AMNISTÍA INTERNACIONAL

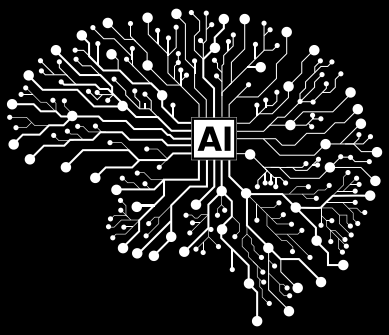
CASO PALANTIR EN ARGENTINA

Puntos principales ..... pág. 2

Hallazgos y recomendaciones ..... pág. 3–8

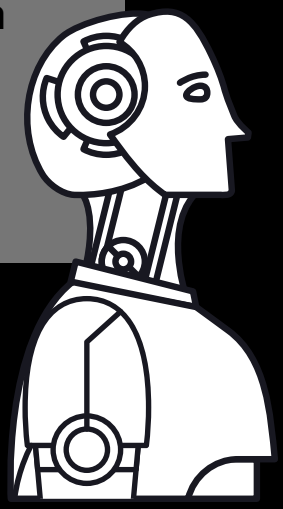
CASO PALANTIR
EN ARGENTINA

PUNTOS PRINCIPALES



Palantir es una empresa estadounidense de análisis de datos e inteligencia artificial que desarrolla sistemas usados por gobiernos y organizaciones para integrar información, generar perfiles y apoyar decisiones en áreas sensibles como seguridad, inteligencia, defensa, migración y salud, con posibles impactos directos sobre derechos fundamentales.

Genera preocupación porque sus sistemas permiten cruzar y analizar datos sensibles para apoyar decisiones estatales en áreas como seguridad y migración, lo que puede aumentar riesgos de vigilancia, perfilamiento, detenciones, deportaciones y otras afectaciones a derechos humanos.



La preocupación no es exclusiva de Argentina ni responde a una reacción local: **forma parte de un debate internacional** cada vez más intenso sobre los límites al uso de tecnologías de análisis masivo de datos en áreas sensibles. Cuando una herramienta permite reunir información dispersa, generar perfiles o producir alertas sobre personas o grupos, **puede profundizar sesgos, reforzar dinámicas discriminatorias y afectar de manera desproporcionada a quienes ya se encuentran en situaciones de vulnerabilidad o estigmatización.**

SE RECOMIENDA AL PODER EJECUTIVO:

- Transparentar cualquier vínculo con Palantir u otras tecnologías de vigilancia.
- No avanzar sin debate público ni garantías de derechos humanos, y asegurar evaluaciones de impacto, auditorías independientes y mecanismos de control.
- Al Congreso, se le solicita ejercer control político y actualizar la regulación sobre datos personales y vigilancia estatal.

AMNISTÍA INTERNACIONAL

CASO PALANTIR EN ARGENTINA

Tecnologías de vigilancia, seguridad y datos personales:

1. ¿QUÉ SE SABE SOBRE EL VÍNCULO ENTRE PALANTIR Y EL GOBIERNO ARGENTINO?

El presidente Javier Milei se reunió con Peter Thiel, cofundador de Palantir, el pasado 23 de abril. Según la información pública disponible, fue la tercera reunión documentada entre ambos desde el inicio de la actual gestión. La reiteración de estos encuentros no puede leerse como un hecho aislado. Configura una relación sostenida con uno de los proveedores globales más influyentes —y más cuestionados— de tecnologías de inteligencia y análisis masivo de datos para gobiernos. En un contexto en el que el Estado argentino está expandiendo activamente sus capacidades de vigilancia, la naturaleza, alcance y propósito de ese vínculo merecen máxima transparencia. **Hasta la fecha, no se ha hecho pública información sustantiva sobre los temas tratados, eventuales acuerdos de cooperación, pruebas piloto, transferencia de datos o provisión de servicios.**

2. ¿QUÉ ES PALANTIR Y POR QUÉ ES RELEVANTE?

