

PROYECTO DE RESOLUCIÓN

Solicitar al Poder Ejecutivo Nacional que, a través de la Jefatura de Gabinete de Ministros, la Secretaría de Innovación, Ciencia y Tecnología, la Agencia de Acceso a la Información Pública y demás organismos competentes, informe de manera detallada, precisa y por escrito, respecto de las políticas, contratos, criterios técnicos y mecanismos de seguridad vinculados con el almacenamiento, procesamiento, gestión y transferencia de datos y sistemas del Estado Nacional mediante servicios de computación en la nube provistos por empresas privadas, nacionales o extranjeras, y en particular respecto de los siguientes puntos:

1. Contratos y servicios de computación en la nube:

- a) Nómina detallada de los convenios marco, contratos, licitaciones, órdenes de compra, acuerdos de colaboración y demás instrumentos vigentes celebrados entre organismos de la Administración Pública Nacional y proveedores de servicios de computación en la nube, incluyendo, entre otros, servicios provistos por Amazon Web Services, Google Cloud, Microsoft Azure y otros proveedores nacionales o internacionales.
- b) Montos comprometidos y efectivamente ejecutados, moneda de contratación y de pago, plazos de vigencia, mecanismos de actualización de precios y partidas presupuestarias afectadas.
- c) Detalle de los servicios contratados, especificando, cuando corresponda, capacidad de almacenamiento, procesamiento, bases de datos, redes, servicios de respaldo, servicios de seguridad, herramientas de analítica, inteligencia artificial y demás servicios asociados.
- d) Criterios técnicos, económicos, de seguridad, interoperabilidad y continuidad operativa utilizados para determinar la conveniencia de contratar servicios de proveedores externos frente a alternativas basadas en infraestructura propia, infraestructura estatal, proveedores nacionales o esquemas híbridos.

2. Inventario de datos, sistemas y servicios críticos

- a) Detalle de las bases de datos, registros oficiales, aplicaciones, sistemas y servicios públicos que hayan sido migrados, se encuentren en proceso de migración o se proyecten migrar hacia infraestructuras de computación en la nube de terceros.
- b) Clasificación de la información alojada o procesada en dichas infraestructuras de acuerdo con su nivel de sensibilidad, criticidad y confidencialidad, especialmente en aquellos casos que involucren datos personales, fiscales, previsionales, sanitarios, biométricos, de identidad, de seguridad o información estratégica del Estado.
- c) Identificación de los sistemas y servicios cuya interrupción pudiera afectar significativamente el funcionamiento de organismos públicos, la prestación de servicios esenciales o el ejercicio de derechos por parte de la ciudadanía.
- d) Informe qué mecanismos existen para garantizar que la migración a servicios de terceros no implique una pérdida de control institucional sobre los datos, sistemas y procesos críticos del Estado.

3. Soberanía, jurisdicción y localización de los datos

- a) Informe sobre la localización geográfica de los centros de procesamiento y almacenamiento utilizados para alojar o procesar información del Estado Nacional, indicando, cuando corresponda, país y jurisdicción en los que se encuentran radicados.
- b) Informe qué mecanismos técnicos y contractuales garantizan que el Estado conserve el control sobre sus datos, incluyendo la administración de las claves criptográficas, políticas de acceso, autenticación, registros de actividad y mecanismos de auditoría.
- c) Informe sobre las jurisdicciones extranjeras a las que se encuentran sujetos los proveedores contratados y sobre las normas de otros Estados que pudieran resultar aplicables a dichos proveedores en virtud de su legislación nacional.
- d) Informe qué análisis jurídicos y de riesgo se realizaron respecto de eventuales requerimientos de acceso a información por parte de autoridades extranjeras, incluyendo aquellos derivados de normas de alcance extraterritorial, y qué mecanismos contractuales y técnicos existen para proteger los derechos, intereses y competencias jurisdiccionales de la República Argentina.
- e) Informe si los contratos vigentes establecen obligaciones específicas respecto de la localización, transferencia internacional, acceso, conservación, eliminación y restitución de los datos pertenecientes al Estado Nacional.

