# Espionaje ilegal en México: Pemex, fiscalías, SEDENA y más han usado software de vigilancia, muestra reporte

Fernanda González ⋮ 4-5 minutes ⋮ 1/31/2025

Las autoridades estatales, fiscalías y entidades de defensa en México han utilizado diversos sistemas y herramientas digitales para intervenir las comunicaciones de los ciudadanos sin su autorización legal, según un informe de la organización no gubernamental Red por la Defensa de los Derechos Digitales (R3D). Defensores de derechos humanos, periodistas y miembros de grupos de oposición están entre las principales víctimas.

El reporte titulado *El Estado de la Vigilancia 2025* revela que distintas instancias gubernamentales y paraestatales han adquirido licencias de uso para programas espía como FinFisher de Gamma International, Galileo de Hacking Team, Pegasus de NSO Group y Reign de Quadream. Estos se instalan sin consentimiento en dispositivos electrónicos para acceder a toda su información, incluyendo conversaciones, llamadas y ubicaciones.

---

Luego del hackeo confirmado a Alejandro Encinas, NSO Group investiga si el uso de Pegasus en México violó sus términos y condiciones de uso.

---

Una filtración masiva de documentos internos de Hacking Team en 2015 expuso la venta de su *spyware* a gobiernos de 35 países con graves crisis de derechos humanos. "**México resultó ser el principal cliente de la firma**, con transacciones realizadas por distintos gobiernos locales, dependencias y agencias federales a través de empresas intermediarias, en la mayoría de los casos, sin contar con facultades legales para ello".

El país habría invertido más de 5.8 millones de euros para acceder a Galileo. La cifra es superior a los 4 millones procedentes de Italia, los 3.1 millones de Marruecos y los 2.4 millones de Arabia Saudita. La investigación señala que gobiernos estatales de Baja California, Campeche, Chihuahua, Durango, Estado de México, Guerrero, Jalisco, Nayarit, Puebla, Querétaro, Tamaulipas y Yucatán establecieron relaciones comerciales con Hacking Team. También identifica como clientes a la Secretaría de la Defensa Nacional (Sedena), el Centro de Investigación y Seguridad Nacional (CISEN), la Policía Federal, la Procuraduría General de la República (ahora Fiscalía General de la República) y Petróleos Mexicanos.

El informe enfatiza en el uso reiterado de Pegasus en México. El programa fue utilizado por primera vez durante el sexenio de Felipe Calderón. Durante la administración de Enrique Peña Nieto, la Fiscalía General de la República (FGR) y el CISEN adquirieron el *software* argumentando prácticas de seguridad nacional. Sin embargo, investigaciones y filtraciones de documentos confidenciales demostraron que Pegasus se utilizó para espiar a periodistas, opositores políticos, defensores de derechos humanos y organizaciones no gubernamentales.

Un reportaje de *The New York Times* en 2023 identificó a México como el mayor usuario de Pegasus a nivel mundial, con un gasto superior a los 60 millones de dólares. La investigación concluyó que, hasta hace dos años, la Sedena era la única entidad en el país que operaba este *malware*.

Andrés Manuel López Obrador, expresidente de México, prometió erradicar el uso de Pegasus y demás prácticas de espionaje. No obstante, el diario estadounidense afirmó que durante su gestión el sistema informático se mantuvo en uso para acceder a la comunicación celular de Raymundo Ramos, defensor de derechos humanos y el periodista Ricardo Raphael.

## Antenas falsas en las tareas de espionaje gubernamental

El análisis de R3D también advierte sobre el empleo de antenas falsas de comunicación en labores de espionaje gubernamental. Estos dispositivos, conocidos como *IMSI catchers* o *stingrays*, simulan las conexiones telefónicas legítimas para recolectar información de manera encubierta. Son capaces de extraer el número IMSI e IMEI del teléfono, los registros de llamadas y mensajes SMS, y los archivos almacenados en el dispositivo.

“Las antenas falsas también pueden aparentar ser un dispositivo de comunicación y actuar de manera anónima para enviar mensajes de texto o realizar llamadas. Además de permitir el ejercicio de vigilancia, **pueden ser utilizadas para bloquear la comunicación de los dispositivos conectados**”, explica el documento.