# PROTECCIÓN DE DATOS Y SOBERANÍA INFORMÁTICA
## IMPACTOS DEL PROYECTO DE REFORMA SOBRE LA INDUSTRIA TECNOLÓGICA ARGENTINA Y LAS CAPACIDADES OPERATIVAS DEL ESTADO

-

Documento de trabajo elaborado por el Observatorio de Derecho Informático Argentino (O.D.I.A.).

Aportes para el debate legislativo sobre la reforma de la Ley de Protección de Datos Personales

### Resumen ejecutivo

La discusión sobre una nueva Ley de Protección de Datos Personales no puede agotarse en la privacidad. En una economía atravesada por servicios en la nube, inteligencia artificial y procesamiento masivo de información, las reglas que determinan quién puede tratar datos, para qué puede reutilizarlos y dónde puede procesarlos son también reglas sobre mercados, infraestructura y desarrollo tecnológico.

El proyecto actualmente bajo análisis avanza deliberadamente en esa dirección. Entre sus objetivos incluye la innovación y el desarrollo económico y amplía las posibilidades de utilización de datos para actividades como analítica, desarrollo de productos e inteligencia artificial. Al mismo tiempo, su artículo 19 reconoce expresamente como supuesto habilitante de una transferencia internacional la elección de infraestructura tecnológica situada fuera de la República Argentina, condicionándola esencialmente a que el proveedor garantice medidas técnicas de seguridad adecuadas.

Desde O.D.I.A. no sostenemos que el proyecto ordene o haga inevitable la extranjerización de la infraestructura informática argentina. Nuestra preocupación es diferente. El proyecto crea condiciones regulatorias que pueden facilitar y normalizar ese proceso sin establecer contrapesos equivalentes destinados a preservar competencia, reversibilidad, auditabilidad, capacidades tecnológicas nacionales y autonomía estatal. En un mercado internacional caracterizado por grandes economías de escala y una elevada concentración de infraestructura, una regulación formalmente neutral puede producir efectos materialmente asimétricos sobre las pequeñas y medianas empresas tecnológicas argentinas.

Cuando estas mismas reglas se proyectan sobre el sector público, el problema adquiere otra dimensión. El Estado puede continuar siendo formalmente responsable por sus bases de datos y, al mismo tiempo, perder progresivamente las capacidades materiales necesarias para almacenarlos, procesarlos, auditar los sistemas utilizados o sustituir a sus proveedores. La extranjerización de los datos puede significar pérdida de oportunidades económicas. La extranjerización de las capacidades necesarias para gobernarlos puede significar pérdida de soberanía.

### 1. Una ley de protección de datos también es una política tecnológica

La Argentina se encuentra frente a la posibilidad de modificar integralmente el régimen establecido por la Ley 25.326. El proyecto introduce cambios significativos en materia de bases de licitud, inteligencia artificial, transferencias internacionales, derechos de los titulares y obligaciones de quienes procesan información personal.

Buena parte de la discusión sobre una reforma de estas características se concentra, razonablemente, en los derechos de las personas. Consentimiento, acceso, rectificación, supresión, seguridad, perfilamiento o tratamiento de información sensible siguen constituyendo dimensiones centrales de cualquier legislación de protección de datos. Sin embargo, limitar el análisis a esos aspectos supone observar sólo una parte del fenómeno.

*Las leyes de protección de datos no regulan únicamente privacidad. También regulan mercados, infraestructura y capacidad tecnológica.*

El propio proyecto reconoce esta dimensión cuando incorpora entre sus finalidades la promoción del uso responsable de la información, la innovación y el desarrollo económico. Si la futura ley pretende producir efectos sobre estas materias, resulta legítimo preguntarse qué tipo de innovación promueve, qué actores se encuentran en mejores condiciones para aprovechar las nuevas reglas, dónde se desarrollará la infraestructura necesaria para hacerlo y qué capacidades tecnológicas permanecerán en nuestro país.

