# Ciberpatrullaje: ¿vigilar y castigar por las dudas?

*María Alicia Bernárdez**

La humanidad suele redundar en puntos comunes. Algunas innovaciones que parecen disruptivas no hacen más que actualizar viejos dilemas. Tropezamos con la misma piedra, incluso en terrenos nuevos.

En un junio particularmente convulsionado para la política argentina entró en vigencia el Decreto N° 383/2025, que reestructura la Policía Federal Argentina (PFA). En sintonía, la Resolución N° 428/2024 del Ministerio de Seguridad instala oficialmente la figura del ciberpatrullaje. La justificación oficial habla de adaptar la tarea policial a los nuevos entornos delictivos digitales.

Según el documento, las fuerzas de seguridad están habilitadas para patrullar en "sitios web de acceso público y fuentes digitales abiertas" para detectar delitos como la trata de personas, el tráfico de armas o el narcotráfico, así como nuevas amenazas como el fraude con criptomonedas (Boletín Oficial). El protocolo establece que no se podrán recolectar datos sensibles ni almacenar información sin orden judicial, y que deberá respetarse la libertad de expresión. A su vez, habilita el uso de inteligencia artificial bajo "supervisión humana adecuada". Todo esto abre un abanico de controversias jurídicas y democráticas.

* Lic. en Gestión Gubernamental - UNPAZ.

Como en la vieja alegoría de la caverna de Platón, lo que los usuarios ven en redes, buscadores o plataformas, muchas veces está filtrado por algoritmos invisibles o poderes que seleccionan qué mostrar. El ciberpatrullaje, entendido como vigilancia de fuentes abiertas, puede convertirse en esa instancia que opera entre sombras y reflejos: observa, clasifica y, a veces, interviene. ¿Pero quién vigila a quienes vigilan? ¿Con qué criterios eligen a sus "perseguidos"? ¿Qué límite hay entre lo privado y lo público? ¿Se usará para cazar falsos positivos?

## Seguridad nacional y vigilancia extendida

> Este decreto y su anexo reglamentario se suman al conjunto de medidas ya implementadas desde el gobierno nacional que vienen ampliando al infinito las facultades policiales, reduciendo controles y garantizando la impunidad de sus ejecutores y mandantes, lo que ya se refleja en el abultado aumento de los fusilamientos de gatillo fácil, las detenciones arbitrarias y la represión cotidiana a la protesta social,

escribió María del Carmen Verdú, abogada de CORREPI.

Se refiere al hecho de que la resolución se inserta en un contexto más amplio maquillado tras un cambio de nombre: la vuelta oficial al nombre SIDE, tras la decisión del Ejecutivo de abandonar la denominación Agencia Federal de Inteligencia (AFI). A esto se suma la reasignación del área de ciberseguridad a su órbita, la aprobación del Plan de Inteligencia Nacional –que prioriza la seguridad nacional como eje rector– y un aumento significativo en los fondos destinados a tareas de monitoreo y vigilancia. El ciberpatrullaje es una pieza fundamental, un engranaje difícil de institucionalizar que tiende a expandir las funciones de inteligencia hacia el espacio digital.

Las voces oficiales argumentan que "el Estado no puede quedarse afuera del mundo digital donde hoy también se delinque", como expresó en 2024 la ministra Patricia Bullrich (*Página 12*). Se trata, dicen, de llevar el viejo patrullaje preventivo a la dimensión virtual.

Sin embargo, varias organizaciones sociales y expertos en derechos digitales advirtieron que el decreto no fue debatido en el Congreso y que sus definiciones son demasiado amplias o vagas. Como señala Lucía Camacho, del Observatorio Legislativo del CELE, la norma "habilita un monitoreo difuso y discrecional, que no está suficientemente regulado ni supervisado" (CELE).

Para ver cómo lo hacen, sin dudas hay que mirar el Boletín Oficial como nunca antes. En julio, publicaron dos resoluciones más: 828/2025 y 829/2025. Con ellas, el Ministerio de Seguridad avanzó en la formalización de un esquema de inteligencia digital que reactiva y regula viejas prácticas de infiltración. La primera norma autoriza a las fuerzas federales a desplegar agentes encubiertos en redes sociales y plataformas digitales, con identidades ficticias creadas a partir de datos del Renaper. La se-

gunda, en paralelo, crea un Consejo Académico designado por el Ejecutivo, encargado de capacitar a estos agentes y supervisar su despliegue operativo.