4. Protección de datos personales y seguridad de la información

- a) Informe los mecanismos de auditoría y control implementados para garantizar el cumplimiento de la Ley N.º 25.326 de Protección de los Datos Personales y demás normativa aplicable, así como de las disposiciones y criterios establecidos por la Agencia de Acceso a la Información Pública.
- b) Informe los protocolos de ciberseguridad aplicables a los servicios contratados, incluyendo mecanismos de cifrado, gestión de identidades y accesos, monitoreo, registro de actividades, detección de incidentes, copias de respaldo y recuperación ante desastres.
- c) Informe los procedimientos establecidos para la notificación, gestión y mitigación de incidentes de seguridad que pudieran afectar información o servicios del Estado Nacional.
- d) Informe qué mecanismos de auditoría independiente existen para verificar el cumplimiento de las obligaciones de seguridad, confidencialidad y protección de datos por parte de los proveedores.
- e) Informe los protocolos previstos ante la rescisión, vencimiento o interrupción de los contratos, incluyendo los procedimientos para la devolución, migración, eliminación y certificación de eliminación de los datos.

5. Dependencia tecnológica, interoperabilidad y portabilidad

- a) Informe qué organismos y sistemas del Estado Nacional presentan actualmente dependencia tecnológica significativa respecto de un proveedor determinado de servicios de nube.
- b) Informe qué mecanismos de interoperabilidad y estándares abiertos se utilizan para evitar situaciones de dependencia tecnológica o *vendor lock-in* que dificulten la migración de datos, aplicaciones y servicios hacia otros proveedores o hacia infraestructura estatal.
- c) Informe qué porcentaje de las cargas de trabajo actualmente alojadas en servicios de terceros puede ser migrado a otra infraestructura sin modificaciones sustanciales de arquitectura, software o datos.

d) Informe si los contratos incluyen cláusulas específicas de portabilidad de datos, interoperabilidad, reversibilidad y asistencia para la migración al finalizar la relación contractual.

e) Informe qué evaluaciones de riesgo se realizan respecto de la concentración de servicios críticos en un reducido número de proveedores tecnológicos.

6. Infraestructura pública y capacidades tecnológicas nacionales

a) Informe los criterios técnicos y económicos utilizados para determinar la utilización de infraestructura propia del Estado, infraestructura de ARSAT S.A., servicios de proveedores nacionales, servicios de proveedores internacionales y esquemas de nube híbrida.

b) Informe el estado actual de la capacidad operativa, de almacenamiento, procesamiento, conectividad y seguridad del Centro Nacional de Datos de ARSAT S.A., incluyendo su nivel de utilización por organismos del Estado Nacional.

c) Informe las inversiones realizadas y proyectadas para ampliar, actualizar y fortalecer las capacidades de infraestructura digital estatal, incluyendo las correspondientes a ARSAT S.A.

d) Informe qué servicios tecnológicos críticos se considera estratégico mantener bajo control, administración o capacidad de supervisión directa del Estado Nacional.

e) Informe si existe una estrategia nacional de infraestructura de nube gubernamental o de utilización coordinada de capacidades estatales y privadas, indicando sus objetivos, organismos responsables y horizonte temporal.

7. Industria nacional y desarrollo de capacidades tecnológicas

a) Informe las políticas implementadas para promover la participación de empresas nacionales, PyMEs, cooperativas y universidades en la provisión, desarrollo, mantenimiento y evolución de infraestructura y servicios tecnológicos destinados al Estado Nacional.

b) Informe las evaluaciones de impacto económico y tecnológico realizadas respecto de la contratación de servicios de proveedores extranjeros, incluyendo sus efectos sobre el sector nacional de software, servicios informáticos, infraestructura tecnológica y empleo calificado.

c) Informe qué mecanismos de contratación, cuando resulte técnica y jurídicamente viable, favorecen el desarrollo de capacidades tecnológicas nacionales y la generación de conocimiento y empleo de alto valor agregado.

d) Informe qué políticas se encuentran vigentes para evitar que la contratación de servicios tecnológicos públicos genere una pérdida progresiva de capacidades internas del Estado y del ecosistema tecnológico nacional.

8. Inteligencia artificial y utilización de datos públicos

a) Informe si organismos de la Administración Pública Nacional utilizan servicios de inteligencia artificial, aprendizaje automático o modelos fundacionales provistos por empresas privadas de servicios en la nube. En caso afirmativo, detalle qué categorías de información son procesadas mediante dichos servicios y qué mecanismos existen para garantizar que los datos estatales no sean utilizados para finalidades distintas de aquellas expresamente autorizadas.

b) Informe si los contratos con proveedores de servicios de nube contemplan disposiciones específicas respecto de la utilización de datos, *prompts*, metadatos, registros de interacción y demás información generada mediante servicios de inteligencia artificial.

c) Informe qué criterios de seguridad, privacidad, trazabilidad, explicabilidad, supervisión humana y soberanía tecnológica se aplican a la incorporación de servicios de inteligencia artificial en organismos públicos.

