



Tecnología

[+ Agregar Clarín en !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Advierten por el uso de inteligencia artificial para predecir delitos y vigilar en internet: qué puede saber el Estado sobre los argentinos

La ONG Derechos Digitales cuestiona la expansión de la vigilancia y la debilidad de sus controles en el país.

El trabajo también examina el reconocimiento facial, el uso de Palantir y el negocio de los datos biométricos en América Latina.

Una especialista explica a Clarín los riesgos del ciberpatrullaje, además de las filtraciones de datos y el registro de iris de World.



El presidente Javier Milei, junto a la ministra de Seguridad, Alejandra Monteoliva. Foto: Francisco Loureiro



JUAN



Clarín

Suscribite



Resumen



Compartir



Seguir



Comentar

01/10/2026 05:45 / Actualizado al 02/10/2026 08:43

Monitorear publicaciones en redes sociales, comparar caras capturadas por cámaras y usar inteligencia artificial para intentar anticipar delitos son facultades que **el Gobierno incorporó a su estructura** de seguridad durante los últimos años: un informe regional pone el foco en Argentina y advierte sobre los riesgos de ampliar esas capacidades tecnológicas sin fortalecer al mismo ritmo los **mecanismos de control**. La privacidad, la libertad de expresión y la posibilidad de cuestionar al poder aparecen entre los derechos comprometidos.

El trabajo, *En la mira 2: un panorama de las amenazas digitales en América Latina*, fue elaborado por la organización Derechos Digitales en el marco del Observatorio Latinoamericano de Amenazas Digitales (OLAD) y publicado este jueves. A partir de un análisis que va de junio de 2024 a mayo de 2025, reúne noticias, investigaciones y publicaciones del Gobierno de Javier Milei en el boletín oficial, en el contexto de un análisis más general de **América Latina**.

“La Resolución 428/2024 habilitó a las fuerzas federales a **monitorear redes sociales** y fuentes abiertas para ‘**prevenir delitos**’, con un catálogo tan amplio que en la práctica casi no tiene límites. A la fecha, ese esquema se consolidó después con el decreto 383/2025, que lo incorporó como facultad de la Policía Federal sin orden judicial y con la resolución 725/2026, que

amplió los supuestos para monitorear a adolescentes”, explica a

Clarín Ximena Cuzcano, analista en Seguridad y Resiliencia



La especialista se refiere a la creación de la Unidad de Inteligencia Artificial Aplicada a la Seguridad, en julio de 2024, firmada por la entonces ministra **Patricia Bullrich**, que le asignó funciones de análisis de cámaras, reconocimiento facial, procesamiento de grandes volúmenes de datos y elaboración de perfiles de sospechosos. Allí se estableció “utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos”.

En junio de 2025, el decreto 383 incorporó al estatuto de la Policía Federal la facultad de realizar tareas preventivas sin autorización judicial en espacios públicos digitales. El alcance incluye redes sociales abiertas, sitios web públicos y otras fuentes accesibles. El mismo artículo exige respetar la protección de datos personales, la libertad de expresión, la intimidad y la privacidad. Esa habilitación se refiere a información pública; no autoriza por sí sola el acceso a conversaciones privadas.

“El riesgo aparece cuando esta práctica se dirige a personas específicas sin que ellas lo sepan, donde monitorean su actividad en redes de forma automatizada y encubierta. Ahora, esta persona podría ser crítica del Gobierno, opositora, periodista, o defensora de derechos humanos”, advierte Cuzcano.



Patricia Bullrich, hoy senadora nacional, pieza clave del armado de Seguridad del Gobierno. Foto: Federico López Claro

El informe examina cómo las publicaciones pueden utilizarse para **clasificar a usuarios** según sus posiciones políticas o reconstruir sus vínculos. El carácter público de un comentario queda, así, en el centro de una discusión sobre los límites de su recolección y análisis por parte del Estado.

“No se sabe qué criterios usan o cuáles son los límites que lo diferencian de una práctica de vigilancia estatal. Como resultado, se puede caer en **hostigamiento contra quienes** son catalogados como opositores o la autocensura”, agrega la especialista sobre los riesgos del esquema.

El protocolo argentino contiene **prohibiciones expresas**. Impide



actividad preventiva concluye o se decide no judicializarla y establece que el ciberpatrullaje debe respetar la libertad de expresión. También prevé trazabilidad, auditoría y reportes de gestión.

