FACULTAD DE CIENCIAS ECONOMICAS Y EMPRESARIALES

LOS EFECTOS DEL AI ACT EN LA COMPETITIVIDAD EUROPEA EN DEFENSA

Autor: Sara Viesca Calero

Directora: Marta Molina Urosa

Madrid | 2024

Declaración de Uso de Herramientas de IA Generativa en Trabajos Fin de Grado en Relaciones Internacionales.

Por la presente, yo, Sara Viesca Calero, estudiante de 5º del Doble Grado de ADE y Relaciones Internacionales (E6) de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "Los efectos del AI Act en la competitividad europea en defensa", declaro que he utilizado la herramienta de IA Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. **Sintetizador y divulgador de libros complicados**: Para resumir y comprender literatura compleja.
2. **Traductor**: Para traducir textos de un lenguaje a otro.
3. **Corrector de estilo literario y de lenguaje:** Para mejorar la calidad lingüística y estilística del texto.
4. **Referencias:** Usado conjuntamente con otras herramientas, como Science, para identificar referencias preliminares que luego he contrastado y validado.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para qué se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 4/05/2025

Firma: Sara Viesca Calero

Índice

Glosario de abreviaciones *4*

Resumen *5*

Abstract *6*

1. Introducción *7*

1.1. Justificación del tema **7**

1.2. Objetivos del trabajo **8**

1.3. Hipótesis y preguntas de investigación **9**

1.4. Metodología **10**

1.5. Enfoque teórico **11**

1.6. Marco conceptual **13**

2. Inteligencia artificial en el ámbito de defensa *14*

2.1. Definición de inteligencia artificial en defensa **15**

2.2. Tecnologías de doble uso **16**

2.3. Dilemas éticos y geopolíticos del uso militar de la IA **19**

3. La Normativa de la UE en materia de IA *21*

3.1 Contexto de la regulación **22**

3.2. Principios y objetivos de la regulación **24**

3.3. ¿Hacia una fragmentación o unificación regulatoria? **26**

3.4. Marco regulatorio internacional en IA **28**

4. El impacto del AI Act en la competitividad europea *32*

4.1. Definición de competitividad y ventaja competitiva **33**

4.2. Liderazgo regulatorio como ventaja competitiva **35**

4.3. Desafíos regulatorios para la autonomía tecnológica estratégica **37**

5. Implicaciones del AI Act en defensa *39*

5.1. Implicaciones Estratégicas: autonomía militar europea **39**

5.2. Implicaciones en I+D **42**

5.3. Implicaciones Económicas **45**

5.3.1. Presupuestos y proyecciones de gasto en defensa: Estados Unidos, China y la Unión Europea (2025-2030) 45

5.3.2. Relación entre los sectores público y privado en defensa 47

6. Conclusiones *50*

Bibliografía *54*

Glosario de abreviaciones

AI: Artificial Intelligence

CAC: Administración del Ciberespacio de China

CBO: Oficina Presupuestaria del Congreso

CDAO: Chief Digital and Artificial Intelligence Office

CE: Comisión Europea

DIH: Derecho Internacional Humanitario

EE. UU.: Estados Unidos

EPL: Ejército Popular de Liberación

HLEG: High Level Expert Group

IA: Inteligencia Artificial

JAIC: Joint Artificial Intelligence Center

LAWS: Lethal Autonomous Weapons Systems

MIC: Made in China

OCDE: Organización para la Cooperación y el Desarrollo Económico

OTAN: Organización del Tratado del Atlántico Norte

PIB: Producto Interior Bruto

RGPD: Reglamento General de Protección de Datos

SAAL: Sistemas de Armas Autónomos Letales

UE: Unión Europea

WEF: World Economic Forum

Resumen

Este trabajo analiza los efectos indirectos del *Artificial Intelligence Act (AI Act)* de la Unión Europea (UE) sobre el desarrollo y la implementación de tecnologías vinculadas al ámbito de la defensa. Aunque el reglamento excluye formalmente las aplicaciones militares, su impacto sobre las tecnologías de doble uso —como los sistemas autónomos o las herramientas de vigilancia— introduce limitaciones normativas que pueden ralentizar la innovación estratégica y debilitar la autonomía tecnológica europea.

Mediante un análisis de fuentes normativas, académicas e institucionales, se examinan las interacciones entre gobernanza tecnológica, competitividad internacional y soberanía estratégica en un contexto marcado por la aceleración geopolítica y la carrera global por el liderazgo en inteligencia artificial. El estudio se estructura en torno a tres dimensiones clave: las implicaciones del *AI Act* para la autonomía militar europea, sus efectos sobre la inversión en investigación y desarrollo, y su impacto económico sobre el ecosistema industrial de defensa. Asimismo, se compara el enfoque regulatorio europeo con los modelos adoptados por Estados Unidos y China, identificando las debilidades estructurales de la UE para traducir su liderazgo normativo en capacidades operativas reales. El estudio advierte que, sin una adaptación más flexible del marco regulatorio, la apuesta ética de la UE por la inteligencia artificial podría convertirse en un obstáculo para su competitividad estratégica en el ámbito de la defensa.