Los datos personales se han convertido en un insumo indispensable para actividades que abarcan desde la publicidad y el comercio hasta la prestación de servicios financieros, la investigación científica, el desarrollo de software y el entrenamiento de sistemas de inteligencia artificial.

Regular sus condiciones de utilización implica entonces intervenir también sobre la actividad informática que se desarrolla alrededor de ellos.

Desde el Observatorio de Derecho Informático Argentino entendemos que esta dimensión debe formar parte del debate parlamentario. El proyecto, tal como está formulado, puede contribuir a consolidar —y eventualmente esclerotizar— una estructura de dependencia respecto de infraestructura tecnológica controlada desde el exterior. Y cuando esa arquitectura regulatoria se proyecta sobre el Estado puede crear las condiciones para un fenómeno todavía más sensible: la extranjerización de capacidades necesarias para el ejercicio de funciones públicas.

Por ello este documento complementa las observaciones artículo por artículo elaboradas por O.D.I.A. Su pregunta es diferente. No busca determinar solamente si cada disposición protege adecuadamente los derechos de los titulares, sino qué modelo tecnológico, productivo y de soberanía informática contribuye a construir el proyecto en su conjunto.

## 2. Más allá de la privacidad. Los datos como insumo económico

Los datos personales tienen una característica singular. Surgen de actividades humanas —trabajar, desplazarse, consumir, estudiar, comunicarse, recibir atención médica— pero pueden convertirse posteriormente en insumos para producir conocimiento, realizar predicciones, desarrollar productos, entrenar sistemas automatizados y organizar mercados.

Nick Couldry y Ulises Mejías han propuesto la categoría de colonialismo de datos para describir el proceso mediante el cual dimensiones cada vez más amplias de la vida humana son convertidas en información susceptible de apropiación y explotación económica. El paralelismo que proponen con los procesos históricos de colonialismo se encuentra, precisamente, en la lógica de apropiación a gran escala de recursos de los cuales posteriormente puede extraerse valor.

No es necesario adoptar íntegramente esa construcción teórica para advertir el problema que pone de manifiesto.

El dato no constituye únicamente un objeto respecto del cual una persona posee derechos. En la economía digital es también un insumo productivo.

Y ese insumo no posee valor económico de manera espontánea. Para convertirlo en conocimiento, predicción o producto es necesario recolectarlo, transportarlo, almacenarlo, combinarlo y procesarlo. Eso requiere centros de datos, capacidad de cómputo, redes, software, modelos, energía y conocimiento técnico.

Couldry y Mejías insisten por ello en que los datos no pueden pensarse separadamente de las infraestructuras a las cuales fluyen y mediante las cuales son procesados. En ese nuevo orden, sostienen, convergen crecientemente el poder económico —la posibilidad de producir valor— y el poder cognitivo —la capacidad de producir conocimiento sobre el mundo—.

Esta observación plantea una pregunta especialmente importante para países como la Argentina.

*¿Qué ocurre cuando una sociedad genera los datos pero no controla las infraestructuras mediante las cuales se obtiene valor de ellos?*

Los datos pueden originarse en nuestro territorio mientras su almacenamiento, procesamiento y transformación en nuevos productos ocurre fuera de él. Una empresa argentina puede producir información sobre sus operaciones que es almacenada en una nube extranjera, procesada mediante herramientas desarrolladas en el exterior y utilizada posteriormente por servicios o modelos que forman parte del ecosistema de ese mismo proveedor.

La Argentina puede entonces participar activamente de la economía de los datos y, sin embargo, quedar ubicada en uno de los extremos de menor valor agregado de esa cadena: generadora de información y consumidora de tecnologías desarrolladas alrededor de ella.

En ese sentido utilizamos en este documento la idea de extractivismo de datos. No porque los datos sean equivalentes a petróleo, litio o cualquier otro recurso natural, sino porque resulta posible identificar relaciones económicas en las que el lugar de generación de un insumo, el lugar donde se lo procesa y el lugar donde se captura el valor producido a partir de él son diferentes.

La legislación de protección de datos no puede resolver por sí sola esa desigualdad. Pero tampoco es neutral frente a ella.