Palantir Technologies es una empresa tecnológica estadounidense especializada en análisis masivo de datos, inteligencia artificial y sistemas de integración de información. A diferencia de otras empresas, no se limita a proveer software: desarrolla infraestructura de toma de decisiones que permite a gobiernos y organizaciones procesar grandes volúmenes de datos para seguridad, inteligencia, defensa y administración pública. Su relevancia radica en que opera en sectores altamente sensibles, donde sus herramientas pueden influir directamente en decisiones estatales que afectan derechos fundamentales. Los productos de Palantir han sido históricamente contratados por fuerzas de seguridad, servicios de inteligencia y agencias militares, y en los últimos años también se han expandido a otras áreas como la administración de la salud.

Algunos de sus principales productos incluyen Gotham (enfocado en defensa, inteligencia y seguridad), Foundry (gestión y análisis de datos para los sectores público y privado), Gaia (análisis geoespacial y operaciones en el campo de batalla) y Apollo / AIP – Artificial Intelligence Platform (infraestructura para desplegar modelos de IA en entornos gubernamentales y corporativos). Además, Palantir ha contribuido al desarrollo de sistemas para el control migratorio en Estados Unidos a partir de estos productos centrales, entre ellos ImmigrationOS y sistemas anteriores como Falcon.

Estos sistemas permiten consolidar información dispersa en distintas bases de datos estatales, cruzarla, generar perfiles de personas o grupos y producir inteligencia operativa para la toma de decisiones.

3. ¿POR QUÉ GENERA PREOCUPACIÓN?

La preocupación que genera no se explica solo por su sofisticación técnica, sino por el tipo de funciones que habilita:

- Cruza datos policiales, migratorios, biométricos, financieros y de redes sociales que normalmente se mantienen separados.
- Sus capacidades de perfilamiento e integración de datos pueden ser utilizadas por autoridades migratorias y de aplicación de la ley involucradas en violaciones sistemáticas de derechos humanos, amplificando los riesgos de señalamiento, detención, deportación y otras medidas coercitivas.
- Habilita decisiones automatizadas o semi-automatizadas en áreas altamente sensibles como la seguridad, el control migratorio y los servicios públicos.
- Concentra en un único proveedor privado el procesamiento de información estatal estratégica de alto valor.

Cuando herramientas de esta naturaleza se incorporan en ámbitos como seguridad, inteligencia, control migratorio o administración pública, pueden ampliar sustancialmente la capacidad de vigilancia, seguimiento, perfilamiento y clasificación de personas.

Por estas razones, el debate sobre Palantir no es meramente técnico ni comercial. Es una discusión sobre el rol del Estado, la soberanía sobre la información pública, los límites democráticos al uso de la tecnología y las garantías necesarias para evitar abusos.

4. ¿QUÉ ANTECEDENTES INTERNACIONALES VINCULADOS CON PALANTIR JUSTIFICAN ESTA PREOCUPACIÓN?

La trayectoria internacional de Palantir refuerza estas preocupaciones. Su tecnología ha sido utilizada en contextos en los que organizaciones internacionales han documentado impactos concretos sobre los derechos humanos.

Estados Unidos — control migratorio y persecución de activistas. Amnistía Internacional ha advertido que productos provistos por Palantir a las autoridades migratorias de Estados Unidos, en particular a ICE y a sus unidades Homeland Security Investigations (HSI) y Enforcement and Removal Operations (ERO), han quedado implicados en el monitoreo de personas migrantes y en la aplicación discriminatoria de la política migratoria. Amnistía también advirtió sobre los riesgos que estos sistemas plantean para estudiantes internacionales y activistas que ejercen sus derechos a la libertad de expresión y a la protesta.