Palabras clave: Inteligencia artificial, *AI Act*, autonomía estratégica, tecnologías de doble uso, competitividad tecnológica, gobernanza tecnológica, defensa, regulación ética, seguridad europea.

Abstract

This paper analyzes the indirect effects of the European Union's Artificial Intelligence Act (AI Act) on the development and implementation of technologies related to the field of defense. Although the regulation formally excludes military applications, its impact on dual-use technologies — such as autonomous systems or surveillance tools — introduces regulatory constraints that may slow down strategic innovation and weaken Europe's technological autonomy.

Through an analysis of legal, academic, and institutional sources, the study examines the intersections between technological governance, international competitiveness, and strategic sovereignty in a context marked by geopolitical acceleration and a global race for leadership in artificial intelligence. The research is structured around three key dimensions: the AI Act's implications for European military autonomy, its effects on investment in research and development, and its economic impact on the defense industrial ecosystem. Furthermore, it compares the European regulatory approach with the models adopted by the United States and China, highlighting the EU's structural weaknesses in translating regulatory leadership into real operational capabilities. The study warns that, without a more flexible adaptation of the regulatory framework, the EU's ethical commitment to artificial intelligence could become an obstacle to its strategic competitiveness in the defense sector.

Key words: Artificial intelligence, AI Act, strategic autonomy, dual-use technologies, technological competitiveness, technology governance, defense, ethical regulation, european security.

1. Introducción

1.1. Justificación del tema

La inteligencia artificial (IA) es un pilar de transformación tecnológica, especialmente en sectores críticos como la defensa, donde las tecnologías disruptivas pueden redefinir el equilibrio de poder global (Academia de las Ciencias y las Artes Militares, 2024). Una tecnología clasificada como disruptiva es aquella que redefine los estándares existentes, reconfigura los procesos convencionales al transformar no solo sus mecanismos operativos, sino también reconfigurando por completo las dinámicas industriales sobre las que se sustentaban (López Vicente, 2009). En este contexto, tanto la Unión Europea como otras potencias han reconocido el potencial estratégico de la IA (Garrigues, 2023). Sin embargo, las aproximaciones regulatorias y estratégicas de estas potencias difieren significativamente (Madariaga, 2024). Mientras que la UE ha adoptado un enfoque regulatorio proactivo con la aprobación de la Ley de Inteligencia Artificial, potencias como EE. UU. han optado por un enfoque de mínima regulación, basada en recomendaciones como la "Iniciativa Norteamericana en IA" lanzada en 2019 que prioriza la inversión en investigación y desarrollo de IA sin imponer restricciones estrictas, permitiendo que el mercado lidere el desarrollo tecnológico (The White House, 2019). Este análisis comparativo busca explorar cómo la regulación europea de IA limita su competitividad en el desarrollo y aplicación de esta tecnología en defensa (Schechner & Meichtry, 2025).

El *AI Act* impone restricciones que limitan el desarrollo y la implementación de ciertas tecnologías de inteligencia artificial en el ámbito civil (European Parliament, 2023), lo que, a su vez, dificulta su reutilización en defensa (Brundage et al., 2018). Un caso específico es la clasificación estricta de los sistemas de IA de alto riesgo, que impone requisitos adicionales de transparencia y supervisión a tecnologías como el reconocimiento facial (European Parliament, 2023), afectando su integración en aplicaciones militares vinculadas a vigilancia y seguridad (Geist, 2023). El *AI Act* introduce restricciones que afectan indirectamente en tecnologías civiles que luego son reutilizadas para fines de defensa. Este aspecto es crucial ya que afecta negativamente a ciertas variables esenciales para el desarrollo de una potencia europea. Este efecto, que

genera un lastre en la competitividad europea en materia de defensa, tiene implicaciones en diversos ámbitos que pueden volver a la UE menos competitiva (Imbalzano, 2025).

1.2. Objetivos del trabajo

El presente estudio busca analizar el impacto del Reglamento de Inteligencia Artificial, al que nos referiremos durante el trabajo por su acrónimo en inglés—*AI Act*— de la Unión Europea en el desarrollo y despliegue de tecnologías relacionadas con la defensa, con especial atención en las implicaciones en la competitividad europea en el ámbito de la seguridad.

A continuación, se enumeran los objetivos de este trabajo:

I. Examinar el marco normativo del *AI Act*, sus principios rectores y su alcance, con énfasis en su exclusión en el sector de defensa.

II. Evaluar los efectos indirectos del *AI Act* sobre las tecnologías de doble uso, particularmente en ámbitos como la vigilancia, la ciberseguridad o los sistemas autónomos.

III. Identificar los riesgos de fragmentación regulatoria entre Estados miembros y su impacto en la coordinación de esta normativa.

IV. Poner de manifiesto los posibles efectos que el *AI Act* puede tener en la competitividad tecnológica e industrial europea frente a otras potencias internacionales.