## 3. Los datos no flotan en la nube

Una de las razones por las cuales esta dimensión económica suele pasar inadvertida reside en una metáfora extraordinariamente eficaz: la nube.

Los datos, sin embargo, no flotan. Detrás de aquello que denominamos nube existen centros de datos, procesadores, redes, sistemas operativos, cables, software, claves, contratos y cadenas de subcontratación. Existen además empresas concretas que administran esas tecnologías y Estados cuyas normas pueden imponerles obligaciones.

De allí que la pregunta por la soberanía informática no pueda reducirse simplemente al lugar físico en el que se encuentra un servidor.

Un equipo puede estar ubicado en territorio argentino y depender completamente de software, licencias, actualizaciones, credenciales o servicios controlados desde el exterior. A la inversa, la utilización de infraestructura internacional tampoco determina automáticamente una pérdida de soberanía.

Tampoco el problema coincide necesariamente con la nacionalidad de la empresa contratada. Una PYME argentina puede prestar un servicio construido sobre infraestructura de un proveedor global, mientras una compañía extranjera podría operar determinados recursos físicamente instalados en nuestro país.La cuestión relevante es, por ello, el control efectivo sobre las capas críticas de la infraestructura.

Desde O.D.I.A. proponemos entender la soberanía informática como la capacidad efectiva de un Estado para decidir, auditar, sustituir y continuar operando las infraestructuras tecnológicas de las cuales depende.

Esos cuatro verbos permiten traducir una categoría generalmente abstracta en preguntas concretas.¿Es posible cambiar de proveedor? ¿Los datos pueden ser recuperados en formatos interoperables? ¿Puede auditarse el funcionamiento del sistema? ¿Quién administra las credenciales y claves críticas? ¿Se conoce la cadena de subcontratación? ¿Existe documentación suficiente para migrar? ¿El Estado o la organización conservarían capacidad de continuar prestando el servicio si finalizara la relación contractual?

Cuando esas posibilidades disminuyen aparece lo que la industria conoce como vendor lock-in: una dependencia respecto de determinado proveedor o ecosistema cuya sustitución se vuelve técnica, económica u organizacionalmente demasiado costosa.

El riesgo puede seguir una secuencia reconocible:

*facilitación normativa → externalización de infraestructura → integración con servicios pertenecientes al mismo ecosistema → incremento de los costos de migración → dependencia tecnológica.*

No se trata de una consecuencia inevitable. Es una trayectoria posible que una política regulatoria debería procurar prevenir.

## 4. ¿Qué dirección regulatoria adopta el proyecto?

El proyecto no obliga a contratar infraestructura extranjera. Tampoco obliga a transferir datos fuera de la Argentina. Sería incorrecto atribuirle esos efectos. Lo relevante es observar los incentivos que produce la regulación considerada como conjunto.

El proyecto amplía las posibilidades de utilización económica de los datos. El artículo 5 reconoce expresamente dentro del interés legítimo actividades vinculadas con el desarrollo o mejora de productos y servicios, la analítica y el entrenamiento de sistemas de inteligencia artificial.

El artículo 13 contempla un régimen especial para datos seudonimizados que alcanza, entre otros supuestos, el desarrollo y entrenamiento de sistemas de inteligencia artificial. Y el artículo 17 establece específicamente condiciones para la utilización de datos personales en entrenamiento, desarrollo y evaluación de sistemas de IA.

Existe detrás de estas reglas una orientación reconocible: facilitar actividades tecnológicas intensivas en datos. Esa orientación no resulta necesariamente objetable. Puede promover innovación y reducir incertidumbre regulatoria. Pero una política que pretende generar esos efectos

debería preguntarse simultáneamente qué actores están en condiciones de aprovecharlos.

El punto se vuelve especialmente evidente al analizar el artículo 19. Después de regular diferentes mecanismos de transferencia internacional, el proyecto incorpora como supuesto autónomo aquel en que el responsable "elija infraestructura tecnológica ubicada fuera de la República Argentina", siempre que el proveedor garantice medidas técnicas de seguridad adecuadas.

