ECIJA

OPINIÓN

Vigilancia digital, control ideológico y el riesgo de criminalizar el pensamiento: una mirada jurídica a los modelos autoritarios del siglo XXI

En 2019, The New York Times publicó más de 400 páginas de documentos internos del gobierno chino que detallaban el funcionamiento de los centros de "reeducación" en Xinjiang. Lo que reveló fue un sistema que no dependía tanto de guardias y rejas, sino de algoritmos...

por Ricardo Chacón
Socio @ ECIJA México

Uso público

Highlights

- En 2019, los Xinjiang Papers revelaron cómo China utilizó inteligencia artificial y vigilancia masiva para controlar ideológicamente a minorías, evidenciando el poder represivo de la tecnología sin contrapesos legales.

- Europa y Estados Unidos ya establecen límites: el AI Act europeo clasifica el reconocimiento facial en espacios públicos como "riesgo inaceptable", y tribunales estadounidenses lo asimilan a una búsqueda inconstitucional sin orden judicial.

- México enfrenta un vacío normativo: sistemas como el C5 operan sin reglas claras sobre almacenamiento, uso o supervisión de datos biométricos, lo que genera riesgos legales y de derechos humanos.

- Urge un marco regulatorio que combine seguridad y libertad: controles judiciales, transparencia, proporcionalidad y responsabilidad empresarial en el uso de tecnologías de vigilancia e inteligencia artificial.

Vigilancia digital, control ideológico y el riesgo de criminalizar el pensamiento: una mirada jurídica a los modelos autoritarios del siglo XXI

Por Ricardo Chacón

En 2019, The New York Times publicó más de 400 páginas de documentos internos del gobierno chino que detallaban el funcionamiento de los centros de "reeducación" en Xinjiang[1]. Lo que reveló fue un sistema que no dependía tanto de guardias y rejas, sino de algoritmos. Reconocimiento facial en cada esquina, análisis predictivo de comportamiento, bases de datos que cruzaban historial de compras con visitas a mezquitas, sensores en teléfonos que detectaban lectura del Corán... La tecnología no vigilaba crímenes; vigilaba ideas. Y lo hacía con una precisión que ningún régimen autoritario del siglo XX había logrado[2].

Esto no es ciencia ficción distópica ni un problema que le corresponda únicamente a organismos internacionales. Es el presente de la vigilancia digital, y sus implicaciones jurídicas nos alcanzan directamente. Porque las mismas empresas que desarrollaron reconocimiento facial para Xinjiang venden tecnología "gemela" en América Latina. Porque los sistemas de video vigilancia inteligente que operan hoy en la Ciudad de México, Monterrey o Guadalajara usan arquitecturas similares. Y porque hasta ahora, ninguna ley mexicana establece con claridad qué puede y qué no puede hacer un algoritmo de vigilancia con los datos biométricos de millones de personas.

El derecho internacional tiene algo que decir al respecto, aunque parezca lejano. Los artículos 9, 12, 18 y 19 del Pacto Internacional de Derechos Civiles y Políticos no son letra muerta: prohíben la detención arbitraria, la persecución por creencias y cualquier forma de vigilancia que vulnere la libertad de pensamiento[3]. La Convención contra la Tortura impone una prohibición absoluta e incondicional que ningún Estado puede suspender, incluso en situaciones de emergencia o supuesta seguridad nacional. En ese contexto, cuando un algoritmo decide quién es 'sospechoso' basándose en religiosidad, afiliación política o perfil ideológico, no se trata simplemente de vigilancia: constituye un método que, si anula la autonomía o busca intimidar de forma sistemática, podría caer dentro del espectro de tratos degradantes o abuso institucional[4]. Estamos ante una forma sofisticada de represión preventiva.

La Unión Europea entendió esto antes que nadie. El AI Act, que entró en vigor este año, clasifica el reconocimiento facial en tiempo real en espacios públicos como "riesgo inaceptable" salvo casos excepcionales y bajo supervisión judicial estricta[5]. No se trata de prohibir la tecnología, sino de someterla a un control equivalente al que se exige para allanar un domicilio o intervenir una comunicación privada. Alemania fue más allá: en 2023 su Tribunal Constitucional anuló un sistema

[1] The Washington Post. Uighurs and their supporters decry Chinese 'concentration camps,' 'genocide' after Xinjiang documents leaked https://www.washingtonpost.com/world/2019/11/17/uighurs-their-supporters-decry-chinese-concentration-camps-genocide-after-xinjiang-documents-leaked/

[2] PBS News. Leaked docs give inside view of China's mass detention camps https://www.pbs.org/newshour/show/leaked-docs-give-inside-view-of-chinas-mass-detention-camps

[3] United Nations - International Covenant on Civil and Political Rights https://treaties.un.org/untc/Pages/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf

[4] Equality & Human Rights Commission - Convention against Torture & other Inhuman, Degrading Treatment or Punishment. https://sthelenaehrc.org/convention-against-torture-other-inhuman-degrading-treatment-or-punishment/

[5] Biometric Update - EU issues guidelines clarifying banned AI uses. https://www.biometricupdate.com/202502/eu-issues-guidelines-clarifying-banned-ai-uses

de vigilancia predictiva en Hamburgo por violar el derecho al libre desarrollo de la personalidad[6]. El argumento fue simple y contundente: nadie puede vivir libremente si sabe que un algoritmo está evaluando constantemente su comportamiento para predecir si cometerá un delito.

