Aula de Estudios Estratégicos
Un espacio universitario para la investigación y el análisis estratégico de los desafíos de seguridad del siglo XXI.

isen | Centro Universitario

Seguridad y vigilancia en la era de la Inteligencia Artificial

DA.02-2026 06/08/2026

Francisco Rubio Damián

Resumen

La incorporación de la inteligencia artificial a las políticas de seguridad está modificando profundamente la forma en que las instituciones previenen, gestionan y responden a los riesgos. El artículo analiza la transición desde un modelo de vigilancia reactiva hacia otro basado en el análisis predictivo y la seguridad algorítmica, examinando sus principales aplicaciones en ámbitos como la videovigilancia inteligente, el reconocimiento biométrico, el análisis predictivo del delito, la gestión de fronteras y la ciberseguridad. Asimismo, estudia el marco jurídico español y europeo, valorando el papel del Reglamento de Inteligencia Artificial y de las garantías constitucionales en la protección de los derechos fundamentales. Finalmente, identifica los principales desafíos asociados a la transparencia, la rendición de cuentas, el control democrático y la preservación del equilibrio entre seguridad, innovación tecnológica y libertades públicas, defendiendo un modelo de gobernanza basado en una supervisión humana significativa y en mecanismos efectivos de control institucional.

Abstract

The integration of artificial intelligence into security policies is profoundly transforming the way institutions prevent, manage, and respond to risks. This article examines the transition from reactive surveillance to predictive, algorithm-driven security, analysing its main applications in intelligent video surveillance, biometric recognition, predictive policing, border management, and cybersecurity. It also explores the Spanish and European legal frameworks, assessing the role of the European Union Artificial Intelligence Act and constitutional safeguards in protecting fundamental rights. Finally, the paper identifies the main challenges related to transparency, accountability, democratic oversight, and the preservation of the balance between security, technological innovation, and civil liberties. It argues for a governance model based on meaningful human oversight and robust institutional accountability mechanisms.

Palabras clave

Inteligencia artificial; seguridad algorítmica; vigilancia; derechos fundamentales; gobernanza digital; Reglamento de Inteligencia Artificial.

Keywords

Artificial intelligence; algorithmic security; surveillance; fundamental rights; digital governance; Artificial Intelligence Act.

Cómo citar el artículo

Rubio Damián, Francisco. Seguridad y vigilancia en la era de la Inteligencia Artificial.

Aula de Estudios Estratégicos-Isen.

https://isen.es/aula-de-estudios-estrategicos/#publicaciones

Seguridad y vigilancia en la era de la Inteligencia Artificial

1. Cambio de paradigma.

La inteligencia artificial (IA) está transformando de manera profunda las políticas y prácticas de seguridad. En un contexto de amenazas complejas y recursos limitados, la IA mejora la capacidad de anticipación, detección y respuesta de las instituciones públicas. En particular, la vigilancia reactiva, es decir, la que se moviliza ante hechos consumados, pierde protagonismo frente a enfoques preventivos orientados a la clasificación y predicción de comportamientos de riesgo. Este cambio, impulsado por la capacidad de la IA para generar y procesar cantidades ingentes de datos, abre la posibilidad de que la seguridad no se sustente exclusivamente en indicios o sospechas concretas, sino también en probabilidades, patrones y perfiles generados algorítmicamente. La transformación tiene así un componente cuantitativo –más datos, más velocidad– y otro cualitativo, que altera la forma en que se define la amenaza y el momento en que interviene el Estado.

La dimensión predictiva no es la única novedad del nuevo paradigma de la vigilancia. Tradicionalmente centrada en personas o situaciones concretas, la IA permite hoy una vigilancia más difusa y distribuida, capaz de extenderse a espacios públicos, infraestructuras digitales y procedimientos administrativos ordinarios. Cámaras, sensores y bases de datos interconectadas, junto con sistemas automatizados, convierten actividades cotidianas en fuentes de información para la gestión de la seguridad. Este enfoque posibilita una actuación más temprana y coordinada, pero también implica que prácticas inicialmente concebidas para contextos excepcionales se integren de forma estable en la gestión rutinaria de la seguridad, difuminando el límite entre lo extraordinario y lo habitual.

