



3.- Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Reconocimiento facial en espacios públicos: ¿más seguridad o menos libertad?

Experta: Victoria Hernández. Grupo Sorolla Educación

Email: vhernandez@gruposorolla.es

Introducción

El reconocimiento facial es una tecnología biométrica que permite comparar la imagen de un rostro con una base de datos para verificar o establecer la identidad de una persona. En los últimos años, su utilización se ha extendido en aeropuertos, estaciones, estadios, fronteras y otros espacios de acceso público. Aunque puede emplearse con finalidades legítimas, como la localización de una persona desaparecida o la investigación de delitos graves, su uso también plantea riesgos importantes para la privacidad, la igualdad y las libertades democráticas.

Los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconocen, respectivamente, el derecho al respeto de la vida privada y familiar y el derecho a la protección de los datos personales. El reconocimiento facial afecta directamente a ambos derechos, ya que permite tratar datos biométricos y, en determinados casos, identificar a personas que no han cometido ningún delito y que simplemente transitan por un espacio público. Sin embargo, las autoridades policiales y algunos gobiernos consideran que esta tecnología puede ser útil para prevenir amenazas graves y mejorar la seguridad de la ciudadanía.

La Unión Europea ha intentado responder a este dilema mediante el Reglamento (UE) 2024/1689, conocido como Reglamento de Inteligencia Artificial o AI Act. Esta norma establece una regulación basada en el nivel de riesgo de los sistemas de inteligencia artificial y prohíbe, con excepciones muy limitadas, la identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales. Las prohibiciones del Reglamento comenzaron a aplicarse el 2 de febrero de 2025.

Contexto

El reconocimiento facial funciona mediante algoritmos que analizan determinados rasgos del rostro y los comparan con imágenes incluidas en una base de datos. Conviene distinguir



entre la verificación biométrica, que confirma si una persona es quien afirma ser —por ejemplo, al utilizar un sistema de acceso autorizado—, y la identificación biométrica remota, que busca determinar quién es una persona desconocida comparando su rostro con una base de datos. Esta segunda modalidad tiene un impacto mucho mayor sobre la privacidad, especialmente cuando se utiliza en lugares abiertos al público.

También existe una diferencia entre la identificación realizada en tiempo real y la identificación a posteriori. La identificación en tiempo real se realiza con imágenes en directo o casi en directo, por ejemplo, a través de cámaras de videovigilancia. La identificación a posteriori analiza imágenes o grabaciones obtenidas previamente. Ambas pueden ser intrusivas, pero la identificación en tiempo real es especialmente sensible porque permite vigilar y localizar a una persona mientras se encuentra en un espacio público.

Uno de los principales riesgos de esta tecnología es el tratamiento masivo de datos biométricos. A diferencia de una contraseña, el rostro no puede cambiarse fácilmente si los datos se filtran, se reutilizan o se emplean de forma indebida. Además, una persona puede ser captada por una cámara sin haber dado su consentimiento, sin saber que está siendo identificada y sin tener una forma clara de impugnar el uso de sus datos.

Otro problema importante es el sesgo algorítmico. Diversas investigaciones han demostrado que los sistemas de reconocimiento facial no presentan el mismo nivel de precisión para todos los grupos de población. Los errores pueden variar según factores como la edad, el sexo o el origen de las personas. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha documentado diferencias demográficas en las tasas de error de numerosos algoritmos de reconocimiento facial. Si un sistema identifica erróneamente a una persona, las consecuencias pueden ser graves: controles injustificados, investigaciones policiales basadas en información incorrecta, daños a la reputación o discriminación.

La vigilancia facial también puede producir un efecto disuasorio sobre las libertades democráticas. Si una persona cree que puede ser identificada automáticamente al asistir a una manifestación, a una reunión política, a una protesta o a un acto religioso, podría decidir no participar. Por ello, el debate no se limita a la privacidad individual: también afecta a la libertad de expresión, reunión, asociación y circulación.