A eso apunta el cuestionamiento de Derechos Digitales: a la amplitud de las facultades y a las garantías necesarias para controlar su aplicación.

“Lo primero que falta es **una ley del Congreso** que defina si el ciberpatrullaje es inteligencia o investigación criminal y que cumpla los estándares de legalidad, necesidad, proporcionalidad y razonabilidad. El ciberpatrullaje no debería usarse para cuidar la imagen del Gobierno, y se debe reafirmar que los datos personales siguen protegidos aunque estén publicados”, dice Cuzcano. La actualización más reciente que menciona la analista fue publicada hace muy poco, el 29 de julio de 2026.

El reporte también recupera la controversia por el **Plan de Inteligencia Nacional** de mayo de 2025. Según la investigación periodística que cita, sus objetivos incluían monitorear a actores que generaran “**pérdida de confianza en políticas económicas**” o “manipularan la opinión pública” durante elecciones. El Gobierno admitió la existencia del documento y negó que habilitara la persecución de opositores y periodistas, según informó este medio.

La preocupación de la organización abarca, además, la información disponible para que los ciudadanos puedan conocer cómo operan estas herramientas. “También falta transparencia,

pues el Estado debería informar qué organismos lo hacen, con
qué fines, tecnologías y bajo qué controles” planteó Cuzcano



Suscribite



político



El Presidente, junto a Alejandra Monteoliva y Patricia Bullrich, exministra de Seguridad.
Foto: Presidencia

Brasil ofrece uno de los ejemplos más concretos de las consecuencias de confiar decisiones policiales a sistemas de

identificación. El informe describe **Smart Sampa**, el programa de videovigilancia y **reconocimiento facial** implementado en San



el objetivo declarado de localizar prófugos y **prevenir delitos mediante el cotejo de imágenes con bases judiciales.**

Entre los episodios citados aparece **un jubilado de 80 años que pasó horas detenido** después de que el sistema lo identificara como un agresor sexual, además de un paciente psiquiátrico esposado en un centro de salud mental por una orden de arresto desactualizada. Los casos muestran problemas en distintos puntos del proceso, desde la identificación hasta la calidad de la información utilizada para decidir una detención.

El despliegue alcanzó las escuelas. Según el informe, cerca de **400 cámaras del sistema fueron instaladas en establecimientos municipales de San Pablo**, con reconocimiento facial en los accesos y registros biométricos de estudiantes, docentes y trabajadores. El trabajo cuestiona la ausencia de políticas claras de privacidad y mecanismos de consentimiento informado para los menores. La promesa de reforzar la seguridad convive allí con la captura de datos de chicos que asisten a clases.

En Argentina, el **Observatorio de Derecho Informático Argentino (O.D.I.A.)** lanzó una campaña en 2024 donde llenaron de códigos QR la Ciudad para concientizar sobre el problema del reconocimiento facial masivo.

El “ciberpatrullaje” y la clasificación política de usuarios aparece en otro grupo de casos de países de América Latina. En Colombia, el documento recoge una investigación sobre la contratación de una empresa para mejorar la imagen del Gobierno que derivó en

una lista de 486 usuarios de X (Twitter) ordenados según una posición favorable, neutral u opositora. En Brasil, una licitación



medir la popularidad del Gobierno y combatir la desinformación.

En Ecuador, la ampliación del análisis de datos se posicionó con una de las empresas tech más polémicas de la actualidad:

Palantir. Durante 2025, el Gobierno formalizó una colaboración con la empresa cofundada por Peter Thiel para implementar su plataforma en el Servicio Nacional de Aduana, con el objetivo de combatir el contrabando y el fraude aduanero.

Según el informe, el acuerdo permite consolidar información de otros organismos públicos, lo que extiende las posibilidades de procesamiento más allá de los registros aduaneros. **Derechos Digitales** advierte sobre las consecuencias de ese cruce masivo para la privacidad y el control de los ciudadanos sobre sus datos.

“Lo vimos con el ciberpatrullaje en Argentina o cómo **en Ecuador el Gobierno contrató a Palantir** para recolectar y cruzar datos de múltiples fuentes de forma masiva”, señaló Cuzcano. Para la analista, la continuidad de esas capacidades merece atención más allá de cada anuncio. “Entonces se forma como una infraestructura permanente de los Estados, que puede seguir operando más allá del gobierno de turno. Y a diferencia de otros patrones, avanza sin que la institucionalidad de control o rendición de cuentas crezca al mismo ritmo”.