Como vemos, anticipación, generalidad y normalización dan forma al hábitat de la seguridad algorítmica, un modelo en el que los sistemas automatizados identifican riesgos, priorizan intervenciones y recomiendan decisiones con impacto directo en derechos y libertades. Aunque formalmente la decisión última corresponda a un ser humano, la experiencia muestra que las recomendaciones algorítmicas condicionan significativamente la actuación de las personas. Esta tendencia humana a confiar en exceso en los sistemas automatizados, algoritmos o IA se le conoce como sesgo de automatización. De este modo, la lógica basada en datos y modelos opacos, propios de la IA, adquiere un rol protagonista en ámbitos tradicionalmente gobernados por criterios jurídicos, políticos y sociales.

La relevancia de este cambio es especialmente significativa en los ámbitos sensibles, es decir, aquellos donde las decisiones pueden ser irreversibles o difíciles de revertir y, además, relevantes, entendiendo por esto último que tienen un impacto directo sobre los derechos fundamentales y la dignidad de las personas. Junto a la salud, la justicia, la educación o la defensa, la seguridad exige estándares reforzados de precaución. Para ello, debería regirse por el principio de inocuidad, según el cual esa decisión, relevante e irreversible, debería ser adoptada por un ser humano. Desde esta perspectiva, la automatización no puede sustituir la responsabilidad humana en la decisión final, sino que debe integrarse de manera que preserve la posibilidad de juicio, control y rendición de cuentas por parte de las personas responsables.

2. Quién vigila hoy: actores y relaciones de poder

La IA se ha incorporado a un amplio abanico de actividades vinculadas a la seguridad y la vigilancia institucional. Con el objetivo de mejorar la eficacia operativa y la asignación de recursos, las fuerzas y cuerpos de seguridad emplean sistemas de análisis de datos, videovigilancia y apoyo a la toma de decisiones para tareas de prevención, investigación y mantenimiento del orden público. Los servicios de inteligencia, por su parte, integran herramientas avanzadas para el tratamiento masivo de información relevante para la seguridad nacional, mientras que, en el ámbito de la defensa, las actividades de inteligencia, vigilancia y reconocimiento resultan hoy inconcebibles sin el apoyo de tecnologías basadas en la IA. Por último, las administraciones públicas utilizan sistemas automatizados para la detección del fraude, la gestión de ayudas o el control migratorio, ampliando el alcance funcional de estas tecnologías más allá del ámbito estrictamente policial o militar.

Junto a la vigilancia pública, la vigilancia privada desempeña un importante papel en el ecosistema digital contemporáneo. Empresas tecnológicas y plataformas digitales recopilan y analizan grandes volúmenes de datos sobre comportamientos, relaciones y desplazamientos de las personas, generalmente con fines comerciales o de prestación de servicios. Estas prácticas permiten prestar servicios más personalizados y eficientes, pero también generan capacidades de observación y análisis con efectos significativos sobre la privacidad y otros derechos fundamentales. En muchos casos, el volumen y la granularidad de los datos gestionados por actores privados son comparables a los de las instituciones públicas, lo que plantea interrogantes sobre el equilibrio de poder informacional en la sociedad digital.

Uno de los rasgos distintivos del escenario actual es la creciente hibridación entre vigilancia pública y privada. Las administraciones dependen cada vez más de proveedores tecnológicos externos para diseñar, implementar y mantener sistemas de IA aplicados a la seguridad, lo que permite acceder a capacidades técnicas avanzadas difíciles de desarrollar internamente. Sin embargo, esta dependencia tecnológica dificulta la transparencia, la autonomía institucional y la rendición de cuentas. En este contexto, no siempre resulta claro qué sistemas se están utilizando, bajo qué criterios operan o quién asume la responsabilidad última de sus efectos, configurando una opacidad que se convierte en un elemento estructural del nuevo ecosistema de vigilancia.

3. IA y seguridad en la práctica: usos actuales y riesgos emergentes

3.1. Videovigilancia inteligente y reconocimiento biométrico

La incorporación de la IA a los sistemas de videovigilancia supone un salto cualitativo cuando estos dejan de limitarse a la observación y añaden la identificación automática de personas. El reconocimiento facial y otras técnicas biométricas transforman imágenes en datos personales especialmente sensibles, susceptibles de ser comparados, clasificados y reutilizados a gran escala. Estas tecnologías resultan particularmente resolutivas en contextos de alta complejidad operativa –grandes infraestructuras de transporte, eventos multitudinarios o entornos urbanos densamente poblados–, donde la identificación rápida de personas puede contribuir a conseguir objetivos legítimos de seguridad. Sin embargo, su uso plantea una alteración sustancial del equilibrio entre seguridad y derechos, al posibilitar formas de supervisión sistemática que no requieren una sospecha individualizada previa.