Reino Unido — datos de salud. Amnistía Internacional, junto con organizaciones de derechos humanos y del ámbito sanitario, pidió al Servicio Nacional de Salud (NHS) que rescinda su contrato con Palantir para la gestión de datos sensibles de salud, citando los riesgos asociados al manejo de información personal y el historial corporativo más amplio de la empresa en materia de derechos humanos, incluidos sus vínculos con Estados involucrados en la perpetración de graves crímenes internacionales.

Alemania — uso policial. En febrero de 2023, el Tribunal Constitucional Federal de Alemania declaró inconstitucionales las disposiciones legales que habilitaban el uso del software de análisis automatizado de datos de Palantir por parte de las fuerzas policiales de Hesse y Hamburgo. El tribunal concluyó que esas disposiciones violaban el derecho a la autodeterminación informativa porque permitían construir perfiles exhaustivos de personas —incluidos testigos y contactos sin ninguna sospecha fundada— sin umbrales legales suficientes. El fallo estableció, por primera vez, requisitos constitucionales específicos para el uso de inteligencia artificial por parte de las fuerzas de seguridad.

Territorio Palestino Ocupado — Palantir ha estado suministrando productos y servicios de inteligencia artificial al ejército y a los servicios de inteligencia israelíes, y está vinculada a las actuales actividades militares de Israel en Gaza. En enero de 2024, la empresa anunció una asociación estratégica con el Ministerio de Defensa israelí para apoyar misiones relacionadas con la guerra. Amnistía Internacional identificó entre los productos provistos a Gotham, Foundry, Gaia y la plataforma AI for Defense de Palantir.

Estos antecedentes demuestran que la preocupación no es exclusiva de Argentina ni responde a una reacción local: forma parte de un debate internacional cada vez más intenso sobre los límites al uso de tecnologías de análisis masivo de datos en áreas sensibles.

5. ¿QUÉ DIJO AMNISTÍA INTERNACIONAL SOBRE LOS RIESGOS DE ESTAS TECNOLOGÍAS?

Amnistía Internacional ha alertado sobre los riesgos de las tecnologías que permiten la integración de bases de datos, el cruce de información sensible y la producción de inteligencia en contextos de seguridad o control migratorio. En relación con Palantir, la organización señaló que sus herramientas fueron utilizadas por agencias migratorias de Estados Unidos para monitorear a personas migrantes y activistas, facilitando prácticas de control y vigilancia incompatibles con los estándares de derechos humanos.

Amnistía Internacional también señala que Palantir no ha demostrado haber llevado adelante los procesos de debida diligencia en derechos humanos exigidos por los estándares internacionales aplicables a las empresas, ni haber adoptado medidas efectivas para prevenir, mitigar y reparar los impactos asociados a sus productos.

La importancia de esta advertencia radica en que muestra cómo una tecnología de este tipo puede ser utilizada para amplificar prácticas estatales abusivas. Cuando una herramienta permite reunir información dispersa, generar perfiles o producir alertas sobre personas o grupos, puede profundizar sesgos, reforzar dinámicas discriminatorias y afectar de manera desproporcionada a quienes ya se encuentran en situaciones de vulnerabilidad o estigmatización. La experiencia internacional indica, por lo tanto, que cualquier eventual incorporación de estas tecnologías debe analizarse con extrema cautela y plena transparencia.

6. ¿CUÁL ES EL CONTEXTO ARGENTINO EN EL QUE SURGE ESTA PREOCUPACIÓN?

