamiento que realice, según corresponda. El responsable deberá responder al requerimiento dentro de los dos días hábiles siguientes a su recepción, ejecutando las medidas que garanticen que el dato ha sido efectivamente bloqueado en todos los sistemas y procesos de la organización y sus terceros intervinientes, cuestión que representa similares desafíos que los que plantea el derecho de supresión y una carga adicional para las organizaciones que deberán contar con tecnología que les permita cumplir con ambos requerimientos (bloqueo y supresión).

En consecuencia la supresión deja de ser una opción y pasa a ser un deber jurídico, cuya omisión puede acarrear sanciones relevantes, asunto especialmente preocupante cuando consideramos el universo PYME chileno, que - generalmente - no cuenta con recursos presupuestarios para adquirir herramientas tecnológicas automatizadas o contratar a un contingente de personal dedicado en forma exclusiva a la eliminación de datos en forma manual.

4. Factibilidad Técnica de Eliminación de Datos Personales

- **Complejidad Técnica en los entornos productivos:**

    - **Realidad Operacional:** La eliminación inmediata y completa de datos personales en sistemas productivos es técnicamente posible y requiere esfuerzos menores que aquellos que podrían requerir los entornos de respaldo. Sin perjuicio de ello, el desafío sigue siendo relevante, especialmente para aquellas organizaciones que no cuentan con una arquitectura de sistemas y procesos debidamente estructurado o que no han realizado un mapeo o "discovery" de los datos personales almacenados en sus sistemas, e incluso en el caso de muchas PYMEs ni siquiera tienen claridad de cuántos sistemas diferentes tratan datos personales (ERP, CRM, planillas, correos, etc). Esta situación es particularmente crítica en empresas cuyo giro no está directamente vinculado a servicios tecnológicos o digitales, pero que igualmente tratan grandes volúmenes de datos personales.

- **Complejidad Técnica de los Respaldos (Backup):**

    - **Realidad Operacional:** La eliminación inmediata y completa de datos personales de todos los sistemas, especialmente de los respaldos o copias de seguridad, es una de las mayores complejidades técnicas que enfrentan las organizaciones. Particularmente respecto de los sistemas de respaldo o "backup" se debe considerar que estos están diseñados para la recuperación ante desastres y la retención de data a largo plazo, lo que dificulta la eliminación granular de datos específicos sin comprometer la integridad, disponibilidad y capacidad de recuperación del sistema.

      Asimismo, la eliminación de ciertos datos almacenados dentro de estos sistemas si bien técnicamente puede ser posible, pues en muchos casos no existen recursos humanos ni financieros, así como capacidades técnicas para "pisar" o "borrar" un dato sin comprometer la totalidad de la información contenida en un repositorio determinado. A mayor abundamiento, los sistemas de respaldo se generan en distintas ventanas de tiempo, ya sean estas de horas, días, semanas, etc., generando grandes volúmenes de datos, generalmente respaldados en más de un sistema o repositorio, complejizando aún más la viabilidad de eliminación (o rectificación) de un dato particular dentro de una base de datos de respaldo en general.

Cumplir con esta obligación implica la contratación de tecnología especializada, que si bien existe, en general no se destina a estos propósitos por cuanto la relación costo/beneficio (horas humanas o desarrollo de funciones específicas versos precio) en la práctica incide en que las empresas proveedoras (i) no ofrezcan el servicio o (ii) el costo de adquirirlo sea demasiado elevado, aspectos ambos que en definitiva tienden a que las organizaciones prefieran internalizar el costo de una potencial sanción ("prefiero pagar la multa").

- **Complejidad Técnica en la cadena de suministro (Proveedores):**

  Realidad Operacional: Hemos abordado como los costos financieros asociados al cumplimiento de estas obligaciones pueden resultar significativos para las organizaciones, que además deben considerar en este esfuerzo a los terceros proveedores que intervienen en el ciclo de vida del dato personal. Ello incluye desde la adquisición de programas especializados para identificar datos personales y proceder a su bloqueo y/o eliminación, hasta las horas-humanas requeridas por el equipo técnico para ejecutar dichas gestiones.