En el contexto español, el debate sobre el reconocimiento biométrico ha tenido una traducción jurídica concreta. Las autoridades de protección de datos han intervenido en varios supuestos para delimitar los márgenes de uso de estas tecnologías, subrayando que su despliegue exige una base legal clara, finalidades estrictamente definidas y garantías reforzadas. Resulta ilustrativa la actuación de la Agencia Española de Protección de Datos en relación con el uso de sistemas de reconocimiento facial en entornos abiertos al público, donde se ha considerado que la invocación genérica de la seguridad no es suficiente para justificar tratamientos biométricos masivos. Aunque estos pronunciamientos no cuestionan la legitimidad de la seguridad como objetivo, ponen de relieve que la proporcionalidad de estas tecnologías debe evaluarse con especial rigor, atendiendo a su carácter altamente intrusivo.

A escala europea, el reconocimiento biométrico en espacios públicos ha generado un debate aún más intenso. Mientras algunas autoridades locales y nacionales han explorado su uso en contextos específicos, otras han optado por restricciones o moratorias ante la dificultad de compatibilizar estas prácticas con los estándares de derechos fundamentales. Este debate se refleja de forma explícita en el Reglamento de Inteligencia Artificial, que establece una prohibición general del reconocimiento biométrico remoto en tiempo real en espacios públicos, acompañada de excepciones limitadas vinculadas a amenazas graves y sujetas a condiciones estrictas. La regulación europea no resuelve definitivamente el dilema, pero reconoce que se trata de uno de los usos de la inteligencia artificial con mayor impacto potencial sobre el carácter abierto y anónimo del espacio público.

Más allá del debate normativo, la videovigilancia inteligente se asocia a riesgos relacionados con la fiabilidad de los sistemas, los sesgos en los datos de entrenamiento o la falta de transparencia sobre su funcionamiento. Además, incluso cuando se plantean usos puntuales o excepcionales, existe un riesgo de normalización, de forma que, tecnologías diseñadas para responder a situaciones extraordinarias tienden a integrarse de forma permanente en la gestión cotidiana de la seguridad, redefiniendo de manera progresiva los límites del espacio público democrático.

3.2. Análisis predictivo y prevención del delito

El uso de sistemas de análisis predictivo en el ámbito de la seguridad introduce otro importante cambio en la lógica de la intervención pública. A diferencia de los modelos tradicionales centrados exclusivamente en la investigación de hechos consumados, estas herramientas buscan anticipar situaciones de riesgo mediante el análisis de datos históricos y la identificación de patrones estadísticos. Desde el punto de vista operativo, la IA permite una actuación más temprana, una priorización de recursos más eficiente y una mayor coherencia en la evaluación de situaciones complejas. Por tanto, en contextos caracterizados por una elevada carga de trabajo y decisiones urgentes, la automatización debe entenderse como un sólido instrumento de apoyo a la acción profesional y no como un sustituto automático de la decisión humana.

En todo caso, los sistemas de análisis predictivo desplazan el foco desde el delito consumado hacia el riesgo y desde la conducta concreta hacia la probabilidad, lo que redefine el concepto de sospecha y plantea serios interrogantes sobre la presunción de inocencia. Estos sistemas no operan sobre hechos probados, sino sobre probabilidades e, inevitablemente, se alimentan de datos que reflejan prácticas institucionales y desigualdades sociales. Como consecuencia, pueden reproducir sesgos estructurales y generar efectos acumulativos de estigmatización, especialmente en personas o entornos clasificados como de mayor riesgo. La dificultad reside en la posible inexactitud de las predicciones y su peso en la práctica decisoria: cuando una recomendación automatizada estructura de forma significativa el marco de actuación, la frontera entre apoyo técnico y decisión efectiva puede volverse difusa.