La discusión sobre Palantir no ocurre en el vacío. Se inscribe en un proceso documentado de expansión de las capacidades estatales de vigilancia entre diciembre de 2023 y diciembre de 2025:

- **Reformas estructurales**. El gobierno impulsó reformas del Sistema Nacional de Inteligencia, del Estatuto de la Policía Federal y creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS) dentro del Ministerio de Seguridad.
- **Nuevos protocolos**. Se aprobaron protocolos como "Ciberpatrullaje", reconocimiento y comparación facial ex post, y el llamado "Protocolo Antipiquetes", ampliando la actuación estatal sobre los espacios digitales y la protesta social.
- **Adquisiciones tecnológicas**. Se documentaron compras de tecnologías de monitoreo de redes sociales, software de procesamiento de imágenes y reconocimiento facial (incluidas licencias de Clearview), drones, vigilancia aérea y herramientas de análisis predictivo.
- **Infraestructura urbana.** El Gobierno de la Ciudad de Buenos Aires amplió su sistema de videovigilancia —cámaras fijas y móviles, drones, sistemas aerostáticos y dispositivos en patrulleros— sin información pública completa sobre su uso.
- **Acuerdo bilateral con Estados Unidos.** En noviembre de 2025 se anunció un acuerdo entre Estados Unidos y Argentina que incluye el reconocimiento de Estados Unidos como jurisdicción adecuada para la transferencia transfronteriza de datos personales y el compromiso de no discriminar servicios digitales estadounidenses. Esto amplía la preocupación porque conecta la eventual llegada o expansión de proveedores privados de tecnología con un contexto más amplio de flujos internacionales de datos, infraestructura digital y regulación.

Este proceso se tradujo en nuevas prácticas de vigilancia y control, entre ellas el monitoreo de redes sociales, el uso de reconocimiento facial, drones y cámaras móviles, así como el cruce de datos entre agencias estatales. En otras palabras, la preocupación por una eventual inserción de Palantir no deriva solo del perfil de la empresa, sino del hecho de que podría incorporarse en un ecosistema estatal que ya venía ampliando sus herramientas de vigilancia, inteligencia y ciberpatrullaje. Esto vuelve especialmente urgente discutir qué tipo de infraestructura se está construyendo, con qué reglas, bajo qué supervisión y con qué resguardos para la población.

7. ¿QUÉ INFORMACIÓN SOLICITÓ AMNISTÍA INTERNACIONAL ARGENTINA Y CUÁL FUE LA RESPUESTA?

Frente a esta situación, Amnistía Internacional Argentina presentó un pedido de información pública a la Secretaría General de la Presidencia para determinar si existieron reuniones, acuerdos, provisión de servicios o cesiones de datos estratégicos entre el Poder Ejecutivo y Palantir Technologies (ver respuesta)

También solicitó información pública al Ministerio de Relaciones Exteriores, Comercio Internacional y Culto para comprender mejor los fundamentos, el alcance y las implicancias del acuerdo con Estados Unidos en materia de transferencias de datos y servicios digitales (ver respuesta).

Las respuestas recibidas fueron insuficientes, lo que revela una falta de transparencia en torno a un asunto de alto interés público. Cuando están en juego posibles vínculos entre el Estado y empresas que proveen infraestructura de vigilancia, así como decisiones que pueden afectar el tratamiento y la circulación de datos personales, la opacidad no es un problema secundario: es uno de los principales factores de riesgo. Sin información clara y completa, se vuelve imposible evaluar la legalidad, la necesidad, la proporcionalidad y el potencial impacto en derechos humanos de las decisiones adoptadas.

8. ¿QUÉ DERECHOS HUMANOS ESTÁN EN RIESGO?

Las tecnologías de vigilancia no son neutrales. Su impacto depende del contexto institucional en el que se implementan, de los fines para los que se utilizan, del tipo de datos que procesan y de los mecanismos de supervisión existentes. Cuando se incorporan a estructuras estatales sin suficiente transparencia, sin evaluación de impacto y sin mecanismos robustos de control democrático, pueden convertirse en herramientas de vigilancia masiva, discriminación, persecución de voces críticas y restricción del espacio cívico.

