

ARANZA BUSTAMANTE

SEGURIDAD

6 DE OCTUBRE DE 2026

No es paranoia, las tecnologías de vigilancia estatal crecen sin control en América Latina

Un informe de Derechos Digitales muestra cómo en América Latina crecen las capacidades de vigilancia estatal mientras persisten controles insuficientes para prevenir abusos y vulneraciones de derechos humanos.



América Latina acelera el uso de tecnologías de vigilancia mientras persisten vacíos de supervisión JUSTHAVEALOOK

En São Paulo, Brasil, una red de 40,000 cámaras instaladas en espacios públicos y privados puede comparar en tiempo real los rostros de las personas con bases de datos judiciales. El sistema, conocido como Smart Sampa, comenzó a implementarse a finales de 2024 con el objetivo de “identificar fugitivos y prevenir delitos” mediante herramientas automatizadas de reconocimiento facial.

Sin embargo, Smart Sampa también ha dejado ver algunos de sus defectos. Más de 8% de las personas detenidas tuvieron que ser liberadas por errores, según el informe *En la mira 2: un panorama de las amenazas digitales en América Latina*, elaborado por Derechos Digitales. Entre los casos documentados figura el de un hombre de 80 años identificado equivocadamente como un agresor sexual o el de un paciente esposado en un centro de salud mental debido a una orden de arresto desactualizada.

Nuestras historias más importantes, diario en tu correo electrónico.

INSCRIBIRSE

Ingresa tu dirección de correo electrónico para suscribirte a nuestro newsletter y formar parte del universo Wired. Tus datos personales serán tratados de acuerdo con nuestra [Convenio de Usuario](#) y [Aviso de Privacidad](#).

El sistema llegó además a escuelas municipales, donde cerca de 400 cámaras generan registros biométricos de estudiantes, docentes y otros trabajadores. El reporte señala que su implementación ocurrió sin políticas claras de privacidad ni mecanismos de consentimiento informado para menores de edad. Los datos oficiales no registran la identidad racial de más de la mitad de las personas, lo que impide evaluar si el sistema incurre en racismo algorítmico.

Brasil es uno de varios casos que han llevado a Derechos Digitales a identificar una tendencia regional. La organización ha documentado cómo distintos gobiernos de América Latina han ampliado el uso de reconocimiento facial, inteligencia artificial (IA), videovigilancia, análisis masivo de datos y monitoreo de redes sociales. Según el informe, los mecanismos de transparencia, protección de derechos, control y rendición de cuentas no se han desarrollado en la misma medida.

En la mira 2 estudia incidentes ocurridos entre junio de 2024 y mayo de 2025 por medio del monitoreo semanal de fuentes abiertas y el trabajo de organizaciones del Observatorio Latinoamericano de Amenazas Digitales. Sus autores reconocen que la capacidad para documentar estos casos varía entre países, por lo que los hallazgos sirven para identificar patrones regionales.



¿Su jefe lo está observando? Por qué el software de vigilancia en el trabajo no logra los efectos deseados

Con la ayuda de la IA, las empresas tienen más opciones que nunca para vigilar y controlar a sus empleados, minuto a minuto, en cada pulsación de tecla. No obstante, su aplicación tiende a ser contraproducente, según la evidencia.

El reconocimiento facial llega antes que las reglas

Paraguay exhibe uno de los ejemplos más claros del desfase. La organización TEDIC documentó cámaras de reconocimiento facial instaladas desde 2018 por al menos 13 instituciones públicas. El informe sostiene que estos sistemas se expandieron sin un marco general específico que regulara su uso y sin estudios de impacto en derechos humanos que permitieran evaluar previamente sus posibles consecuencias.

En 2024, el reconocimiento facial también comenzó a incorporarse directamente en la legislación. La Ley 7269 estableció la vigilancia biométrica obligatoria en estadios de fútbol, extendiendo su uso a espacios con grandes concentraciones de personas. Al conectarse con bases de datos, estos sistemas pueden intentar identificar automáticamente a alguien mientras circula por un lugar, por lo que resulta relevante definir qué imágenes pueden utilizarse, quién accede a los registros y cómo puede cuestionarse una identificación errónea.