La formulación produce un desplazamiento importante. La utilización de infraestructura extranjera queda evaluada esencialmente desde una lógica de seguridad de la información.Pero seguridad, jurisdicción, competencia y soberanía tecnológica responden a problemas diferentes.

Un proveedor puede cumplir estándares extraordinariamente elevados de ciberseguridad y, al mismo tiempo, generar dependencia respecto de tecnologías propietarias, estar sometido a jurisdicciones extranjeras o dificultar materialmente la migración hacia un proveedor alternativo.

La regulación propuesta no pondera expresamente ninguna de esas dimensiones. A esto se agrega otra característica del proyecto. En distintos artículos aparece una protección particularmente intensa de la propiedad intelectual y los secretos comerciales frente al acceso a información técnica. El artículo 25 establece que el derecho a revisión de una decisión automatizada no puede implicar "en ningún caso" la divulgación de algoritmos, modelos, ponderaciones o información técnica o comercial sensible; el artículo 28 admite incluso que el responsable rechace una solicitud cuando cumplirla revele necesariamente información comercial confidencial o secretos industriales.

El problema alcanza su máxima expresión en el artículo 43. Aunque habilita a la autoridad de control a realizar inspecciones y auditorías técnicas, establece que esa facultad no podrá implicar, "en ningún caso", acceso a código fuente, algoritmos, secretos comerciales o propiedad intelectual.

Esta combinación merece ser observada desde la perspectiva que proponemos.

Externalización y opacidad son problemas diferentes, pero pueden reforzarse mutuamente. La autonomía tecnológica no exige solamente poder contratar a quien se prefiera. Exige también poder controlar aquello que se contrata y poder sustituirlo.

## 5. Una ley de datos también determina quién puede hacer negocios con ellos

Este aspecto resulta especialmente importante para la industria informática argentina y, en particular, para sus pequeñas y medianas empresas.

Una empresa global de tecnología puede distribuir productos sobre una infraestructura que ya posee escala mundial. Cuenta con capacidad de cómputo amortizada entre millones de clientes, redes internacionales, servicios de almacenamiento, bases de datos administradas, herramientas de inteligencia artificial, sistemas de autenticación, analítica y múltiples productos integrados.

Una PYME argentina opera en condiciones diferentes. Esto resulta particularmente visible en el modelo Software as a Service (SaaS).La prestación de software ya no requiere necesariamente instalar una aplicación en equipos administrados por el cliente. Un proveedor puede ofrecer desde otro país un servicio completo cuya aplicación, almacenamiento, procesamiento, mantenimiento y actualización se realizan enteramente mediante infraestructura ubicada en el exterior. La habilitación regulatoria contenida en el artículo 19 disminuye una potencial fricción jurídica para ese tipo de prestación.

Esto no significa que la ley deba impedir el SaaS extranjero ni reservar mercados para empresas nacionales. Significa reconocer que la igualdad regulatoria formal entre actores que poseen capacidades radicalmente distintas no produce necesariamente condiciones competitivas equivalentes.

Una empresa argentina que desarrolla un buen producto puede no estar compitiendo solamente contra otro software. Puede estar compitiendo contra un ecosistema que combina aplicación, infraestructura, inteligencia artificial, almacenamiento, seguridad y capacidad financiera a escala global.

Por eso, una política regulatoria que reduce los costos jurídicos de importar capacidad informática debería preguntarse también qué condiciones existen para producir esa capacidad dentro del país.El problema es particularmente sensible porque la infraestructura puede funcionar como puerta de entrada hacia otras capas del mercado.

Una vez que los datos de una organización se encuentran alojados en determinado ecosistema, resulta frecuentemente más conveniente incorporar los servicios de base de datos, analítica, inteligencia artificial, seguridad, autenticación o automatización ofrecidos por el mismo proveedor.

La decisión inicial sobre infraestructura puede entonces condicionar decisiones posteriores sobre software y servicios. De tal modo, la extranjerización de infraestructura puede arrastrar la extranjerización de otras capas de la cadena tecnológica.