9. Estrategia nacional de soberanía tecnológica

a) Informe si el Poder Ejecutivo Nacional cuenta con una estrategia integral de soberanía tecnológica y digital aplicable a la Administración Pública Nacional y, en caso afirmativo, detalle sus objetivos, instrumentos, organismos responsables e indicadores de cumplimiento.

b) Informe qué criterios se utilizan para determinar cuáles datos, sistemas, infraestructuras y capacidades tecnológicas deben considerarse estratégicos para la seguridad, autonomía y funcionamiento del Estado Nacional.

c) Informe qué medidas se encuentran previstas para garantizar que la utilización de servicios tecnológicos privados resulte compatible con la protección de los datos de la ciudadanía, la continuidad de los servicios públicos, la seguridad nacional, la autonomía decisoria del Estado y el desarrollo de capacidades tecnológicas nacionales.

d) Informe si se encuentra prevista la elaboración de una política de nube gubernamental que contemple criterios de soberanía, seguridad, interoperabilidad, portabilidad, eficiencia económica y fortalecimiento de las capacidades tecnológicas nacionales.

Diputado Nicolás Trotta.-

FUNDAMENTOS

Señor Presidente:

La transformación digital del Estado ha convertido a los datos, las infraestructuras tecnológicas y las capacidades de procesamiento en activos estratégicos para el funcionamiento de las instituciones públicas y para el ejercicio de derechos por parte de la ciudadanía.

En este contexto, la utilización de servicios de computación en la nube constituye una herramienta tecnológica de enorme relevancia para mejorar la capacidad de almacenamiento, procesamiento, escalabilidad y prestación de servicios digitales del Estado. Sin embargo, su incorporación no puede ser analizada exclusivamente desde una perspectiva de eficiencia o reducción de costos. La contratación de infraestructura y servicios tecnológicos externos también plantea interrogantes vinculados con la protección de los datos personales, la seguridad de la información, la continuidad operativa, la jurisdicción aplicable, la interoperabilidad, la portabilidad y la autonomía tecnológica del Estado.

La cuestión adquiere especial relevancia cuando se trata de información perteneciente al Estado Nacional y, particularmente, de datos personales y sensibles de millones de ciudadanos y ciudadanas. La administración pública tiene la responsabilidad de garantizar que dichos datos sean tratados conforme al marco jurídico argentino, bajo condiciones adecuadas de seguridad, confidencialidad, trazabilidad y control institucional.

La contratación de servicios de empresas tecnológicas transnacionales no constituye, por sí misma, una vulneración de la soberanía nacional. Sin embargo, la creciente concentración mundial de infraestructura y servicios digitales plantea riesgos que deben ser identificados, evaluados y gestionados por el Estado. Entre ellos se encuentran la dependencia respecto de proveedores específicos, las dificultades para migrar datos y aplicaciones, la concentración de servicios críticos, la eventual aplicación de legislaciones extranjeras y la pérdida progresiva de capacidades tecnológicas propias.

En este sentido, la soberanía tecnológica no debe ser entendida como el aislamiento del Estado respecto del ecosistema tecnológico global, sino como la capacidad efectiva de la República Argentina para tomar decisiones autónomas sobre sus datos, infraestructuras y sistemas críticos, establecer reglas para los proveedores privados, garantizar la continuidad de los servicios públicos y contar con alternativas tecnológicas viables.

Un aspecto central de esta discusión es la jurisdicción a la que se encuentran sometidos los proveedores tecnológicos. Determinadas legislaciones extranjeras pueden imponer obligaciones a empresas sujetas a su jurisdicción aun cuando la información objeto de un requerimiento se encuentre físicamente almacenada fuera del territorio de ese Estado. El denominado CLOUD Act de los Estados Unidos constituye uno de los ejemplos más relevantes de este fenómeno y justifica que el Estado argentino evalúe adecuadamente sus implicancias jurídicas y de seguridad antes de alojar información estratégica en infraestructuras sometidas a jurisdicciones extranjeras.