Ante estos riesgos, el AI Act prohíbe como regla general el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales. No obstante, los Estados miembros pueden establecer excepciones legales y muy limitadas para la búsqueda de víctimas concretas, incluidas personas desaparecidas; para



prevenir una amenaza específica y grave contra la vida o la seguridad física de las personas, o un atentado terrorista; y para localizar o identificar a sospechosos de determinados delitos especialmente graves.

Estas excepciones no permiten una vigilancia indiscriminada de la población. El uso debe limitarse a confirmar la identidad de una persona que sea un objetivo específico, debe ser necesario y proporcionado, y ha de restringirse en el tiempo, el espacio geográfico y el número de personas afectadas. Como regla general, también requiere autorización previa de una autoridad judicial o de una autoridad administrativa independiente cuya decisión sea vinculante.

Principales enfoques

La solución al debate sobre el reconocimiento facial en espacios públicos no es sencilla. Existen posiciones muy diferentes, ya que entran en conflicto valores importantes como la seguridad pública, la privacidad, la igualdad y la protección de las libertades democráticas.

Quienes defienden una prohibición total consideran que ningún objetivo de seguridad justifica la vigilancia biométrica en espacios públicos. Organizaciones como Amnistía Internacional y European Digital Rights consideran que la identificación biométrica remota puede facilitar formas de vigilancia masiva y afectar especialmente a colectivos vulnerables, activistas, periodistas, personas migrantes y minorías étnicas. Desde esta perspectiva, las excepciones previstas por el AI Act pueden abrir la puerta a usos cada vez más amplios de la tecnología y dificultar el control ciudadano sobre las actuaciones policiales.

Desde la perspectiva de la seguridad pública, las fuerzas policiales y algunos gobiernos sostienen que el reconocimiento facial puede ser útil en situaciones concretas. Por ejemplo, podría contribuir a localizar a una persona desaparecida, identificar a un sospechoso de un delito especialmente grave o responder ante una amenaza terrorista. Quienes defienden este enfoque consideran que prohibir por completo la tecnología impediría utilizar una herramienta potencialmente eficaz para proteger a la población, siempre que existan controles estrictos y se respeten los derechos fundamentales.

Sin embargo, permitir el uso de esta tecnología sin límites claros también implicaría riesgos graves. El hecho de que un sistema pueda ser útil no significa que deba emplearse en cualquier circunstancia. Una identificación errónea puede afectar a personas inocentes, y la recopilación de imágenes de miles de ciudadanos puede normalizar una vigilancia constante. Por ello, la experiencia europea parece orientar la regulación hacia soluciones intermedias:



prohibición como regla general, excepciones muy restringidas, autorización previa, supervisión independiente, evaluación de impacto sobre los derechos fundamentales y obligación de utilizar el sistema solo cuando sea estrictamente necesario.

Este enfoque busca evitar dos extremos: renunciar por completo a una herramienta que podría tener utilidad en circunstancias excepcionales o aceptar que las autoridades puedan identificar automáticamente a cualquier persona en lugares públicos. El objetivo debe ser que la seguridad no se convierta en una excusa para reducir de forma permanente la privacidad y las libertades de la ciudadanía.

La Unión Europea debe desempeñar un papel importante en este ámbito porque el uso de tecnologías de vigilancia no afecta solo a un Estado, sino al conjunto de los derechos fundamentales dentro del espacio europeo. El AI Act establece normas comunes para todos los Estados miembros y exige controles específicos para determinados usos de la inteligencia artificial. Además, la regulación europea permite que los ciudadanos cuenten con una protección mínima común, aunque la aplicación práctica dependa también de las leyes nacionales y de las autoridades competentes de cada país. En España, la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) tiene como misión promover un uso ético y seguro de la IA y velar por el cumplimiento de la normativa aplicable, en coordinación con las autoridades competentes.

Preguntas clave

¿Debe prohibirse completamente el reconocimiento facial en espacios públicos? Esta pregunta plantea si los riesgos para la privacidad, la igualdad y las libertades democráticas son tan graves que ninguna excepción puede justificarse, o si existen situaciones excepcionales en las que el uso de esta tecnología puede ser legítimo.