El informe ubica el caso paraguay dentro de una tendencia regional en la que distintos países han ampliado legalmente sus capacidades de vigilancia. Chile, por ejemplo, fortaleció su legislación de protección de datos y ciberseguridad, pero su normativa antiterrorista también permite utilizar tecnologías para interceptar comunicaciones. En El Salvador, la ley de protección de datos funciona junto con un marco de ciberseguridad que otorga amplias facultades bajo objetivos de seguridad nacional y orden público, pero establece controles limitados sobre cómo pueden ejercerse esas facultades.

Ciberpatrullaje de las redes

Argentina amplió estas herramientas hacia la IA y el monitoreo de internet. El gobierno de Javier Milei creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad, que habilita a las fuerzas federales a patrullar redes sociales y la *dark web*, analizar imágenes con reconocimiento facial, crear perfiles de sospechosos, utilizar drones y recurrir a algoritmos con el propósito de anticipar posibles delitos.

El país también incorporó el ciberpatrullaje como una facultad explícita para analizar información disponible públicamente en internet. Cuando esta práctica se apoya en sistemas automatizados, las autoridades pueden revisar grandes volúmenes de publicaciones, relacionar cuentas y detectar patrones a una escala difícil de alcanzar de forma manual.

Derechos Digitales distingue esta práctica del perfilamiento, mediante el cual las publicaciones pueden utilizarse para clasificar a una persona según sus opiniones o comportamientos. La organización cuestiona que el hecho de publicar algo abiertamente en internet permita a las autoridades recopilarlo y analizarlo sin restricciones, especialmente cuando sistemas automatizados pueden procesar información de miles de usuarios al mismo tiempo.

La IA añade nuevas posibilidades a estas tareas. En las conclusiones de *En la mira 2*, la organización señala que esta tecnología aparece cada vez con mayor frecuencia en los incidentes documentados y que debe analizarse dentro de infraestructuras más amplias capaces de clasificar información, construir perfiles, identificar personas y ampliar las posibilidades de vigilancia.



Agentes de la policía mexicana supervisan la seguridad en el Centro de Comando, Control, Cómputo, Comunicaciones y Coordinación (C5) en Zapopan, estado de Jalisco, México. **ULISES RUIZ/GETTY IMAGES**

Varias bases de datos, una sola plataforma

Ecuador muestra otra forma de expansión de estas capacidades. Entre enero y mayo de 2025, el país formalizó una colaboración con Palantir Technologies para implementar su plataforma de análisis de datos en el Servicio Nacional de Aduana (SENAE). La idea era combatir el contrabando y el fraude con una herramienta capaz de procesar información de distintas fuentes e identificar relaciones y patrones.

El alcance puede superar la información generada directamente por las aduanas, ya que el contrato permite al SENAЕ incorporar datos procedentes de otras entidades públicas dentro de la plataforma. Derechos Digitales advierte que esa concentración aumenta los riesgos para la privacidad y para el control que las personas mantienen sobre sus datos, sobre todo cuando información recopilada termina procesándose dentro de un mismo sistema.

Agrégalos a tus Fuentes Preferidas en Google para seguir nuestro contenido →



La infraestructura de vigilancia ecuatoriana también se extendió a las cámaras instaladas en las ciudades. Un decreto presidencial de septiembre de 2024 dispuso que el ECU-911 asumiera el control de aquellas administradas por gobiernos locales e implementara videovigilancia en tiempo real con reconocimiento facial y lectura de placas vehiculares. Así, distintas herramientas permiten recopilar información en espacios públicos y después relacionarla con otros registros en poder del Estado.

El caso también muestra el papel de las empresas que desarrollan estas tecnologías. Palantir provee la plataforma que permite integrar y analizar información procedente de distintas instituciones, mientras el gobierno decide para qué utilizarla y qué datos incorporar.

Esa relación plantea preguntas sobre las obligaciones de ambos actores: “Estados y empresas almacenan grandes volúmenes de datos personales para operar servicios, administrar programas y gestionar trámites cotidianos. Cuando el tratamiento de datos se realiza sin estándares adecuados de seguridad y gobernanza o con procesos de tercerización poco controlados, aumenta la probabilidad de exposición o acceso indebido”.

