

La vigilancia avanza en la región

Cuando las tecnologías digitales se usan para vulnerar la privacidad Un informe del Observatorio Latinoamericano de Amenazas Digitales advierte sobre el aumento del ciberespionaje estatal.



Página 12
Por Santiago Brunetto
12 Octubre 2026

Cuando las tecnologías digitales se usan para vulnerar la privacidad Un informe del Observatorio Latinoamericano de Amenazas Digitales advierte sobre el aumento del ciberespionaje estatal.

La vigilancia digital, el ciberpatrullaje estatal y el uso de software espía contra periodistas y militantes se expandió y consolidó en los distintos países de América Latina durante los últimos años. Así lo evidencia un informe del Observatorio Latinoamericano de Amenazas Digitales (OLAD), que advierte sobre diversos casos que dan cuenta de usos ya “institucionalizados” a nivel estatal de la cuestión. Se le suman otros fenómenos como la explotación de datos personales a gran escala y sus consecuentes filtraciones, fruto de las presuntas políticas de “innovación” a partir de Inteligencia Artificial (IA) montada sobre “infraestructuras vulnerables”.

El informe “En la mira 2: Un panorama de las amenazas digitales en América Latina”, analiza más de cien “incidentes” ocurridos en diversos países de la región entre junio de 2024 y mayo de 2025. Según explica Ximena Cuzcano, analista en Seguridad y Resiliencia Digital de Derechos Digitales, el documento es “diferente a los informes de ciberseguridad normales, que suelen poner el foco sólo en la ciberdelincuencia, porque incorpora la perspectiva de derechos humanos y el impacto de los incidentes en el interés público más allá de los ciberdelinquentes, sumando también el rol de actores como los gobiernos o las empresas privadas”.

La especialista agrega que “entendemos la inseguridad digital no sólo a partir de lo que ocurre con los dispositivos sino particularmente en base a qué le pasa a las personas y sus derechos”. El informe comienza por explicar, así, que los “incidentes” considerados en el estudio son “aquellos eventos vinculados al uso, control

o abuso de tecnologías digitales que generan impactos sobre derechos como la libertad de expresión, privacidad y protección de datos, el acceso a la información, la integridad y seguridad de personas y colectivos, así como la participación cívica en entornos digitales”.

Ante la consulta por los principales hallazgos del OLAD, Cuzcano no duda en remarcar, en primera instancia, la visualización

de los “incidentes” en una “línea de tiempo” que permite hablar ya de tendencias asentadas en la región y ya no de “casos aislados”: “Nos dimos cuenta de que los países replican distintos patrones, en muchos casos ya hablando de prácticas institucionalizadas”, señala.

De entre ellas, la especialista destaca antes que nada la problemática de la vigilancia y lo hace, primero, ejemplificando con un caso argentino: la Resolución N° 428/2024 del Ministerio de Seguridad, entonces a cargo de Patricia Bullrich, que ese año habilitó el ciberpatrullaje. “Fue un hecho muy importante porque

habilitó a las fuerzas federales a monitorear redes sociales o incluso a hacerlo de forma automatizada a través de la compra de software a otros países. La resolución, además, permite monitorear un catálogo tan amplio que, en la práctica, casi no hay límites ni criterios de proporcionalidad”, señala la especialista, que agrega que a esto “se fueron agregando más facilidades para las fuerzas federales, como la capacidad de la Policía Federal de monitorear sin orden judicial”.

En el informe, aparecen otros casos similares de la región en

torno a la vigilancia digital, que “reflejan la expansión del control estatal sobre la vida de las personas en la región”. “Entre las tendencias documentadas destacan el uso de spyware contra periodistas

y activistas; el acceso físico forzado a dispositivos durante detenciones u operativos policiales; el despliegue de sistemas de reconocimiento facial, videovigilancia masiva y plataformas de análisis masivo de datos; y el ciberpatrullaje en redes sociales”, agrega.

Se mencionan allí distintos casos vinculados mayormente con el uso del software Pegasus, de la empresa israelí NSO Group. “En 2024, Estados Unidos confirmó haber financiado el uso de Pegasus en Colombia para operaciones contra el narcotráfico durante la administración de Iván Duque, pagando 11 millones de dólares”, señala el informe, que agrega que, en Ecuador, “la Asamblea Nacional resolvió en diciembre de 2024 iniciar un proceso de fiscalización ante denuncias de uso de Pegasus por parte del gobierno de Daniel Noboa para vigilar a periodistas, opositores y activistas”. En abril de 2025, por su parte, en México se reveló que 456 personas fueron atacadas con este software entre abril y mayo de 2019.

Otros casos dan cuenta de vigilancias de discursos en redes sociales, documentadas en dos tipos de prácticas: “El perfilamiento, que consiste en caracterizar a personas usuarias de redes sociales según si sus publicaciones son favorables, críticas u opositoras al gobierno; y el ciberpatrullaje”, indica el informe.

“En Colombia, una investigación reveló que el gobierno contrató a una empresa para posicionar favorablemente su imagen ante la opinión pública; en la práctica, ello derivó a la elaboración de un listado de 486 personas usuarias de X clasificadas según su posición favorable, neutral u opositora al gobierno”, ejemplifica el documento, que agrega que “en Uruguay la Dirección General de la Policía reconoció en 2024 que monitoreaba redes sociales”.

“Ese mismo año, un adolescente fue detenido tras ser identificado erróneamente como participante de enfrentamientos en centros educativos, al ser confundido con un homónimo en redes sociales”, continúa el informe en un caso que recuerda a detenciones producidas en Argentina, como la de Daniel Vera, acusado de haber proferido ataques a través de redes contra el presidente Javier Milei, o de Nahuel Morandini y Roque Villegas, detenidos en Jujuy en 2024, acusados de publicar en redes sociales un rumor sobre la vida privada del exgobernador Gerardo Morales.

En el apartado del análisis masivo de datos personales, otra multinacional aparece mencionada: se trata de Palantir Technologies, la compañía estadounidense de software y análisis de big data fundada por el recientemente asentado en Buenos Aires, Peter Thiel. Cuzcano señala sobre esto que “Palantir, empresa que abiertamente dice que va a apoyar a Estados Unidos, ya ha tenido contratos con diferentes presidentes de la región”.