Esto no permite afirmar que el proyecto vaya necesariamente a provocar pérdida de mercado para las PYMEs argentinas; pero si permite sostener que puede modificar las condiciones regulatorias de competencia dentro de un mercado previamente caracterizado por enormes asimetrías de escala.

Y esa consecuencia debería ser evaluada si, como declara el propio proyecto, uno de los objetivos perseguidos es contribuir al desarrollo económico.

Portabilidad, interoperabilidad, estándares abiertos, reversibilidad y reducción del vendor lock-in no son únicamente cuestiones técnicas. También son instrumentos de política de competencia capaces de facilitar que proveedores pequeños ingresen a mercados que de otro modo pueden quedar cerrados alrededor de ecosistemas tecnológicos verticalmente integrados.

## 6. Cuando el Estado externaliza datos puede externalizar también capacidades

Hasta aquí el problema puede plantearse fundamentalmente en términos de estructura económica, competencia y desarrollo tecnológico. Sin embargo, cuando quien externaliza infraestructura es el Estado, la naturaleza de la discusión cambia.

La Administración Pública depende crecientemente de sistemas informáticos para recaudar impuestos, administrar prestaciones sociales, gestionar servicios sanitarios, identificar personas, organizar información educativa, controlar fronteras, investigar delitos, administrar recursos y ejecutar políticas públicas.

Esos sistemas ya no constituyen, en muchos casos, simples herramientas auxiliares sino que conforman parte de la capacidad operativa del Estado.

Por capacidades operativas entendemos aquí la combinación de infraestructura, recursos tecnológicos, conocimientos y posibilidades de decisión que permiten al Estado ejercer efectivamente las funciones que el ordenamiento jurídico le atribuye.

La distinción es importante. Un organismo puede conservar formalmente una competencia y, sin embargo, perder parte de la capacidad material necesaria para ejercerla autónomamente. También puede continuar siendo jurídicamente responsable por una base de datos y depender enteramente de un tercero para almacenarla, procesarla, interpretarla, modificar los sistemas asociados o recuperar su información.

El artículo 35 establece determinadas garantías respecto de las bases de datos públicas, incluyendo la obligación de identificar su finalidad, estructura, procedimientos de obtención y conservación y las transferencias o interconexiones previstas.Sin embargo, el proyecto no construye un régimen específico destinado a diferenciar aquellos tratamientos o infraestructuras cuya externalización pueda comprometer capacidades estratégicas del Estado.

Tampoco el artículo 19 distingue, con carácter general, entre la utilización de infraestructura extranjera por parte de una empresa privada y aquella destinada al tratamiento de información necesaria para el ejercicio de funciones públicas.

Desde nuestra perspectiva, existe allí una diferencia cualitativa. El riesgo no consiste únicamente en que un dato público sea almacenado fuera del territorio nacional. Un organismo puede desconocer aspectos relevantes de la arquitectura que utiliza; depender del proveedor para realizar modificaciones; carecer de personal capaz de operar el sistema; quedar condicionado por APIs, formatos o tecnologías propietarias; enfrentar costos prohibitivos para migrar; o perder capacidad para auditar efectivamente cómo determinadas herramientas procesan la información.

En ese escenario, la titularidad formal de los datos no garantiza autonomía real.La secuencia de riesgo que describíamos anteriormente puede adquirir entonces un último eslabón:

*dependencia tecnológica →*
*pérdida de autonomía operativa estatal.*

Éste es el punto donde la discusión sobre extractivismo, desarrollo productivo y protección de datos se convierte claramente en una discusión sobre soberanía. Un Estado que externaliza infraestructura no externaliza únicamente almacenamiento. Puede externalizar también capacidad para conocer, operar y decidir.

## 7. La soberanía informática también se decide en la contratación pública

La legislación de protección de datos no determina por sí sola cómo contratará tecnología el Estado, pero establece parte del marco dentro del cual esas contrataciones serán posibles.