En el contexto español, el sistema VioGen constituye un ejemplo relevante y socialmente legitimado de análisis predictivo aplicado a la seguridad. Desarrollado y gestionado por el Ministerio del Interior, VioGen evalúa el riesgo en casos de violencia de género y orienta la adopción de medidas de protección con impacto directo en las víctimas y personas investigadas. Su aportación facilita una respuesta temprana y coordinada en un ámbito de extrema sensibilidad, donde la omisión o el retraso pueden tener consecuencias graves. El sistema no adopta decisiones de forma autónoma, sino que genera una valoración que debe ser integrada por los profesionales responsables junto con otros elementos del caso. Por lo tanto, estas recomendaciones, que se obtienen tras la combinación de múltiples variables difíciles de manejar de forma exclusivamente manual, no sustituyen la valoración profesional.

Precisamente por su valor y legitimidad, VioGen permite ilustrar con claridad uno de los dilemas centrales de la seguridad algorítmica. En entornos sensibles, caracterizados por decisiones relevantes y potencialmente irreversibles, la exigencia de intervención humana significativa no puede entenderse como una mera formalidad. Las cuestiones clave son, primero, si el profesional está preparado para apartarse de la recomendación automatizada y, segundo, si dispone de tiempo, información y respaldo institucional suficientes para ejercer un juicio verdaderamente deliberativo. En este punto el debate se conecta con el principio de inocuidad y con las recomendaciones de la UNESCO que subrayan que, en contextos de alto impacto, la decisión final debe recaer de forma inequívoca en una persona, capaz de asumir responsabilidad y rendir cuentas.

3.3. Control migratorio y gestión de fronteras

La aplicación de sistemas de IA al control migratorio y a la gestión de fronteras se ha intensificado en los últimos años en el marco de las políticas europeas de seguridad y gestión de flujos. Estas tecnologías se emplean para apoyar tareas como el análisis de grandes volúmenes de información, la detección de patrones de movilidad o la interoperabilidad entre bases de datos, especialmente en escenarios caracterizados por la urgencia operativa y la cooperación transnacional. Desde la perspectiva institucional, la automatización se presenta como una herramienta para mejorar la eficacia y la coherencia de decisiones que deben adoptarse en escenarios complejos y bajo fuerte presión temporal.

A escala europea, este enfoque se ha materializado en el desarrollo y la interconexión de grandes sistemas de información migratoria y fronteriza. Instrumentos como el Sistema de Información de Schengen, Eurodac o los sistemas de gestión de visados, coordinados en buena medida con el apoyo operativo de Frontex, incorporan de forma creciente funciones de análisis automatizado y cruce masivo de datos. Aunque estos sistemas no adoptan decisiones de manera autónoma, sí estructuran de forma decisiva el entorno en el que se toman decisiones relevantes sobre control fronterizo, retorno o acceso a procedimientos administrativos. Este diseño ha generado un amplio debate en el ámbito europeo sobre la transparencia de los criterios aplicados, la fiabilidad de los datos utilizados y la capacidad real de las personas afectadas para comprender y cuestionar los resultados obtenidos.

En el caso español, la utilización de tecnologías digitales en el ámbito migratorio no se ha traducido en limitaciones sistemáticas de la acogida ni del acceso a los procedimientos de protección internacional. España aplica estas herramientas en el marco de la normativa europea y de sus propias garantías constitucionales, lo que ha permitido mantener un enfoque garantista en comparación con otros contextos. Sin embargo, la participación plena en sistemas europeos interconectados implica que las lógicas de diseño, los estándares técnicos y las decisiones adoptadas a nivel de la Unión influyen directamente en las prácticas nacionales. En este sentido, el debate relevante no se centra tanto en actuaciones concretas ya desplegadas, sino en cómo se gobiernan estos sistemas y cómo se articulan mecanismos efectivos de información, revisión y recurso en un entorno crecientemente automatizado.

Desde una perspectiva de derechos digitales, el principal reto consiste en evitar que la eficiencia operativa y la gestión del riesgo desplacen progresivamente las garantías jurídicas. La automatización puede contribuir a una gestión más ordenada y coherente de los flujos migratorios, pero también puede generar efectos de opacidad y asimetría de poder si no se acompaña de controles adecuados. En este ámbito, como en otros usos de la inteligencia artificial en seguridad, la cuestión central va más allá de la mera existencia de sistemas tecnológicos avanzados y se debe enfocar en la capacidad para definir sus límites, supervisar su funcionamiento y corregir sus efectos cuando inciden de manera desproporcionada sobre derechos fundamentales.