La discusión tampoco puede reducirse a la ubicación física de los servidores. Resulta necesario conocer quién administra las claves de cifrado, quién posee capacidad efectiva de acceso, qué mecanismos de auditoría existen, qué ocurre ante un incidente de seguridad y qué posibilidades tiene el Estado de recuperar y migrar sus datos ante la finalización de un contrato.

La dependencia tecnológica constituye, en este sentido, una cuestión fundamental a considerar en materia de soberanía digital. Un Estado puede conservar formalmente la titularidad de sus datos y, al mismo tiempo, encontrarse en una situación de dependencia crítica si sus sistemas fueron

diseñados de manera tal que resulta técnica o económicamente inviable migrarlos a otra infraestructura.

Por ello, la interoperabilidad, los estándares abiertos, la portabilidad de los datos y las cláusulas de reversibilidad contractual deben constituir elementos centrales de cualquier política pública de infraestructura digital.

Asimismo, la Argentina cuenta con capacidades tecnológicas estatales que deben ser consideradas dentro de una estrategia integral. ARSAT S.A. constituye una infraestructura estratégica construida a partir de una política de desarrollo tecnológico nacional. Su capacidad en materia de centros de datos, conectividad y servicios tecnológicos debe ser evaluada de manera objetiva y comparada con las alternativas disponibles en términos de costos, seguridad, capacidad, escalabilidad y continuidad operativa.

El objetivo no debe ser establecer una oposición simplista entre infraestructura estatal y proveedores privados. El desafío consiste en construir una arquitectura tecnológica en la que el Estado conserve capacidad de decisión y alternativas efectivas, evitando dependencias irreversibles y aprovechando, cuando corresponda, las capacidades del sector privado, de las empresas nacionales, de las universidades, del sistema científico-tecnológico y de las empresas y sociedades estatales.

Esta cuestión adquiere una nueva dimensión con la expansión de la inteligencia artificial. Los grandes proveedores de servicios en la nube se han convertido progresivamente en actores centrales no solo de la infraestructura digital, sino también del acceso a capacidades de inteligencia artificial. En consecuencia, las decisiones actuales sobre almacenamiento, procesamiento, infraestructura y contratación tecnológica pueden condicionar la capacidad futura del Estado argentino para desarrollar y utilizar sistemas de inteligencia artificial.

El Estado debe garantizar que los datos públicos utilizados en sistemas de inteligencia artificial se encuentren protegidos, que su utilización tenga una finalidad legítima y determinada, que no sean empleados para fines distintos de los autorizados y que existan mecanismos adecuados de supervisión, trazabilidad y seguridad.

La soberanía tecnológica también implica fortalecer el ecosistema productivo nacional. La contratación pública representa una herramienta de política de desarrollo capaz de generar demanda para empresas nacionales, PyMEs tecnológicas, universidades y centros de investigación, contribuyendo a la creación de capacidades, conocimiento y empleo de alto valor agregado.

La Argentina no puede limitarse a ser un consumidor pasivo de tecnologías desarrolladas y controladas por actores concentrados a nivel global. Una política tecnológica de Estado debe procurar que la transformación digital de la Administración Pública contribuya simultáneamente a mejorar los servicios que recibe la ciudadanía y a fortalecer las capacidades tecnológicas, científicas y productivas del país.

La cuestión, por lo tanto, no consiste en elegir entre Estado o mercado, ni entre infraestructura pública o privada. Se trata de garantizar que el Estado argentino tenga la capacidad institucional, tecnológica y jurídica necesaria para decidir cuándo, cómo y bajo qué condiciones utiliza cada alternativa.

Una política de soberanía tecnológica moderna debe combinar innovación y regulación, infraestructura pública y participación privada, capacidades nacionales e integración internacional, eficiencia y seguridad. Sobre todo, debe evitar que decisiones tecnológicas adoptadas en el

presente generen dependencias estructurales que condicionen las capacidades de decisión del Estado en el futuro.

Por todo lo expuesto, resulta necesario que el Poder Ejecutivo Nacional informe al Congreso de la Nación sobre las condiciones en las que se están almacenando, procesando y gestionando datos y sistemas estatales mediante servicios de computación en la nube, los riesgos asociados, los mecanismos de protección implementados, las condiciones contractuales vigentes, las alternativas disponibles y las políticas destinadas a preservar y fortalecer las capacidades tecnológicas soberanas de la República Argentina.

Por los motivos expuestos, solicito a mis pares el acompañamiento del presente proyecto de resolución.

Diputado Nicolás Trotta.-