La decisión concreta suele materializarse posteriormente en un lugar mucho menos visible que el debate legislativo: el expediente de contratación pública. Es allí donde se determina qué proveedor administrará el servicio, qué tecnologías utilizará, durante cuánto tiempo se mantendrá el contrato, qué información deberá entregar cuando finalice, qué posibilidades tendrá el organismo para auditarlo y cuánto costará migrar hacia otra solución.

Precio, calidad y seguridad son dimensiones imprescindibles de una contratación tecnológica. Sin embargo, para determinados sistemas estatales no deberían ser las únicas.

La contratación debería considerar desde su origen la posibilidad de salida. Reversibilidad, interoperabilidad, documentación, acceso a registros, administración de credenciales, jurisdicción, conocimiento de subcontratistas, transferencia de conocimiento y continuidad operativa pueden convertirse en requisitos tan importantes como la disponibilidad del servicio.

La capacidad de sustituir a un proveedor no debería comenzar a discutirse cuando el contrato está próximo a vencer sino que debería formar parte de su diseño.

Existe una fórmula sencilla para expresar esta idea: La soberanía informática no exige que el Estado haga todo por sí mismo. Exige que ninguna contratación lo coloque en una situación en la que ya no pueda hacerlo.

## 8. El Salvador como advertencia regional

La experiencia de El Salvador constituye un ejemplo particularmente útil para observar cómo decisiones sobre infraestructura, contratación pública y capacidades estatales pueden terminar integrándose dentro de una misma arquitectura jurídica.

En septiembre de 2023 la Asamblea Legislativa sancionó el Decreto 840, Ley General para la Modernización Digital del Estado. La propia norma señala que el Gobierno salvadoreño había celebrado una alianza estratégica con Google LLC para impulsar su transformación digital y define a Google y determinadas entidades vinculadas como “Socio Estratégico”.

La legislación no se limitó a establecer objetivos generales de digitalización. Creó un régimen destinado específicamente a instrumentar esa alianza. En su artículo 8 estableció un procedimiento administrativo específico para la contratación de los servicios del socio estratégico y que el artículo 14 excluyó esas adquisiciones de la Ley de Compras Públicas. Asimismo, la propia ley contempló además asignaciones presupuestarias agregadas de al menos 500 millones de dólares para los servicios vinculados con la alianza.

La relevancia del caso no es meramente hipotética. Con posterioridad, servicios estatales concretos comenzaron a apoyarse en ese ecosistema tecnológico. Google describe, por ejemplo, la utilización de su infraestructura en la plataforma nacional de salud digital DoctorSV y en la modernización del sistema de facturación electrónica del Ministerio de Hacienda salvadoreño.

El caso salvadoreño es sustancialmente distinto del proyecto argentino. La iniciativa que analizamos no selecciona a un proveedor determinado, no celebra una alianza estratégica con una empresa y no crea una excepción a nuestro régimen general de contratación pública.Precisamente por eso el ejemplo resulta útil.

Si bienal caso no es presentado como una predicción sobre lo que necesariamente sucederá en la Argentina, sino como advertencia sobre la relación entre reglas de datos, decisiones de infraestructura y contratación pública.

Una decisión inicialmente presentada como una opción tecnológica puede transformarse posteriormente en contratos de largo plazo, integración creciente de servicios y dependencia de un determinado ecosistema el cual se inscribe en realidades geo política específicas.

Una ley puede no disponer la extranjerización de las capacidades estatales y, sin embargo, contribuir a generar las condiciones jurídicas para que decisiones administrativas posteriores avancen en esa dirección.Por ello entendemos que el debate debe darse antes de que esas dependencias se encuentren consolidadas.

## 9. Soberanía informática no significa aislamiento

Plantear estas preocupaciones no supone proponer una política de autarquía tecnológica.La Argentina no puede ni necesita desarrollar internamente todos los componentes tecnológicos que utiliza. Los proveedores internacionales pueden aportar escala, innovación, seguridad y servicios que sería extremadamente costoso reproducir localmente.