3.4. Seguridad informática y ciberseguridad

En el ámbito de la seguridad informática y la ciberseguridad, la IA se ha consolidado como una herramienta esencial para la protección de infraestructuras digitales, servicios públicos y sistemas críticos. Ante un volumen creciente de ciberataques y vulnerabilidades, estos sistemas permiten analizar de manera continua grandes cantidades de datos procedentes de redes sociales y comunicaciones, identificar patrones anómalos y activar respuestas rápidas. En muchos casos, la automatización resulta imprescindible para gestionar amenazas que superan las capacidades humanas de análisis en tiempo real. Por tanto, y a diferencia de otros usos de la IA en seguridad, aquí la automatización no responde tanto a una opción estratégica como a una necesidad operativa: el volumen, la velocidad y la sofisticación de los ciberataques hacen inviable una respuesta basada exclusivamente en análisis humanos.

En España, estas capacidades se integran de manera sistemática en las estrategias públicas de ciberseguridad. Organismos como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN-CERT) o el Mando Conjunto del Ciberespacio (MCCE) utilizan herramientas avanzadas de análisis automatizado para la detección de amenazas, la gestión de incidentes y la protección de redes y servicios esenciales. A nivel europeo, esta aproximación se ve reforzada por iniciativas de cooperación y coordinación que reconocen explícitamente el papel de la inteligencia artificial como elemento clave para la defensa frente a riesgos cibernéticos transnacionales. En este contexto, el uso de IA se percibe de forma mayoritariamente positiva, al orientarse a la protección de sistemas y servicios de los que depende el funcionamiento ordinario de la sociedad.

No obstante, incluso en este ámbito ampliamente consensuado, el uso de inteligencia artificial plantea cuestiones relevantes desde la perspectiva de los derechos digitales. La monitorización continua de redes y comunicaciones puede implicar el tratamiento de metadatos y, en determinados supuestos, de contenidos, lo que exige salvaguardas adecuadas para evitar injerencias desproporcionadas en la privacidad o la libertad de expresión. Además, la dependencia de soluciones tecnológicas complejas, a menudo desarrolladas por proveedores externos, introduce desafíos en términos de transparencia, auditabilidad y control público de los sistemas empleados.

La experiencia de la ciberseguridad ofrece así una enseñanza valiosa para el conjunto del debate sobre IA y seguridad: incluso cuando el uso de la inteligencia artificial es ampliamente aceptado y socialmente necesario, resulta imprescindible acompañarlo de marcos claros de gobernanza, supervisión y rendición de cuentas. La legitimidad de estas herramientas no deriva únicamente de su eficacia técnica, sino de su integración en un ecosistema institucional que preserve las garantías democráticas y permita un control efectivo de sus efectos.

4. El marco jurídico español ante la seguridad algorítmica

El uso de sistemas de IA en el ámbito de la seguridad en España se inserta en un marco jurídico que reconoce de manera explícita la centralidad de los derechos fundamentales y somete la actuación de los poderes públicos a límites bien establecidos. La Constitución, la legislación sectorial y la normativa de protección de datos configuran un sistema en el que cualquier injerencia en derechos como la privacidad, la libertad personal o la igualdad debe apoyarse en una base legal suficiente y superar un juicio de proporcionalidad. Este marco no es meramente declarativo: en la práctica, ha permitido cuestionar, reconducir o limitar determinados usos tecnológicos cuando se ha considerado que no cumplían con las exigencias constitucionales, como ha puesto de manifiesto la jurisprudencia del Tribunal Constitucional y la actuación de autoridades independientes.

La introducción de sistemas algorítmicos en seguridad no invalida estas garantías, pero sí las somete a una presión específica. El ordenamiento jurídico español está bien equipado para evaluar decisiones singulares adoptadas por personas identificables, pero encuentra mayores dificultades cuando se enfrenta a sistemas que operan de manera continua, automatizada y a gran escala. En estos supuestos, cuestiones clásicas del Derecho público —como la identificación del acto decisorio, la motivación de la decisión o la atribución de responsabilidad— se vuelven más complejas. La inteligencia artificial no elimina la necesidad de cumplir con los principios de legalidad y proporcionalidad, pero obliga a reinterpretarlos en contextos en los que la intervención pública ya no adopta la forma de una decisión puntual, sino de una infraestructura técnica permanente.

