Breves comentarios al Proyecto de Ley de Protección de Datos Personales del Ministerio de Desregulación y Transformación del Estado

Fundación Vía Libre, julio 2026

Presentación

Desde la Fundación Vía Libre hemos insistido reiteradamente y por largo tiempo sobre la necesidad de una reforma de la Ley de Protección de Datos Personales 25.326, sancionada en un contexto con desafíos muy diferentes a los actuales para la protección de datos, por lo que celebramos que existan iniciativas de actualización.

Sin embargo, el proyecto de Ley de Protección de Datos Personales compartido por el Ministerio de Desregulación y Transformación del Estado introduce retrocesos concretos que resultan especialmente sensibles en el contexto tecnológico actual. Priorizamos a continuación los cuatro puntos sobre los que consideramos más urgente llamar la atención: 1) transferencia internacional por elección de infraestructura tecnológica extranjera; 2) entrenamiento de IA, supresión en modelos ya entrenados y decisiones automatizadas; 3) cesión estatal y listados sin consentimiento; y 4) consentimiento tácito.

A lo largo de los puntos que abordamos aquí veremos que el proyecto delega en el responsable del tratamiento (sea privado o estatal) la decisión sobre cuándo hace falta consentimiento, cuándo un dato es demasiado sensible para divulgar su lógica de construcción, o cuándo un límite técnico justifica no eliminar un dato a pedido del titular. Quien evalúa la procedencia del derecho es la misma parte cuyo interés está en juego. Ese desplazamiento del control hacia el propio regulado no es un detalle técnico, sino una cuestión central para la efectivización de derechos en un escenario donde la acumulación e interconexión de datos, el uso de infraestructura de nube extranjera y el entrenamiento de sistemas de IA sobre información personal son prácticas corrientes.

Actualizar el marco regulatorio creado por la Ley 25.326 es necesario y deseable, pero una reforma que amplía las excepciones al consentimiento y reduce el control externo sobre quienes procesan datos (en particular el propio Estado) es un retroceso en función de los estándares de derechos humanos que la propia norma dice perseguir. Instamos a que, de mínima, se corrijan estas cuestiones antes de su envío al Poder Legislativo.

Finalmente, agradecemos la convocatoria a enviar nuestras observaciones, y nos reservamos la posibilidad de ampliarlas oportunamente. Para ampliar la información aquí compartida, ofrecemos como puntos de contacto: Beatriz Busaniche, bea@vialibre.org.ar; Enrique Chaparro, echaparro@vialibre.org.ar; Margarita Trovato, margarita@vialibre.org.ar.

1. Transferencia internacional por elección de infraestructura tecnológica extranjera (art. 19, inciso f)

El proyecto declara lícita la transferencia internacional de datos personales por la sola decisión del responsable de utilizar "infraestructura tecnológica ubicada fuera de la República Argentina", exigiendo únicamente que el proveedor "garantice medidas técnicas de seguridad adecuadas", sin requerir una decisión de adecuación ni intervención de la autoridad de control.

Una decisión comercial u operativa (qué proveedor de nube utilizar) no puede sustituir el control de adecuación que exige el resto del propio artículo 19 y que es estándar en la región y en el derecho comparado. Este inciso es particularmente riesgoso cuando quien elige esa infraestructura es el propio Estado para las bases de datos que administra sobre la población.

Propuesta: eliminar el inciso f) del art. 19, o subordinarlo a homologación previa de la autoridad de control equivalente a la exigida para los demás mecanismos del mismo artículo.

2. Entrenamiento de IA, supresión en modelos ya entrenados y decisiones automatizadas (arts. 17, 23 y 25)

Art. 17 - Entrenamiento de sistemas de IA. El artículo dice textualmente que el tratamiento de datos personales para entrenar, desarrollar o evaluar sistemas de IA "será válido como interés legítimo conforme al art. 5 (principio de licitud), inciso f[1]", cuando se cumplan tres condiciones: que no incluya datos sensibles sin consentimiento expreso, que haya medidas de seguridad proporcionales según estándares internacionales y que el titular tenga un mecanismo de oposición gratuito y accesible, pero esa oposición "producirá efectos a partir del siguiente ciclo de entrenamiento o actualización del modelo". Esta redacción trae dos problemas aparejados: por un lado, convierte el entrenamiento de IA en un supuesto que automáticamente configura "interés legítimo" si se cumplen esos tres requisitos formales, en vez de someterlo a una ponderación caso por caso entre el interés del responsable y los derechos del titular, como exige esa misma base de licitud en el art. 5.f para cualquier otro caso. Por otro lado, la oposición es solo hacia adelante; no habilita revisiones ni reclamos para datos que ya hayan sido utilizados en el entrenamiento, sin siquiera evaluar esa licitud.

Art. 23 - Supresión de datos en modelos ya entrenados. El régimen de supresión en sistemas de IA ya entrenados subordina la eliminación efectiva de datos a que no se afecte la "integridad fundamental del modelo", permitiendo sustituir la supresión por medidas alternativas cuando no sea "técnicamente viable" hacerla. Acá el límite no es el secreto sino la viabilidad operativa. Si bien es cierto que eliminar el aporte de un conjunto de datos personales de los parámetros ya entrenados de un modelo de IA es materialmente difícil, el proyecto responde a este problema 1) dejando esta evaluación

[1] Sobre este punto también es importante aclarar que el proyecto tiene un error de referencia: si bien remite al art. 5.f) para la licitud en el entrenamiento de sistemas de IA, entendemos que pretende/debe hacerlo al inciso g.