Quis custodiet ipsos custodes?

Supervisar estas tecnologías implica establecer límites concretos sobre su uso. El informe menciona reglas que delimiten las facultades de las autoridades, transparencia sobre el funcionamiento de los sistemas, evaluaciones de impacto, protección de datos y procedimientos para investigar errores o usos indebidos. También importa definir durante cuánto tiempo puede conservarse la información y en qué circunstancias puede compartirse entre instituciones.

Los casos documentados muestran que incorporar una tecnología también implica decidir qué institución puede utilizarla, con qué información y bajo qué controles. Sin embargo, Derechos Digitales encuentra que esas reglas no siempre se desarrollan al mismo tiempo que las nuevas facultades de vigilancia.

“Se observan intentos de validar legalmente prácticas como el ciberpatrullaje o ampliar capacidades estatales de análisis y vigilancia, sin que ello venga acompañado, en igual medida, de mecanismos proporcionales de control y rendición de cuentas”.

Los casos de Brasil, Paraguay, Argentina y Ecuador muestran distintas formas de esa expansión. También dejan ver que la discusión alcanza tanto a los gobiernos que adoptan estas tecnologías como a las empresas que las desarrollan y suministran. A medida que los sistemas adquieren mayor capacidad para identificar personas, seguir actividades y relacionar información, también aumenta la necesidad de definir quién responde cuando producen errores, afectan derechos o terminan utilizándose para fines distintos de aquellos que justificaron su implementación.

También te puede interesar...

- El [imperio de los creadores](#): ¿Qué sigue para una industria imparable? Un especial de WIRED en español.
- [Regístrate ya a WIRED Futures](#), el evento gratuito para entender y disfrutar el futuro. 30 de septiembre, CDMX.
- Agrega a WIRED en español como una de tus [Fuentes Preferidas en Google](#).
-  Mantente al tanto de las últimas noticias de [WIRED desde Google News](#), en nuestro [Canal de WhatsApp](#) o en el [newsletter](#) diario.
- [¿Cómo elegir el mejor auto eléctrico?](#) Una guía especial de WIRED en español.

TAGS

AMÉRICA LATINA

INTELIGENCIA ARTIFICIAL

PRIVACIDAD

ARGENTINA

El newsletter diario de WIRED en español

Recibe las mejores historias del mundo tech, seleccionadas cada día por nuestro equipo editorial.

INSCRIBIRSE

Ingresa tu dirección de correo electrónico para suscribirte a nuestro newsletter y formar parte del universo Wired. Tus datos personales serán tratados de acuerdo con nuestra [Convenio de Usuario](#) y [Aviso de Privacidad](#).

MAS DE WIRED



CULTURA

México tiene cada vez menos hijos: qué hay detrás de la caída de la fecundidad

Cada vez nacen menos bebés en México y América Latina. Aunque el costo de vida pesa, la caída de la fecundidad también refleja cambios profundos en las expectativas sobre la crianza.

POR ARANZA BUSTAMANTE



SEGURIDAD

Alertas y falsas esperanzas: miles de videos desinforman a los migrantes en TikTok y otras redes

Consejos que prometen proteger a migrantes pueden terminar desinformándolos. Un estudio muestra cómo TikTok concentra alertas, videos y recomendaciones que parecen útiles, pero pueden llevar a decisiones riesgosas.