## Jurisprudencia comparada: consensos y límites

Otros países ya enfrentaron este debate. Tenemos cientos de ejemplos. En España, el Tribunal Supremo avaló ciertas formas de vigilancia digital, pero en 2020, el Ministerio del Interior debió limitar las acciones tras una polémica por patrullajes encubiertos en redes sociales. Se alertó que podrían incidir sobre la opinión pública o condicionar protestas. En palabras de la jurista española Paloma Llaneza: "No es lo mismo observar lo que circula que intervenir en la circulación".

En Alemania, la Corte declaró inconstitucional en 2020 el sistema de vigilancia digital automática del Servicio de Inteligencia Exterior por afectar derechos fundamentales sin las debidas garantías.

En América Latina el ciberpatrullaje, aunque se presenta como medida preventiva del delito, en la práctica ha sido un claro sistema de vigilancia que viabilizó, judicializar o intimidar a personas por ejercer su libertad de expresión.

> En Perú, se firmaron convenios para entrenar cibersoldados, en alianza con una empresa israelí, país cuestionado por sus tecnologías de vigilancia, importando modelos de guerra digital sin debate. En Colombia, el ciberpatrullaje es una práctica oficial de la Policía Judicial para recolectar información pública, sin garantías de proporcionalidad.

Así lo explicita Ximena Cuzcano en un artículo para *Derechos Digitales*. Y en Brasil una sátira sobre Bolsonaro terminó en una detención y hubo casos similares en Uruguay y México.

## ¿Prevención o precrimen?

Se problematiza la existencia de sistemas de vigilancia cuya escalabilidad no tiene precedentes, se polemiza sobre todo por su alcance, supervisión y límites democráticos. ¿Se necesita orden judicial para patrullar las redes? ¿Los agentes se identifican o simulan perfiles civiles? ¿Quién fiscaliza el uso de esa información? ¿Qué margen hay para el abuso, el error o la estigmatización?

Como señala *Chequeado*, el uso de inteligencia artificial agrava la preocupación: ¿quién programa los algoritmos? ¿Qué sesgos incorporan? ¿Qué sucede si clasifican erróneamente a alguien como "sospechoso"? Sobran ejemplos al respecto. La vigilancia algorítmica puede funcionar como una caja negra, opaca al control ciudadano.

En este punto, las distopías dejan de ser mera ficción. La película *Minority report* (2002), dirigida por Steven Spielberg, anticipa un sistema de justicia basado en la predicción del crimen, donde las personas son arrestadas por delitos que aún no cometieron. "No hay garantías procesales posibles si el Estado cree saber de antemano lo que uno hará", advertía el filósofo Byung-Chul Han. La analogía no es caprichosa: cuando la prevención se vuelve presunción, la libertad individual corre peligro.

## Del espacio público al espacio privado: una frontera difusa

Quienes defienden el ciberpatrullaje argumentan que las redes constituyen espacio público. Pero en verdad, se trata de un híbrido complejo, donde lo personal se vuelve visible y lo privado puede ser rastreado. La Corte Interamericana de Derechos Humanos ha sostenido que la vigilancia estatal debe cumplir con principios de legalidad, necesidad y proporcionalidad (*caso Escher y otros vs. Brasil*, 2009).

Desde organizaciones como Access Now y Fundación Vía Libre se advierte que el monitoreo en redes puede convertirse en una herramienta de control social, sobre todo en contextos de conflicto o protesta. La socióloga Natalia Aruguete advierte que "la vigilancia digital puede funcionar como un mecanismo de inhibición del disenso, aun sin llegar a la represión directa" (*Tiempo Argentino*).

La posibilidad de ser observados –incluso sin saber por quién ni cuándo– modifica los comportamientos, condiciona el lenguaje, limita la protesta.

## Pensar libremente, ¿un privilegio?

En tiempos de democracia, pensar libremente no debería generar sospechas. Pero si lo digital se convierte en un territorio policial, la sospecha se convierte en método. Como en la caverna de Platón, la ciudadanía corre el riesgo de confundir vigilancia con iluminación, sombras con realidad.

El filósofo Giorgio Agamben escribió que "la excepción no es lo contrario del derecho, sino su técnica más eficaz". Si el ciberpatrullaje se instala como normalidad sin debate, sin límites, sin controles, podríamos estar naturalizando una excepción permanente.

¿Volver a tropezar con la misma piedra?