Tampoco sostenemos que todos los datos deban necesariamente permanecer físicamente dentro del territorio nacional. El problema no es la integración tecnológica internacional.El problema es, al menos en esta instancia, la dependencia sin capacidad de salida.

Una política de soberanía informática debe permitir distinguir entre aquello que razonablemente puede contratarse y aquello cuya externalización requiere salvaguardas adicionales.

Resulta necesario preservar la posibilidad de auditar, sustituir proveedores, migrar información y continuar operando al tiempo que también debe indagarse qué capacidades resulta razonable desarrollar dentro del país.

Esta mirada no es incompatible con la competencia. Por el contrario, reducir dependencias y promover interoperabilidad puede abrir mercados a actores más pequeños, facilitar el ingreso de nuevos proveedores y disminuir posiciones dominantes construidas alrededor de costos de salida artificialmente elevados.

La discusión tampoco debería reducirse a una oposición entre empresas argentinas y empresas extranjeras.Una política tecnológica sofisticada debe observar qué capas controla cada actor, dónde se captura el valor, qué capacidad conserva el cliente para migrar y qué conocimientos permanecen en el país.

En definitiva, la soberanía informática significa conservar capacidad de elección.

## 10. Una agenda legislativa para preservar capacidades

Desde O.D.I.A. consideramos que estas preocupaciones pueden traducirse en una agenda concreta para el tratamiento parlamentario del proyecto.

*1. Diferenciar los tratamientos privados de aquellos vinculados con funciones estatales estratégicas.*
El Congreso debería evaluar la incorporación de condiciones adicionales cuando organismos públicos pretendan utilizar infraestructura situada en el extranjero para sistemas vinculados con funciones críticas. No todos los tratamientos estatales requieren las mismas salvaguardas, pero tampoco parece adecuado aplicarles indiscriminadamente el mismo régimen que a una relación comercial ordinaria.

*2. Complementar el criterio de seguridad del artículo 19.*
La seguridad técnica es indispensable, pero para determinados tratamientos deberían considerarse además jurisdicción, reversibilidad, interoperabilidad, auditabilidad, subcontratación y capacidad efectiva de migración. La elección de infraestructura extranjera no debería analizarse exclusivamente desde la posibilidad de proteger el dato frente a un incidente.

*3. Incorporar mecanismos destinados a reducir el vendor lock-in.*
La portabilidad entre proveedores, utilización de formatos interoperables, documentación adecuada y estrategias de salida pueden favorecer simultáneamente soberanía, competencia e innovación. Estas obligaciones adquieren especial importancia en contrataciones públicas de largo plazo.

*4. Preservar las facultades de auditoría.*
La propiedad intelectual y los secretos comerciales pueden justificar deberes de confidencialidad y mecanismos de acceso restringido. No deberían convertirse en barreras absolutas que impidan a la autoridad de control o a los órganos judiciales conocer información técnica indispensable para fiscalizar un sistema. La prohibición absoluta prevista en el artículo 43 merece ser reconsiderada.

*5. Exigir evaluaciones previas de dependencia tecnológica para determinadas contrataciones estatales.*
Así como determinados tratamientos requieren evaluar riesgos para derechos personales, los sistemas públicos estratégicos deberían considerar también riesgos de continuidad, migración, concentración y pérdida de capacidades operativas.

*6. Incorporar el impacto productivo al debate sobre innovación.*
Si el proyecto pretende promover desarrollo económico, resulta razonable evaluar qué efectos tendrán sus reglas sobre las PYMEs tecnológicas argentinas y sobre las posibilidades de desarrollar localmente software, infraestructura, ciberseguridad, auditoría y servicios asociados. Esto no exige establecer mercados cautivos ni impedir la competencia extranjera, sino evitar que el diseño regulatorio ignore las asimetrías estructurales existentes.

*7. Utilizar la contratación pública para conservar conocimiento y capacidad estatal.*
En los sistemas relevantes deberían contemplarse cláusulas de transferencia de conocimiento, documentación, gestión de credenciales, reversibilidad y continuidad operativa. Tercerizar la prestación de un servicio no debería significar tercerizar íntegramente la posibilidad de comprenderlo y gobernarlo.