En Estados Unidos el camino ha sido distinto pero converge en el mismo punto. La FTC no tiene una ley específica de IA, pero ha comenzado a aplicar normas de protección al consumidor para sancionar usos engañosos o discriminatorios de algoritmos. Lo interesante es que varios estados —Massachusetts[7], California[8], Illinois[9]— prohibieron o restringieron severamente el reconocimiento facial en manos de autoridades locales. La razón no fue tecnológica, fue constitucional: la Cuarta Enmienda protege contra búsquedas irrazonables, y un sistema que escanea permanentemente los rostros de todas las personas en un espacio público equivale a una búsqueda masiva y continua sin causa probable.

México, en cambio, opera en un limbo regulatorio peligroso. Las ciudades han instalado miles de cámaras con capacidad de reconocimiento facial —el C5 de la Ciudad de México es uno de los sistemas más grandes de América Latina— pero no existe un solo ordenamiento que regule su uso, que obligue a transparentar los algoritmos que procesan esos datos, que establezca cuánto tiempo se almacenan las imágenes o que garantice el derecho de las personas a saber si están siendo rastreadas. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares no aplica a autoridades. La Ley General de Transparencia exige publicar información, pero no regula el uso de tecnologías de vigilancia. Y la Constitución protege la privacidad, sí, pero la Suprema Corte no ha tenido oportunidad de pronunciarse sobre si el reconocimiento facial masivo y automatizado viola ese derecho.

Este vacío, además de plantear un problema de libertades civiles, es un riesgo operativo y legal para cualquier empresa que desarrolle, venda o implemente estas tecnologías en México. Imaginemos el caso de una compañía de software que provee análisis de video inteligente a gobiernos estatales. Hoy no existe claridad sobre qué datos pueden procesarse, bajo qué condiciones, ni con qué salvaguardas técnicas o legales. Tampoco se ha definido con precisión quién asume la responsabilidad cuando un sistema genera falsos positivos o se emplea con fines distintos a los autorizados. Si en el futuro la Corte declarara inconstitucional el uso de determinadas tecnologías de reconocimiento facial, la pregunta sería inevitable: ¿qué ocurriría con los contratos vigentes? ¿Quién respondería por los daños ocasionados? ¿La empresa desarrolladora? ¿La autoridad contratante? O ambos.

Las empresas serias ya lo están notando. En Europa, proveedores de tecnología de reconocimiento facial comenzaron a incluir cláusulas de cumplimiento con el AI Act en sus contratos, a realizar auditorías de sesgo algorítmico y a documentar exhaustivamente cómo entrenan sus modelos. En Estados Unidos, algunas simplemente se salieron del mercado de vigilancia gubernamental porque el riesgo reputacional y legal no valía la pena. En México todavía no llegamos ahí, pero

[6] Bundesverfassungsgericht Federal Constitutional Court - Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html

[7] En la ley M.G.L. c.6 § 220 de Massachusetts (entrada en vigor el 1 de julio de 2021), se exige que los organismos policiales que soliciten o realicen búsquedas con reconocimiento facial lo hagan por solicitud por escrito, solo cuando haya orden judicial o en casos de emergencia. (https://www.mass.gov/doc/facial-recognition-report-september-1-2021/download)

[8] Se aprobó el proyecto de ley AB 1814 que busca prohibir que un match de reconocimiento facial sea el único fundamento para probable causa o para dictar una orden. (https://sjud.senate.ca.gov/system/files/2024-06/ab-1814-ting-sjud-analysis.pdf)

[9] En Illinois existe la Biometric Information Privacy Act (BIPA), que impone fuertes restricciones al uso de datos biométricos por entidades privadas sin consentimiento. Si bien no se dirige principalmente al uso por autoridades, es una de las leyes más robustas en EE. UU. sobre reconocimiento facial. (https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa)

cuando llegue la regulación —y llegará, porque la presión internacional y social lo exigirá— muchas empresas descubrirán que llevan años operando en una zona gris que de pronto se volvió ilegal.

Por eso urge que esta conversación llegue al Congreso, pero no como bandera ideológica sino como necesidad técnica. México necesita una ley que regule el uso gubernamental de inteligencia artificial en seguridad pública, que establezca los mismos controles que existen para otras formas de vigilancia intrusiva: orden judicial, proporcionalidad, temporalidad limitada, supervisión independiente. Y necesita también regular el lado privado: las empresas que recopilan datos biométricos, que hacen perfilamiento predictivo, que venden análisis de comportamiento. Porque el autoritarismo tecnológico no siempre viene del Estado; a veces viene disfrazado de "personalización de servicios" o "mejora de la experiencia del usuario".

Para los abogados y para quienes asesoramos a empresas tecnológicas, el mensaje es claro: la gobernanza de estos sistemas ya no es opcional. Implementar reconocimiento facial, análisis predictivo o cualquier forma de vigilancia automatizada sin protocolos claros de protección de datos, sin evaluaciones de impacto en derechos humanos, sin mecanismos de auditoría y sin transparencia sobre cómo funcionan los algoritmos es, cada vez más, una apuesta de altísimo riesgo. La pregunta no es si vendrá la regulación, sino qué tan preparados estaremos cuando llegue.

La defensa del pensamiento libre no es un lujo de sociedades prósperas. Es el cimiento de cualquier democracia funcional. Las tecnologías de vigilancia llegaron para quedarse, pero su legitimidad dependerá enteramente de los límites que sepamos imponerles. La verdadera innovación no consiste en lo que la inteligencia artificial puede hacer, sino en lo que una sociedad decide no permitirle hacer. Y esa decisión, en México, todavía está pendiente.

Ricardo Chacón es socio y director de ECIJA México.

ECIJA México

info@ecija.com

T. +52 55 5662 6840