Un ámbito especialmente revelador de esta tensión es el de los controles preventivos. La normativa vigente prevé instrumentos como las evaluaciones de impacto y otros mecanismos de análisis previo precisamente para anticipar riesgos sobre derechos fundamentales. Sin embargo, en el ámbito de la seguridad, estos controles tienden a desarrollarse en circuitos internos de la administración y con un grado limitado de publicidad, en parte por razones de confidencialidad operativa. Esto no implica necesariamente una ausencia de control, pero sí reduce la posibilidad de escrutinio externo y de debate público informado sobre la proporcionalidad de los sistemas antes de su despliegue. El control judicial, por su parte, sigue siendo una garantía central, pero su activación suele producirse de forma reactiva, una vez que los sistemas ya están en funcionamiento.

Desde esta perspectiva, el principal desafío del marco jurídico español no es la falta de normas, sino su capacidad para seguir siendo efectivo en un contexto de automatización creciente. La inteligencia artificial exige reforzar y adaptar garantías ya existentes para evitar que principios como la responsabilidad, la trazabilidad de las decisiones o la posibilidad de impugnación efectiva se diluyan en procesos técnicos difíciles de desentrañar. La cuestión central no es si el Derecho está siendo superado por la tecnología, sino si las instituciones jurídicas disponen de los instrumentos necesarios —y de la voluntad política— para asegurar que la incorporación de la IA en seguridad se produzca sin erosionar los fundamentos del Estado de derecho.

5. Europa como marco de límites, excepciones y legitimación

La Unión Europea ha asumido un papel central en la regulación de la IA, con el objetivo declarado de promover un desarrollo tecnológico compatible con los valores democráticos y los derechos fundamentales. Instrumentos como el Reglamento General de Protección de Datos (2016) y el Reglamento de Inteligencia Artificial (2024) han situado a la Unión como un referente internacional en la regulación de usos de alto riesgo. En el ámbito de la seguridad y la vigilancia, este enfoque se traduce en la introducción de prohibiciones explícitas, obligaciones reforzadas y exigencias de evaluación previa que buscan limitar los impactos más intrusivos de la automatización.

Al mismo tiempo, el marco europeo incorpora de forma expresa amplias excepciones cuando entran en juego finalidades vinculadas a la seguridad, el orden público o la prevención de delitos graves. El propio Reglamento de Inteligencia Artificial, que prohíbe con carácter general el reconocimiento biométrico remoto en espacios públicos, contempla supuestos excepcionales para usos policiales bajo determinadas condiciones. Esta arquitectura normativa refleja un equilibrio político deliberado: establecer límites claros sin cerrar por completo la puerta a tecnologías que los Estados consideran necesarias para responder a amenazas complejas. El resultado es un sistema que no elimina la vigilancia algorítmica, sino que la canaliza y, en cierto modo, la legitima bajo determinadas garantías formales.

Desde la perspectiva española, el marco europeo actúa simultáneamente como límite y como legitimación. Por un lado, impone obligaciones de evaluación, documentación y control que refuerzan las garantías existentes. Por otro, proporciona un marco de referencia que facilita la normalización de determinados usos de la IA en seguridad, siempre que se ajusten formalmente a los requisitos establecidos. La cuestión clave pasa así de ser si Europa permite o prohíbe determinados usos, a cómo se interpretan y aplican en la práctica las cláusulas de excepción, las obligaciones de control y los mecanismos de supervisión previstos. En ese margen de aplicación concreta se juega buena parte del equilibrio real entre seguridad, derechos y democracia.

6. Transparencia, control democrático y rendición de cuentas

La transparencia constituye uno de los principales desafíos en el uso de sistemas de IA, en general, y de los aplicados a la seguridad, en particular. A diferencia de otras políticas públicas, este ámbito combina de forma estructural tres factores que limitan el acceso a la información: la complejidad técnica de los sistemas utilizados, la frecuente externalización tecnológica y la invocación de razones de confidencialidad vinculadas a la eficacia operativa. Como resultado, incluso cuando existen marcos normativos que reconocen el derecho a la información y la publicidad de la actuación administrativa, el conocimiento público sobre qué tecnologías se emplean, con qué alcance y bajo qué criterios resulta a menudo fragmentario y difícil de reconstruir.

