



GOBIERNO, ¿ESPÍA?

GABRIEL TORRES ESPINOZA / PROFESOR E INVESTIGADOR DE LA UNIVERSIDAD DE GUADALAJARA @GABRIELTORRES

La verdadera amenaza no es que el Estado tenga acceso a los datos, sino que los tenga sin control

La polarización del debate público en México ha conducido, no pocas veces, a discusiones marcadas por el maniqueísmo, la desinformación o el oportunismo político. Tal es el caso del reciente paquete legislativo en materia de seguridad e inteligencia, aprobado en el Congreso de la Unión, que incluye la creación de una CURP biométrica y el fortalecimiento de las capacidades del Estado para el cruce de bases de datos. Inmediatamente, una parte de la opinión pública alzó la voz para advertir la supuesta instauración de un “gobierno espía”. Se trató de una reacción automática –e incluso poco reflexiva–, que reduce un tema complejo a una consigna alarmista.

Presentar el acceso a datos por parte del Estado, como una renuncia a los derechos civiles, es un error conceptual de origen. El acceso a información personal no puede equipararse al espionaje, si dicho acceso está regulado, justificado, limitado y supervisado por instituciones descentradas y por el Poder Judicial. Como advierte Carlos A. Pérez Ricart (2025), “la inteligencia no

es sinónimo de autoritarismo si se ejerce bajo controles democráticos”. No se puede exigir que el Estado actúe con eficacia ante la violencia criminal, mientras se le niegan las herramientas mínimas para hacerlo, en un mundo digital.

Un Estado sin capacidad de cruce de datos, sin inteligencia estratégica y sin plataformas interoperables, está condenado a la ineficacia, la descoordinación y la irrelevancia. Según el Inegi (Envipe 2023), 94.2% de los delitos no se denuncian o no se investigan en México. ¿Cómo puede combatirse la

impunidad con fiscalías que operan en papel, policías sin datos en tiempo real y tribunales saturados de expedientes inconexos? La fragmentación institucional y la carencia de interoperabilidad tecnológica no son sólo fallas técnicas, sino factores estructurales que alimentan la violencia y minan la confianza ciudadana. Y, sin embargo, el contraste más paradójico está en el comporta-

miento cotidiano de millones de personas. Cada día, los ciudadanos mexicanos entregan voluntariamente sus datos biométricos y personales a bancos, aerolíneas, redes sociales, plataformas de

streaming o aplicaciones móviles. Se autoriza la localización GPS, el reconocimiento facial, el historial de consumo, las preferencias políticas, las conversaciones privadas. Pero se rechaza que el Estado –único responsable legítimo del uso de la fuerza pública y de la procuración de justicia– tenga acceso

a los mismos datos para prevenir delitos, identificar cuerpos o esclarecer desapariciones. ¿Es esto una defensa férrea de la privacidad o una forma encubierta de autocomplacencia colectiva? La verdadera amenaza no es que el Estado tenga acceso a los datos, sino que los tenga sin control; o, peor aún que no los tenga en absoluto y condene la política de seguridad pública, a la ceguera operativa.

“Un Estado sin capacidad de cruce de datos, sin inteligencia estratégica y sin plataformas interoperables, está condenado a la ineficacia”.