Esta agenda no sustituye las observaciones específicas sobre

el articulado sino que las complementa.Una vez que se reconoce que la regulación de datos también produce efectos sobre mercados e infraestructuras, esas consecuencias pasan a formar parte legítima del análisis legislativo.

## 11. Conclusión. Una discusión sobre datos es también una discusión sobre capacidades

La Argentina necesita discutir la actualización de su régimen de protección de datos personales.Pero modernizar una legislación no significa simplemente adaptarla a tecnologías y modelos de negocios que ya existen. Significa también decidir qué relación pretende construir el país con esas tecnologías y qué capacidades quiere conservar frente a ellas.

El proyecto actualmente analizado facilita nuevos usos económicos de los datos y procura generar condiciones favorables para la innovación. Esa decisión puede ofrecer oportunidades relevantes.

Pero la innovación no ocurre en un vacío. Tiene lugar en un escenario geo político particular y un mercado internacional profundamente concentrado, en el cual un número reducido de empresas controla proporciones relevantes de la infraestructura, el cómputo y los servicios necesarios para transformar datos en nuevos productos.

Una norma que facilita la utilización de infraestructura externa sin incorporar contrapesos sobre interoperabilidad, reversibilidad, dependencia y capacidad de auditoría puede contribuir a consolidar esa estructura. Esto importa para las empresas argentinas que desarrollan software.

Importa para las PYMEs que pretenden competir contra servicios ofrecidos globalmente bajo modelos SaaS. Importa para decidir si el crecimiento de las actividades intensivas en datos desarrollará nuevas capacidades tecnológicas dentro del país o incrementará fundamentalmente el consumo de capacidades producidas fuera de él.

Y cuando quien contrata esos servicios es el Estado, importa todavía más.Un Estado puede conservar formalmente la responsabilidad sobre sus bases y perder materialmente la capacidad para gobernar las tecnologías mediante las cuales las administra.

Una dependencia públicapuede mantener la competencia jurídica pero perder la capacidad y autonomía operativa. Puede ser responsable por los resultados de un sistema que ya no posee capacidad suficiente para auditar, modificar o reemplazar.

Desde O.D.I.A. entendemos que la protección de los derechos personales y la soberanía informática no constituyen agendas contrapuestas. Son dimensiones diferentes de una misma pregunta sobre cómo se distribuye el poder en una sociedad crecientemente organizada alrededor de datos e infraestructura tecnológica.

La discusión parlamentaria ofrece una oportunidad para evitar que la Argentina se limite a adaptar su legislación a una economía digital cuya arquitectura material ya viene determinada desde otros centros. Una nueva ley puede proteger los derechos de las personas y, al mismo tiempo, fomentar competencia, preservar la posibilidad de desarrollar empresas tecnológicas nacionales y establecer garantías específicas para que la transformación digital del Estado no derive en dependencia estructural.

Ya no alcanza con preguntarnos quién puede utilizar nuestros datos. Debemos preguntarnos tambien quién controla la infraestructura mediante la cual esos datos se convierten en conocimiento, dónde se captura el valor producido a partir de ellos y qué capacidades conservará la Argentina para gobernar sus propios sistemas de información.

La extranjerización de los datos implica una pérdida de oportunidades económicas para el desarrollo de nuestro país. Sin embargo, la extranjerización de las capacidades necesarias para gobernarlos y utilizarlos implica una cesión de soberanía y la consolidación de un grado inédito de dependencia técnico-política. En la era digital, las fronteras de la soberanía también atraviesan los datos, los servidores y las infraestructuras que los vuelven inteligibles. Allí donde un Estado pierde la capacidad de gobernarlos, comienza también a perder la capacidad de decidir por sí mismo.

*Observatorio de Derecho Informático Argentino (O.D.I.A.) — Documento de trabajo elaborado como aporte al debate legislativo sobre la reforma de la Ley de Protección de Datos Personales. Ciudad Autónoma de Buenos Aires, agosto de 2026.*