Esta opacidad no responde necesariamente a una voluntad deliberada de ocultación, sino a la forma en que se organizan los procesos de decisión y adquisición tecnológica en el ámbito de la seguridad. La información relevante suele dispersarse entre contratos, documentos técnicos y procedimientos internos que no están pensados para facilitar el escrutinio externo. En el caso de los sistemas basados en IA, esta dificultad se ve agravada por la dependencia de soluciones desarrolladas por terceros y por la utilización de modelos cuyo funcionamiento no resulta fácilmente explicable incluso para los propios operadores públicos. El desafío, por tanto, no es solo jurídico, sino también organizativo y técnico.

Los mecanismos de control preventivo previstos en el ordenamiento —como las evaluaciones de impacto o los análisis de proporcionalidad— adquieren en este contexto una importancia particular. Sin embargo, en el ámbito de la seguridad, estos instrumentos suelen desplegarse en circuitos internos de la administración y con un grado limitado de publicidad, lo que reduce su capacidad para generar debate público o control externo antes del despliegue de los sistemas. La confidencialidad operativa puede estar justificada en determinados aspectos, pero cuando se convierte en la regla general dificulta la evaluación social de riesgos que, por su naturaleza, afectan a derechos fundamentales. El control judicial sigue siendo una garantía central, pero su carácter predominantemente reactivo limita su eficacia preventiva frente a tecnologías que operan de forma continua.

El control democrático se articula principalmente a través de los parlamentos y de las autoridades independientes. En el caso del control parlamentario, este se ejerce habitualmente mediante instrumentos generales —preguntas, solicitudes de información o comparecencias— que permiten una fiscalización política relevante, pero no siempre un seguimiento técnico sostenido de sistemas complejos y en rápida evolución. La ausencia de estructuras estables y especializadas dificulta un control continuado de las tecnologías de vigilancia algorítmica. Por su parte, autoridades como la Agencia Española de Protección de Datos cuentan con competencias clave para supervisar determinados usos de la inteligencia artificial, pero se enfrentan a límites técnicos, materiales y competenciales cuando los sistemas son altamente complejos o se utilizan en contextos protegidos por regímenes de confidencialidad.

Desde la perspectiva de la rendición de cuentas, el principal riesgo no es la inexistencia de responsables, sino la difuminación de la responsabilidad a lo largo de cadenas técnicas y organizativas difíciles de desentrañar. Cuando las decisiones se apoyan en sistemas algorítmicos desarrollados por terceros, integrados en procesos administrativos complejos y utilizados por múltiples actores, resulta más difícil identificar quién debe responder por errores, sesgos o efectos desproporcionados. Garantizar una atribución clara de responsabilidades y mecanismos efectivos de revisión no es solo una exigencia jurídica, sino una condición necesaria para preservar la confianza ciudadana en el uso legítimo de la inteligencia artificial en seguridad.

7. Impactos democráticos de la vigilancia algorítmica

La expansión de sistemas de vigilancia basados en IA tiene efectos que trascienden los casos individuales y se proyectan sobre el funcionamiento cotidiano de la democracia. Más allá de los impactos directos sobre derechos concretos, la percepción de estar sometido a observación, análisis o evaluación automatizada puede influir en el comportamiento de las personas en el espacio público y digital. Este fenómeno, conocido en el debate público como efecto desaliento o chilling effect, ha sido ampliamente discutido en relación con tecnologías de vigilancia tradicionales y adquiere una nueva dimensión cuando la supervisión se apoya en sistemas automatizados de difícil comprensión para la ciudadanía.

En el contexto europeo, este debate ha emergido de forma recurrente en relación con el uso de tecnologías de reconocimiento biométrico y de análisis masivo de datos en espacios abiertos. Diversos informes institucionales y debates parlamentarios han advertido de que la mera posibilidad de identificación o seguimiento automatizado puede alterar la forma en que las personas ejercen derechos como la libertad de expresión, de reunión o de participación política, incluso cuando no existe una vigilancia individualizada efectiva. El impacto democrático no deriva tanto de una intervención concreta como de la modificación del entorno en el que se desarrollan las interacciones sociales, especialmente cuando los criterios de supervisión resultan opacos o difícilmente impugnables.