- **Privacidad y protección de datos personales: el cruce de información dispersa permite construir perfiles detallados de personas que no son sospechosas de ningún delito.**
- **Libertad de expresión: el monitoreo de redes sociales y comunicaciones produce un efecto inhibidor por el cual las personas se autocensuran por temor a ser observadas.**
- **Libertad de reunión y derecho a la protesta: el reconocimiento facial en manifestaciones desalienta la participación política, especialmente entre voces críticas del gobierno.**
- **Libertad de asociación: los análisis de redes y vínculos pueden mapear afiliaciones políticas, sindicales o comunitarias.**
- **Igualdad y no discriminación: los sistemas predictivos y biométricos reproducen y amplifican sesgos estructurales contra comunidades migrantes, jóvenes de barrios populares, personas trans, periodistas y defensores de derechos humanos.**
- **Debido proceso: las decisiones automatizadas o semi-automatizadas pueden afectar derechos sin garantías adecuadas de revisión.**
- **Acceso a la información pública: la opacidad sobre estas tecnologías impide el control ciudadano y democrático.**

Esto involucra no solo la responsabilidad del Estado, sino también la de las empresas. Amnistía Internacional recuerda que, de conformidad con los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, las empresas deben evitar causar o contribuir a impactos adversos sobre los derechos humanos a través de sus propias actividades, y también utilizar su influencia para prevenir o mitigar aquellos impactos a los que están directamente vinculadas a través de sus productos, servicios o relaciones comerciales. Estas obligaciones exigen llevar adelante procesos de debida diligencia en derechos humanos y comunicar adecuadamente cómo se abordan esos riesgos.

9. ¿CUÁLES SON LOS PRINCIPALES RIESGOS DE UNA EVENTUAL INSERCIÓN DE PALANTIR EN ARGENTINA?

En Argentina, una eventual inserción de Palantir en áreas de seguridad, inteligencia, migración o administración pública podría tener consecuencias especialmente graves.

- Vigilancia masiva y perfilamiento. Una herramienta capaz de cruzar datos policiales, migratorios, biométricos, financieros y sociales transformaría capacidades hoy fragmentadas en una vigilancia integrada y persistente sobre la población.
- Profundización de prácticas discriminatorias. Los sistemas opacos y predictivos reproducen sesgos estructurales y convierten desigualdades preexistentes en decisiones automatizadas con efectos concretos sobre la vida de personas migrantes, manifestantes, juventudes y otros grupos históricamente estigmatizados.
- Privatización de funciones estratégicas del Estado. Delegar funciones soberanas en un proveedor privado implica dependencia tecnológica, secreto contractual, debilitamiento del control democrático y pérdida de capacidad estatal para auditar y revertir decisiones.
- Erosión silenciosa de derechos fundamentales. Los efectos no siempre son visibles ni inmediatos: muchas veces operan a través del disciplinamiento, la autocensura y el temor a ser monitoreado. Esto reduce el espacio cívico, debilita la deliberación pública y desalienta la participación política.

Estas advertencias no son hipotéticas: surgen tanto del modelo de negocios de Palantir —que se especializa precisamente en integrar datos y producir inteligencia operativa para los Estados— como de los usos concretos que ya ha tenido su tecnología en otros contextos.

10. ¿POR QUÉ ESTOS RIESGOS SON AÚN MAYORES EN CONTEXTOS DE OPACIDAD Y DÉBIL SUPERVISIÓN INSTITUCIONAL?

Porque en contextos de opacidad institucional y debilidad de los organismos de supervisión, la promesa de "modernización" puede encubrir la consolidación de infraestructuras de vigilancia difíciles de desmontar una vez instaladas. Cuando no existe información pública suficiente sobre qué sistemas se implementan, qué datos utilizan, qué objetivos persiguen y qué organismos los supervisan, el margen para los abusos crece significativamente.

La pregunta fundamental es qué acceso a los datos de la población —y a los propios datos del Estado— puede quedar habilitado, con qué fines y bajo qué garantías. Si la infraestructura tecnológica permite recolectar, clasificar y analizar información proveniente de múltiples fuentes sin supervisión efectiva, la relación entre el Estado y la población se altera de manera estructural. El problema, por lo tanto, no se agota en una única decisión de contratación: remite al modelo de gobernanza de los datos, a la arquitectura institucional de la vigilancia y a los límites del poder estatal.