En definitiva, si bien las empresas de mayor tamaño pueden asumir estos costos, la situación es distinta para las PYMEs, que enfrentan dificultades tanto para financiar este tipo de tecnologías como para contar con el personal necesario que les permita cumplir con los plazos establecidos en la ley. Esta carga se acentúa cuando el titular ejerce sus derechos de rectificación, supresión u oposición y solicita el bloqueo temporal de los datos, medida que el responsable debe implementar dentro de los dos días hábiles siguientes a la recepción de la solicitud. Todo ello no sólo puede impactar significativamente la actividad operacional y la sostenibilidad financiera de las PYMEs, sino que también podría evidenciar una **falta de sentido de realidad en la aplicación práctica de la norma** y constituir una desigualdad ante la ley, al imponer obligaciones homogéneas a actores con capacidades económicas y técnicas profundamente dispares.

  - **Implicancias para las organizaciones:**
    - **Costos:** La implementación de soluciones que permitan la eliminación selectiva en backups puede ser extremadamente costosa y no existe claridad de su disponibilidad en el mercado.
    - **Integridad del Sistema:** Una eliminación inadecuada (p.e. realizada a través de procesos manuales o tecnologías rudimentarias), podría afectar la capacidad de restaurar sistemas completos, poniendo en riesgo la continuidad operativa de las organizaciones.
    - **Plazos de Retención de Backups:** Es común que las políticas de retención de backups superen los plazos de finalidad de tratamiento de datos personales, cuestión que se relaciona con la necesidad de

continuidad operativa y no necesariamente con una voluntad de mantener datos personales almacenados “por si acaso”.

- **Inviabilidad técnica de eliminación de un dato aislado dentro de una base de datos general:** que ocurre habitualmente respecto de bases de datos no estructuradas, *per se* complejas de identificar a través de un mapeo o descubrimiento de datos, determinando en consecuencia un posible incumplimiento de la ley.

- **Implicancias para la Agencia de Protección de Datos Personales:**
  - **Viabilidad de la Fiscalización:** ¿Qué capacidades técnicas tiene la Agencia para verificar el cumplimiento de esta obligación? Consideramos que se trata de una pregunta válida, de cuya respuesta dependerá el *enforcement* y el nivel de criticidad que las organizaciones deban imprimir al cumplimiento de esta obligación en particular. Ante la falta de recursos para fiscalizar el cumplimiento efectivo de esta obligación, consideramos que los esfuerzos deberían orientarse a determinar alternativas al cumplimiento, ofreciéndose como parte de una medida destinada al cumplimiento progresivo de la obligación de supresión de datos.

- **Consideraciones Prácticas y Soluciones:** El análisis de las capacidades locales en materia de disponibilidad y acceso a la tecnología, en adición al análisis de la experiencia comparada - especialmente en el caso europeo - nos animan a sugerir a esta Comisión las siguientes medidas alternativas al cumolimiento de la obliación de liminación o supresión total de datos personales, ello sin perjuicio de que puedan identificarse otras:
  - **Anonimización en Backups:** Ya contenida tácitamente en la Ley como una alternativa a la eliminación en ambientes productivos, se deberá analizar la viabilidad técnica de anonimizar datos personales en ambientes de respaldo, garantizando que no se afecte la integridad ni la disponibilidad de los datos frente a una contingencia operacional que requiere la restauración de bases de datos productivas.
  - **Seudoanimización:** Evaluar la posibilidad de seudoanimizar datos personales como una medida de cumplimiento, una vez que la finalidad de tratamiento ha cesado y no hay base legal para su retención identificable. Esta medida podría acompañarse de políticas sólidas de restricción y control de acceso a los datos seudonimizados, reduciendo así la posibilidad de una brecha o incidente.
  - **Fomentar la eliminación total en ambientes productivos:** Permitiendo mantener los mismos datos en entornos de respaldo,

en la medida en que se acrediten niveles de seguridad adecuados y debidamente certificados.

- **Políticas de Retención de Backups:** Establecer y documentar políticas claras de retención de backups que consideren tanto los plazos legales y de finalidad para los datos personales como la continuidad operacional, asegurando que los datos se eliminen de los respaldos tan pronto como sea técnicamente factible, operacionalmente seguro y legalmente permitido.
- **Segregación de Datos:** Si es posible, segregar los datos personales de otros datos en los sistemas de backup para facilitar su gestión y eliminación. Sin embargo esta medida puede resultar poco eficiente o viable para las empresas ya que requiere incurrir en altos costos tecnológicos y horas humanas.