¿Son suficientemente estrictas las excepciones previstas en el AI Act? El Reglamento permite determinadas excepciones para fines policiales, como la búsqueda de personas desaparecidas, la prevención de amenazas graves o la investigación de ciertos delitos. La cuestión es si estas condiciones son lo bastante precisas para impedir abusos y evitar que la excepción se convierta en la norma.

¿Cómo se puede garantizar que no haya discriminación algorítmica? Los sistemas de reconocimiento facial pueden presentar errores diferentes según la edad, el sexo o el origen de las personas. Es necesario debatir qué auditorías, pruebas independientes y mecanismos



de reparación deben establecerse antes de utilizar estas herramientas en contextos policiales.

¿Puede la seguridad pública justificar la identificación de personas en espacios abiertos al público? La protección frente al terrorismo, la trata de personas o la delincuencia grave es una responsabilidad esencial de los Estados. Sin embargo, esta necesidad debe equilibrarse con el derecho de las personas a desplazarse, reunirse y expresarse sin sentir que están siendo vigiladas permanentemente.

¿Hasta qué punto la vigilancia facial condiciona la participación democrática? La posibilidad de ser identificado mediante cámaras puede disuadir a algunas personas de acudir a protestas, reuniones o manifestaciones. Esta cuestión obliga a reflexionar sobre cómo proteger el espacio público como lugar de participación libre y plural.

¿Qué papel debe desempeñar la Unión Europea en la regulación de esta tecnología? La UE debe decidir hasta qué punto debe establecer normas comunes, exigir transparencia a las autoridades y garantizar mecanismos de supervisión eficaces. El objetivo es evitar que existan niveles muy distintos de protección de los derechos fundamentales entre los Estados miembros.

Conclusión

El reconocimiento facial en espacios públicos representa uno de los debates más complejos relacionados con la inteligencia artificial y los derechos fundamentales. Esta tecnología puede tener utilidad en situaciones excepcionales, como la búsqueda de una persona desaparecida o la respuesta ante una amenaza grave. Sin embargo, también puede afectar de forma profunda a la privacidad, a la igualdad de trato y a la libertad de participar en la vida pública sin temor a ser identificado automáticamente.

El AI Act constituye un paso importante al prohibir con carácter general la identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales y al permitir solo excepciones limitadas. No obstante, la efectividad de estas garantías dependerá de cómo las apliquen los Estados miembros, de la independencia de las autoridades que supervisen los sistemas y de la posibilidad real de que los ciudadanos conozcan, cuestionen y recurran los usos indebidos de sus datos biométricos.

Por ello, la utilización del reconocimiento facial debería estar sometida a los principios de necesidad, proporcionalidad, transparencia y control independiente. Europa tiene la



oportunidad de demostrar que es posible desarrollar y utilizar tecnologías avanzadas sin renunciar a los derechos y libertades que constituyen la base de una democracia. La seguridad pública es necesaria, pero solo será legítima si se construye respetando la dignidad, la privacidad y la libertad de todas las personas.

Fuentes y enlaces recomendados

- Carta de los Derechos Fundamentales de la Unión Europea, arts. 7 y 8.
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:12012P/TXT>
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act).
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es>
- Comisión Europea. AI Act: Shaping Europe's digital future.
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- Comisión Europea. Navigating the AI Act: preguntas frecuentes sobre prácticas prohibidas y excepciones. <https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act>
- National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT): Demographic Effects.
<https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects>
- NIST. Face Recognition Vendor Test (FRVT): programa y resultados de evaluación.
<https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt>
- European Digital Rights (EDRi). How to fight biometric mass surveillance after the AI Act: a legal and practical guide.
<https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/>
- Amnistía Internacional. EU: Bloc's decision to not ban public mass surveillance in AI Act sets a devastating global precedent.
<https://www.amnesty.org/en/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-global-precedent/>
- Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Información institucional y funciones. <https://aesia.digital.gob.es/en/es>