11. ¿QUÉ DEBERÍA EXIGIRSE FRENTE A CUALQUIER ACERCAMIENTO ENTRE EL ESTADO ARGENTINO Y EMPRESAS TECNOLÓGICAS?

Cualquier negociación, contratación o acercamiento entre el Estado argentino y empresas proveedoras de tecnologías de vigilancia como Palantir debería estar sujeta, como mínimo, a condiciones estrictas de transparencia, acceso a la información pública, evaluación de impacto en derechos humanos, control legislativo y judicial, auditorías independientes y garantías efectivas de habeas data.

Esto significa que ningún acuerdo, programa piloto, contrato o intercambio de datos debería avanzar sin suficiente conocimiento público sobre sus términos, objetivos, alcance y mecanismos de supervisión. También significa que cualquier decisión en esta materia debe estar acompañada por mecanismos eficaces para prevenir abusos, reparar daños y garantizar la rendición de cuentas.

Además, no solo el Estado debe rendir cuentas. Las empresas involucradas también deben demostrar qué procesos de debida diligencia realizaron, qué salvaguardas contractuales, técnicas y procedimentales existen, y de qué manera aseguran que sus productos no causan, no contribuyen y no quedan directamente vinculados a violaciones de derechos humanos. Si no pueden garantizarlo, deberían abstenerse de avanzar o considerar una finalización responsable de la relación comercial.

Amnistía Internacional ha llamado previamente a todos los Estados, instituciones públicas y empresas a utilizar su influencia derivada de sus inversiones, incluso mediante la desinversión responsable de Palantir y el cese de la compra de equipos y servicios de la empresa, para detener nuevas ventas de equipos y servicios de Palantir a Israel, dado su probable uso en crímenes internacionales, incluido el genocidio.

Amnistía también ha instado a los Estados y a las instituciones públicas a garantizar que Palantir quede excluida de cualquier actividad que implique introducir sus materiales y servicios en sus mercados, incluyendo, entre otras medidas, prohibir su participación en ferias y exposiciones, reuniones gubernamentales, contratos y participación en subvenciones de investigación y actividades con organismos públicos.
Amnistía ha pedido que estas medidas permanezcan vigentes hasta que la empresa pueda demostrar que no está contribuyendo al apartheid de Israel, a la ocupación ilegal ni a sus crímenes en virtud del derecho internacional.

RECOMENDACIONES

Al Poder Ejecutivo Nacional

- Hacer pública toda información sustantiva sobre reuniones, acuerdos, pruebas piloto, contrataciones o cesiones de datos vinculadas a Palantir y a otros proveedores de tecnologías de vigilancia.
- Abstenerse de avanzar en cualquier acuerdo, prueba piloto, contratación o esquema de intercambio de datos con Palantir mientras no exista transparencia plena, debate público informado y garantías compatibles con los estándares internacionales de derechos humanos.
- Realizar y publicar evaluaciones de impacto en derechos humanos previas a cualquier adquisición o despliegue de tecnologías de vigilancia.
- Garantizar mecanismos efectivos de habeas data, supervisión técnica independiente y auditorías externas.
- Suspender el avance del acuerdo bilateral con Estados Unidos en materia de transferencia transfronteriza de datos hasta tanto exista un debate público informado y se aseguren garantías equivalentes a los estándares internacionales.

Al Congreso Nacional

- Ejercer su función de control mediante interpelaciones, pedidos de informes y, de ser necesario, comisiones investigadoras.
- Avanzar en la actualización del marco legal de protección de datos personales y en la regulación específica del uso estatal de tecnologías de vigilancia, con audiencias públicas y participación de organizaciones especializadas.