5. El Bloqueo o Indisponibilidad Temporal como Paso Previo a la Eliminación

- **Concepto de Bloqueo (Ley N° 21.719, Artículo 8° ter):** El bloqueo de datos se define como la suspensión temporal de cualquier operación de tratamiento de los datos almacenados tanto a entornos productivos como a respaldos.
- **Importancia del Bloqueo Previo:** Antes de la eliminación definitiva, el bloqueo o la indisponibilidad temporal de los datos personales es un paso fundamental para garantizar que no sean objeto de tratamiento alguno, salvo su conservación debidamente restringida para el cumplimiento de obligaciones legales o el ejercicio o defensa de reclamaciones.

6. Conclusión

- Las organizaciones manejan datos en múltiples sistemas, bases de datos y ubicaciones geográficas (nube, on-premise, sistemas heredados, etc.), lo que requiere procesos y herramientas automatizadas para rastrear y eliminar un dato de forma completa. De modo que, cualquier empresa que reciba solicitudes de supresión deberá responder rápido y en múltiples sistemas, algo imposible sin automatizar búsquedas, verificaciones y eliminaciones.

- Adicionalmente, dichas organizaciones deberán abordar las complejidades técnicas de la eliminación, especialmente en entornos de respaldo, cuestión que no necesariamente es viable desde un punto de vista de recursos existentes, especialmente en aquellos casos de empresas pequeñas y medianas que no cuentan con estructuras internas ni presupuesto para acceder a las tecnologías disponibles en el mercado.
- El bloqueo o la indisponibilidad temporal de los datos, con medidas técnicas como la restricción de acceso, segregación lógica y cifrado, es un paso esencial antes de

la eliminación definitiva, garantizando el cumplimiento y la seguridad de la información. Estas medidas parecen alzarse como una alternativa temporal a la eliminación total en entornos productivos, sin embargo no es suficiente ni técnicamente viable en entornos de respaldo.

- De acuerdo a lo establecido en el artículo 10 de la Ley N° 21.719, el ejercicio del derecho de supresión siempre será gratuito para los titulares y no se podrá exigir el pago de los costos directos a los titulares como podría ocurrir en el caso del derecho de los derechos de acceso y portabilidad cuando son ejercidos más de una vez por trimestre. Esto implica que todos los costos recaen en la organización requerida.

- La Agencia deberá identificar alternativas para el cumplimiento de este derecho/deber considerando la evidente asimetría y desigualdad en el acceso existente entre empresas pequeñas y medianas y grandes empresas que cuentan con recursos y acceso a la tecnología que podría utilizarse para el cumplimiento de una solicitud de eliminación de datos personales. Lo contrario - consideramos - redundará en que las organizaciones prefieran internalizar el costo de una multa (potencial por cierto) o simplemente en que, ante la falta de capacidades técnicas y presupuestarias de la Agencia para fiscalizar el cumplimiento, el derecho de supresión termine siendo letra muerta.

- Por lo tanto, será necesario combinar exigencia regulatoria con realismo técnico: aceptando la pasividad de respaldos, priorizando la supresión en entornos productivos, promoviendo la seudonimización y estableciendo plazos de retención razonables. El desafío para Chile será adaptar esas soluciones a nuestra realidad, sin perder de vista que la finalidad última no es sólo borrar datos, sino **proteger derechos fundamentales sin asfixiar la viabilidad de las organizaciones**.

- El propio UK GDPR, según la guía oficial del Information Commissioner's Office (ICO), reconoce que el borrado no siempre es técnicamente simple ni inmediato. Por eso permite que el responsable implemente "medidas razonables" según la tecnología disponible, los costos, las limitaciones técnicas y la estructura de los sistemas, en vez de exigir un borrado absoluto e instantáneo en todos los entornos. Esta flexibilidad técnica está pensada precisamente para sistemas complejos —copias de seguridad, entornos distribuidos, logs o repositorios legacy— donde eliminar datos de forma total puede ser inviable o poner en riesgo la integridad operativa. En esos casos, la organización puede aplicar bloqueos, aislamiento o eliminación progresiva, siempre que adopte medidas efectivas para impedir el uso de los datos y documente por qué el borrado inmediato no es posible.