POR ARANZA BUSTAMANTE

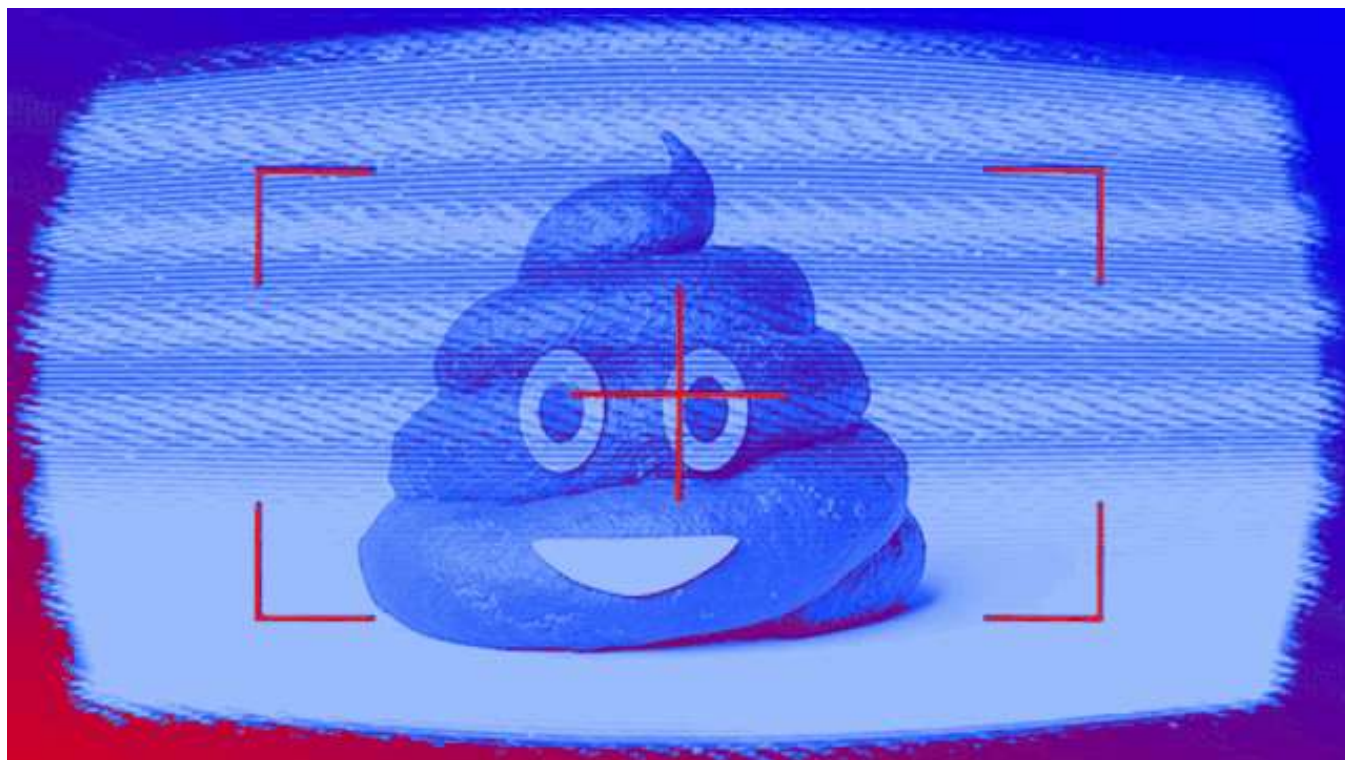


SEGURIDAD

¿Quién responde por el algoritmo que recluta jóvenes para el crimen organizado?

En Colombia, México y Ecuador, el crimen organizado usa los algoritmos de las redes sociales para atraer a niños, niñas y adolescentes a sus filas. Las plataformas lo saben, pero evitan hacer todo lo que podrían para enfrentarlo.

POR JOSÉ LUIS PEÑARREDONDA, CLIP



CIENCIA

Ya existen inodoros que usan IA para analizar tus heces

Si las empresas prometen que pueden ayudar a los usuarios a monitorear su salud intestinal, por qué los expertos sugieren que los inodoros inteligentes aportan pocos beneficios a la persona promedio.

POR GABRIELA GALVIN



CULTURA DIGITAL

La IA reproduce sesgos y prejuicios distintos cuando habla español: estas investigadoras colombianas los están rastreando

El estudio SESGO mostró que los modelos de inteligencia artificial diseñados en inglés no están entrenados para identificar los estereotipos propios de América Latina y, por lo tanto, los reproducen.

POR ARANZA BUSTAMANTE



SEGURIDAD

"Me sentí totalmente violentada": Que un hombre use lentes Meta en una cita es una *red flag* inmediata

A medida que crece la preocupación por las tecnologías de vigilancia, personas solteras están contando que han sido grabadas a escondidas durante sus citas.