El vínculo de Peter Thiel con la Argentina también se amplió en 2026: el empresario lleva varios meses en el país y su fondo compró acciones de Vista Energy por unos 76 millones de dólares. La información publicada registra esa inversión y sus

reuniones en Buenos Aires, pero no detalla otros proyectos locales



presencia merece atención por el poder que tienen estas plataformas para procesar **grandes volúmenes de datos**.



Peter Thiel, saliendo de la Casa Rosada el 23 de abril de este año. Foto: Reuters

Filtraciones de datos: el negocio de los data brokers

El informe dedica buena parte de su análisis a las filtraciones de datos. Durante la última década, no sólo en Argentina sino en todo el mundo, una gran cantidad de datos personales empezaron a filtrarse por distintos problemas de seguridad, tanto de empresas como Estados.

Sólo por mencionar algunos en Argentina, desde entidades públicas como el Senado de la Nación, la Dirección Nacional de Migraciones y el PAMI, hasta entidades privadas como Ingenio Ledesma, OSDE o Mercado Libre, sufrieron filtraciones de datos

de usuarios que luego terminan circulando en foros

underground. Vale aclarar muchos nombres que aparecen en



sólo comerciales) de los mercados de Telegram y la así llamada “dark web”.

El informe identifica **filtraciones en 12 países** y describe errores de configuración, accesos abusivos y fallas en proveedores tecnológicos que pueden oficial como la puerta de entrada de las filtraciones de datos.

En Argentina, uno de los antecedentes es la puesta en venta de más de 665.000 estudios médicos de pacientes atendidos en hospitales y sanatorios, entre ellos **radiografías, ecografías, tomografías y análisis de laboratorio**. El documento remite a la cobertura de este medio sobre el ataque al proveedor Informe Médico, publicada en abril de 2025.

Hay casos citados de América Latina: en **Colombia**, una configuración incorrecta dejó abierto un espacio de almacenamiento de la aplicación de pagos GoPass y expuso información de casi un millón de usuarios, incluidas patentes e identificaciones tributarias. En **Costa Rica**, el documento registra una falla en la infraestructura de Movistar que dejó accesibles cerca de 650.000 archivos, entre ellos documentos de identidad y selfies utilizadas para verificar usuarios.

El informe vincula estos incidentes con **decisiones sobre cuánto se recolecta**, quién puede acceder, qué proveedores intervienen y durante cuánto tiempo se conserva la información, en lo que es una desobediencia de una máxima en ciberseguridad: **no recolectar más datos de los necesarios** (además de sólo

recolectar aquellos que se pueda asegurar proteger).



sigue siendo necesario almacenarlos. La responsabilidad alcanza a los organismos y empresas que diseñan y administran esos sistemas, un área crítica en Argentina que llevó a la **creación de la Agencia Federal de Ciberseguridad en 2024**, dentro de la SIDE. A comienzos de 2026, el Gobierno reformuló ese esquema: la agencia pasó a llamarse **Agencia Federal de Ciberinteligencia** y mantuvo sus funciones vinculadas a inteligencia dentro del sistema de inteligencia nacional, mientras que las tareas de ciberseguridad propiamente dichas quedaron bajo el nuevo **Centro Nacional de Ciberseguridad**, dependiente de la Jefatura de Gabinete.

El informe toma a World, antes Worldcoin, como ejemplo del debate sobre el consentimiento para entregar datos biométricos: en agosto de 2023, **9.500 personas en Argentina escanearon su iris** en un día a cambio de entre 30 y 50 dólares, en un contexto de inflación superior al 115%. La empresa sostiene que convierte las imágenes en códigos y usa herramientas criptográficas para proteger la identidad; Derechos Digitales cuestiona las condiciones en que se obtuvo el consentimiento, **la posibilidad de borrar los datos** y quién mantiene el control sobre ellos.

Para las herramientas estatales de vigilancia, Cuzcano propone que ese examen empiece antes de su incorporación. “Además, **antes de comprar herramientas de vigilancia debería evaluar su impacto** en derechos humanos y suspender la compra cuando los riesgos superen los beneficios”, sostuvo. Conocer qué información se reúne, cómo se utiliza y quién responde por un error forma parte de las garantías que reclama la investigación