Estos efectos no se distribuyen de manera uniforme. La vigilancia algorítmica tiende a concentrarse en determinados espacios, actividades o colectivos definidos como de mayor riesgo, lo que puede reforzar percepciones de desigualdad ante la ley. Cuando ciertos grupos experimentan una supervisión más intensa o intrusiva, se debilita la confianza en la neutralidad de las instituciones y en la universalidad de las garantías. Desde una perspectiva democrática, el reto no consiste únicamente en evitar abusos individuales, sino en preservar un espacio público en el que el ejercicio de derechos no esté condicionado por la anticipación de una evaluación automatizada permanente.

8. Seguridad, neutralidad tecnológica y desplazamiento del debate político

El despliegue de tecnologías de IA en el ámbito de la seguridad suele apoyarse en una narrativa que presenta estas herramientas como respuestas necesarias a amenazas complejas y cambiantes. En este marco, la seguridad aparece como un objetivo prioritario que tiende a desplazar a un segundo plano el debate sobre alternativas, límites o costes en términos de derechos. La apelación a la urgencia, la eficacia o la inevitabilidad tecnológica reduce el espacio para la deliberación democrática, especialmente cuando las decisiones se adoptan en contextos de presión operativa o bajo marcos de excepción.

A esta dinámica contribuye la percepción de neutralidad tecnológica asociada a los sistemas de inteligencia artificial. La complejidad técnica de los modelos y la especialización del conocimiento necesario para comprender su funcionamiento favorecen que decisiones profundamente normativas se presenten como cuestiones técnicas de diseño, calibración o implementación. En el ámbito europeo, este desplazamiento se ha observado en debates sobre tecnologías de vigilancia, donde las discusiones políticas sobre proporcionalidad o legitimidad se han traducido, en la práctica, en debates sobre precisión, tasas de error o mejoras técnicas, relegando a un segundo plano las preguntas sobre oportunidad y límites democráticos.

Este fenómeno no implica que la tecnología sustituya al debate político, sino que puede reconfigurarlo de manera silenciosa. Cuando las decisiones se encapsulan en marcos técnicos o regulatorios altamente especializados, la participación efectiva de parlamentos, sociedad civil y ciudadanía se vuelve más difícil. Recuperar la dimensión política de la seguridad algorítmica no significa rechazar la innovación ni negar la necesidad de herramientas avanzadas, sino reconocer que la definición de riesgos aceptables, prioridades de protección y límites de la vigilancia es, en última instancia, una cuestión democrática. Mantener abierto ese espacio de deliberación constituye una condición esencial para que la inteligencia artificial se integre de forma legítima en las políticas de seguridad.

9. Dilemas abiertos y líneas de futuro

El avance de la inteligencia artificial en el ámbito de la seguridad plantea dilemas que no admiten respuestas simples ni soluciones cerradas. La cuestión central no es si estas tecnologías deben utilizarse, sino en qué condiciones pueden integrarse en sistemas democráticos sin erosionar los derechos y garantías que los definen. En entornos sensibles, caracterizados por decisiones relevantes y potencialmente irreversibles, resulta imprescindible reflexionar sobre los límites de la automatización, el papel efectivo de la decisión humana y la capacidad real de control y revisión de los sistemas desplegados.

En este contexto, el principio de inocuidad y la exigencia de intervención humana significativa adquieren una relevancia particular. No se trata de frenar la innovación ni de rechazar el uso de herramientas avanzadas, sino de asegurar que su incorporación no diluya responsabilidades ni desplace los mecanismos de protección construidos a lo largo del tiempo. La gobernanza de la seguridad algorítmica exige, por tanto, una combinación de normas claras, prácticas institucionales responsables y un debate público informado que permita ajustar de forma continua el equilibrio entre seguridad y derechos.

Para España, en el marco europeo, este debate representa una oportunidad además de un desafío. La forma en que se interpreten y apliquen las normas existentes, la ambición con la que se desarrollen mecanismos de control y la voluntad de someter estas tecnologías a escrutinio público determinarán si la IA se consolida como una herramienta al servicio de una seguridad democrática o como un factor de presión sobre un equilibrio ya de por sí delicado. Mantener abierto este debate no es una señal de debilidad, sino una expresión de madurez democrática.