POR JASON PARHAM

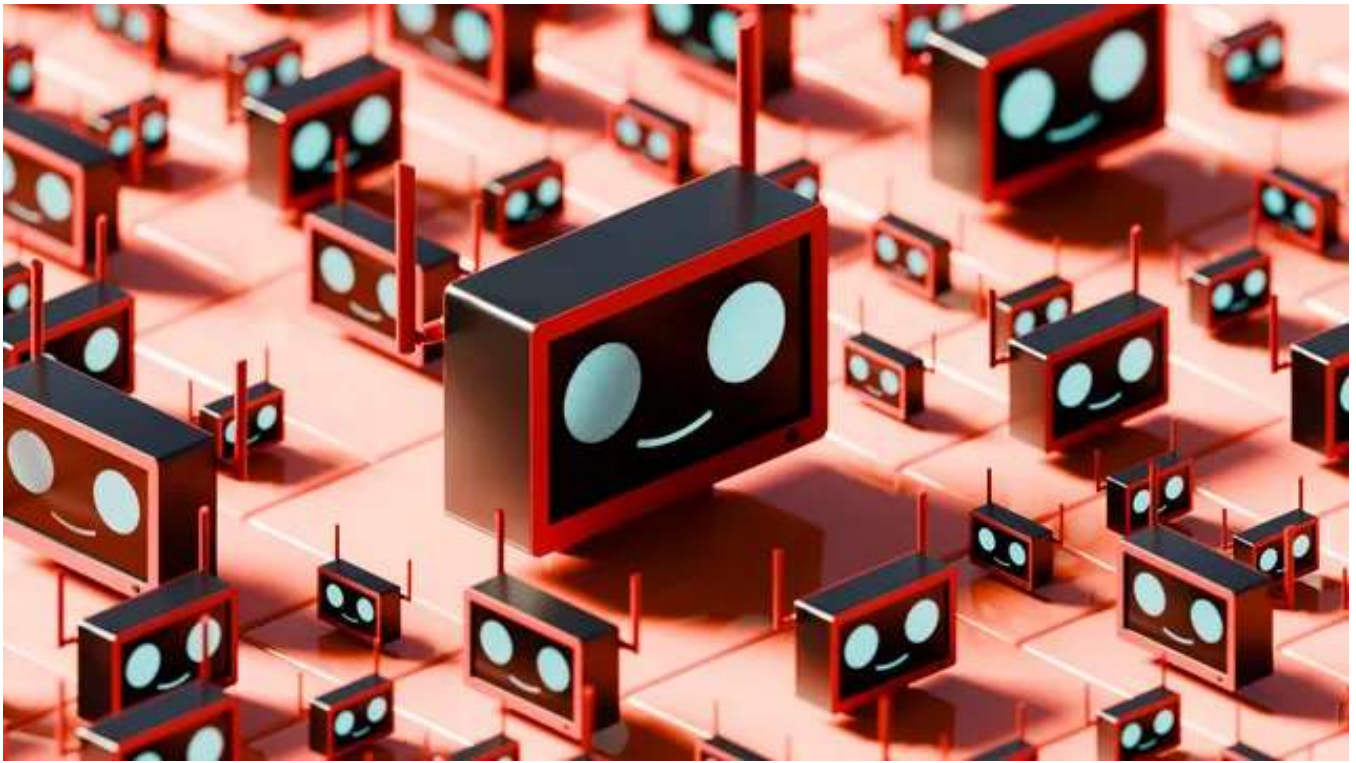


NEGOCIOS

Muse: La nueva IA de Meta quiere ayudarte con todo. A cambio, también quiere saber todo de ti

La aplicación Muse sigue la tendencia de Meta de incluir a los usuarios de forma predeterminada en la recopilación de datos para el entrenamiento de la IA. Además, te anima a compartir los datos de tu cuenta bancaria, tu correo electrónico y tu pasaporte.

POR REECE ROGERS



CULTURA DIGITAL

Agentes de IA crean un lenguaje propio que los humanos no pueden entender

Los agentes de IA generaron expresiones que adquirieron significados específicos dentro de sus comunidades, mientras que otras resultaron indescifrables para los investigadores.

POR FERNANDA GONZÁLEZ