únicamente en cabeza del responsable (debe hacerlo mediante un informe técnico “accesible” para la autoridad de control, pero no se prevé en la norma intervención alguna) y 2) sin precisar de forma suficiente el estándar de "integridad del modelo" (estabilidad, rendimiento, funcionalidad), por lo que queda sujeto a la decisión discrecional del responsable. En este sentido, la norma termina equiparando el interés puramente comercial de quien lo entrena y/o utiliza con el ejercicio de derechos personalísimos como la privacidad o la autodeterminación informativa.

Art. 25 - Derecho a revisión en decisiones automatizadas y elaboración de perfiles. El derecho a revisión de decisiones automatizadas exige solicitud expresa del titular (no opera por defecto) y excluye explícitamente la divulgación de "algoritmos, modelos, ponderaciones ni información técnica o comercialmente sensible". Un derecho de revisión que no permite conocer la lógica detrás de la decisión es un derecho vacío, un reclamo sin argumento: la persona puede pedir que se revise, pero no puede saber sobre qué basar su objeción ni tiene herramientas para evaluar la respuesta. El secreto comercial es un interés legítimo, pero no puede oponerse de forma dogmática al derecho de una persona a comprender decisiones que la afectan en materia de crédito, salud, trabajo u otros derechos.

Propuesta:

1) Que el art. 17 someta el entrenamiento de IA al test de ponderación de interés legítimo caso por caso, y que la oposición tenga efecto retroactivo sobre el modelo vigente cuando sea técnicamente viable, no sólo sobre ciclos futuros.
2) Que el art. 23 defina con precisión el estándar de "integridad del modelo" que impida su aplicación discrecional, y exija verificación previa por parte de la autoridad de control sobre la inviabilidad técnica invocada (no sólo una declaración jurada del responsable).
3) Que el art. 25 mantenga el derecho a no ser objeto de la decisión por defecto (no solo a solicitud) y que se garantice información significativa sobre la lógica aplicada, bajo los criterios de explicabilidad e interpretabilidad.

3. Cesión estatal y listados sin consentimiento (art. 5, incisos d., i., g.)

El proyecto coloca el consentimiento como una de las bases posibles para la licitud del tratamiento (art. 11), no la única. Habilita también otros supuestos (art. 5) en los que no haría falta consentimiento. Entre ellos incluye el tratamiento de "listados" limitados a nombre, DNI, identificación tributaria, ocupación, fecha de nacimiento y domicilio (inc. i), el intercambio de datos entre organismos estatales "para eximir al titular de aportarlos" (inc. d) o el tratamiento para “la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan otros derechos y libertades fundamentales del titular.”, incluyendo entre los “intereses legítimos”, entre otros, “la mejora razonable de

productos y servicios", "la analítica interna" o "el entrenamiento de sistemas de inteligencia artificial" (inc. g).

Estas cláusulas van en sentido contrario a la reciente decisión de la Corte Suprema de la Nación en el caso Torres Abad, sobre principios de finalidad, consentimiento y proporcionalidad y razonabilidad de las excepciones. Allí el Tribunal entendió que la redacción actual de ley deja prácticamente sin efecto el derecho a la privacidad y sus derivados, porque "los entes estatales estarían exentos, virtualmente en todos los casos, de cumplir con la exigencia del consentimiento." (cons. 14 del fallo).

Las previsiones de este proyecto vuelven a habilitar un paraguas enorme de supuestos en los que el consentimiento del titular se vuelve prescindible. Es difícil, incluso, pensar en casos en los que no se habiliten los supuestos alternativos al consentimiento que se listan en el art. 5. Más aún, el proyecto ni siquiera contempla el requisito de finalidad en este artículo. Como principio general, los datos personales no deben ser utilizados sin consentimiento del titular para un propósito distinto de aquel para el que fueron recogidos, expresamente mencionado cuando se obtuvo el consentimiento.

Recordemos que, además del derecho de los titulares sobre sus datos personales entregados de manera activa, el entrecruzamiento de bases y el procesamiento masivo de datos permite inferir información personal y construir perfiles sobre los que es mucho más complejo para los titulares ejercer derechos como acceso u oposición. Es indispensable reforzar las salvaguardas para que estos procesos no sucedan sin consentimiento y en circunstancias que no son de estricta necesidad y proporcionalidad. Para más información sobre este punto recomendamos la lectura de los informes de la Fundación Vía Libre "Protección legal de datos personales inferidos" (mayo 2023), "Gestión de datos personales por parte del Estado" (abril 2024) y "El Estado de los datos: del registro a la vigilancia" (junio 2026).

Propuesta: eliminar o acotar estrictamente los supuestos del art. 5 alternativos al consentimiento, específicamente los incisos d), i) y g) a condiciones de necesidad y proporcionalidad verificables, con intervención de la autoridad de control.

4. Consentimiento tácito (art. 11)

El proyecto admite el consentimiento tácito "siempre que surja de manera manifiesta del contexto de la relación" entre titular y responsable, exceptuando solo datos sensibles y de niños, niñas y adolescentes.

Es fundamental señalar dos cuestiones alarmantes de esta previsión: por un lado, que el consentimiento tácito traslada la carga de la autonomía informativa del titular al responsable, que es quien decide unilateralmente qué contexto "manifiesta" una autorización.

Por otro, que muchos de los datos que hoy alimentan perfiles e inferencias pueden no ser "sensibles" en sentido técnico, pero su tratamiento agregado sí resulta serlo en sus efectos. Así, la excepción prevista tampoco resulta suficiente.

Propuesta: eliminar la figura del consentimiento tácito como categoría general, manteniendo el estándar de consentimiento expreso.