



Manuel Alejandro Guerrero

Identificación Digital, ¿amenaza a la privacidad?

Los estados modernos siempre han buscado consolidar el poder. Sin embargo, en las democracias modernas, los controles constitucionales, los derechos humanos y las libertades civiles históricamente han limitado la extralimitación del gobierno.

Hoy en día, la tecnología está alterando ese equilibrio. Incluso en democracias consolidadas, los gobiernos están explorando maneras de ampliar las facultades de vigilancia, utilizando nuevas herramientas digitales que pueden rastrear, monitorear y centralizar los datos de sus ciudadanos de maneras sin precedentes.

El sistema de identificación digital propuesto por el Reino Unido, denominado "BritCard", ilustra tanto las promesas como los riesgos. Las autoridades afirman que, con este sistema, se simplificará el acceso a los servicios públicos, se verificarán los derechos laborales y se evitarán fraudes. Sin embargo, los críticos advierten que podría convertirse en una vigilancia masiva, vinculando datos de redes sociales, banca, salud y hasta vacunación. Todo esto, sin mencionar los riesgos de hackeo y seguridad al contar con una base de datos amplísima y centralizada. La preocupación se agrava por la participación de empresas tecnológicas privadas, como Oracle, que ven la centralización de datos ciudadanos como una oportunidad comercial, pero también —y no es menor— de control del comportamiento.

Estados Unidos ofrece lecciones similares. Iniciativas como la Real ID y las licencias de conducir móviles, junto con programas federales avanzados de vigilancia, demuestran cómo la tecnología puede combinarse con las facultades estatales para monitorear a las personas —algo que ha apoyado la actual administración Trump—, a veces sin la supervisión ni el consentimiento adecuados de sus usuarios. Mientras tanto, el sistema Aadhaar de la India, a pesar de la aprobación de la Corte Suprema, pone de manifiesto los peligros: millones

de personas han sido excluidas de servicios esenciales debido a errores, persisten los riesgos para la privacidad y la supervisión independiente es limitada.

México no puede ignorar estas lecciones. La Ley General de Población establece la CURP Biométrica como nueva identificación —obligatoria para todos los efectos prácticos de acceder a trámites y servicios— y otorga al gobierno facultades discrecionales para rastrear nuestros datos. Más allá de las posibilidades de crear y resguardar debidamente una base de datos tan inmensa y costosa, la cuestión aquí es que la CURP Biométrica debe interpretarse en el contexto de lo que sucede en el último año: el desmantelamiento de los pesos y contrapesos que protegen contra el abuso de poder (desde el Inai hasta la Suprema Corte) y una serie de intentos de aprobar regulaciones que otorgan al Estado poderes de vigilancia irresponsables. En algunos casos, estos intentos han fracasado —como la revocación del artículo 109 de la Ley de Telecomunicaciones o la iniciativa de un representante en el Congreso para castigar con prisión a quienes creen y difundan memes, stickers y deepfakes de políticos y servidores públicos—, pero en otros han sido aprobados. Estos son los casos de la Ley del Sistema Nacional de Investigación e Inteligencia y la CURP Biométrica. Estos días, el Senado tendrá la última palabra sobre la reforma al Código Fiscal, que da acceso permanente y en tiempo real a la información de las plataformas respecto de todo tipo de transacciones comerciales, pero sin las debidas protecciones, prevenciones y medidas legales que aseguren que dicho acceso sea proporcional, no abusivo y protector de la privacidad.