V. Analizar otros modelos regulatorios de IA como el estadounidense o el chino, con el fin de contextualizar el enfoque europeo y evaluar su viabilidad estratégica en un entorno internacional competitivo.

VI. Estudiar las implicaciones del *AI Act* en la autonomía estratégica de la Unión Europea, especialmente en el marco del rearme europeo y la aspiración a una mayor independencia militar frente a aliados externos.

VII. Examinar el impacto del *AI Act* sobre el ecosistema de innovación y la inversión en I+D en defensa dentro de la UE.

1.3. Hipótesis y preguntas de investigación

En base a los objetivos para este trabajo, se plantea la siguiente hipótesis que guiará este estudio:

> *"A pesar de que el AI Act no regula directamente las aplicaciones militares, su diseño e implementación afectan negativamente al desarrollo de capacidades tecnológicas en el ámbito de la defensa, dadas las restricciones impuestas a tecnologías de doble uso, fundamentales para la competitividad global de la Unión Europea".*

A partir de esta hipótesis, se plantean una serie de preguntas de investigación que estructuran y orientan el análisis a lo largo del trabajo.

En primer lugar, resulta pertinente preguntarse cuáles son los mecanismos concretos a través de los cuales el *AI Act* —pese a excluir formalmente los usos militares— termina condicionando el desarrollo de tecnologías aplicables al ámbito de la defensa. ¿Cómo afecta la calificación de alto riesgo a sistemas inicialmente concebidos para un uso civil, pero con claro potencial dual? ¿Hasta qué punto esta normativa limita la posibilidad de reutilizar dichas innovaciones en contextos estratégicos?

Asimismo, este trabajo se interroga sobre el modelo de liderazgo normativo que la Unión Europea ha querido proyectar a través del *AI Act.* ¿Puede esta forma de regulación traducirse en una ventaja competitiva en el ámbito de la defensa, o se trata más bien de un *soft power* normativo que pierde efectividad frente a modelos más ágiles y operativos como los de Estados Unidos o China? ¿Es sostenible la competitividad tecnológica europea bajo un marco regulatorio tan exigente?

Por último, cabe cuestionarse si la rigidez del enfoque europeo —centrado en valores éticos y en la protección de derechos fundamentales— está dificultando la inversión privada en tecnologías estratégicas y agravando la brecha de innovación ya existente. ¿Qué consecuencias estratégicas podría tener esta apuesta normativa sobre la autonomía militar de la Unión Europea?

Estas preguntas estructuran el desarrollo del presente análisis, articulado en torno al estudio de los efectos indirectos del *AI Act* sobre la autonomía estratégica, la inversión en I+D y el ecosistema industrial de defensa europeo. Para responderlas, se delimitarán previamente conceptos clave como inteligencia artificial, tecnologías de doble uso, competitividad y ventaja competitiva.

1.4. Metodología

Este trabajo adopta un enfoque cualitativo y documental basado en el análisis crítico de fuentes secundarias. Dado el carácter normativo y estratégico del objeto de estudio se ha optado por una metodología centrada en la revisión y el análisis interpretativo de fuentes.

En concreto, la investigación se ha desarrollado a partir de los siguientes métodos:

- Revisión bibliográfica y documental: Se ha realizado un análisis exhaustivo de literatura académica relevante, incluyendo artículos en revistas científicas, libros especializados y documentos de organismos internacionales. Esto ha permitido identificar los marcos teóricos y conceptuales que sustentan el debate sobre gobernanza tecnológica, regulación digital y tecnologías de doble uso. Esta revisión también ha sido fundamental para identificar las temáticas clave del campo de estudio.

- Análisis normativo y jurídico: Se ha prestado especial atención al estudio del Reglamento Europeo sobre la Inteligencia Artificial, dada su importancia en este trabajo, examinando su evolución legislativa, sus principios fundamentales y su articulación técnica. Este análisis se ha complementado con otras normativas

relacionadas, así como con documentos oficiales tanto europeos como de otros países estudiados.

- Consulta de fuentes especializadas y periodísticas: Con el fin de contextualizar el debate actual, se han incorporado artículos y análisis publicados en medios especializados como *The Economist, Politico, Euractiv* o El Orden Mundial, así como informes de centros de pensamiento *(think tanks)* europeos y transatlánticos (*Carnegie Europe, Bruegel, Euractiv*, entre otros). Estas fuentes han contribuido a identificar posiciones divergentes entre los actores institucionales, empresariales y académicos respecto al impacto del *AI Act* en la competitividad y la autonomía estratégica de la Unión Europea.

- Estudio de casos y ejemplos ilustrativos: A lo largo del trabajo se han incluido casos concretos de aplicación de tecnologías de inteligencia artificial en tecnologías duales y en defensa —como drones comerciales, sistemas autónomos o sensores inteligentes— con el fin de ejemplificar los desafíos regulatorios en contextos reales y evaluar la aplicabilidad práctica de la normativa.

La combinación de estas técnicas permite ofrecer una visión estructurada, crítica y bien fundamentada del marco regulatorio europeo, así como de sus implicaciones indirectas el sector estratégico de defensa.

1.5. Enfoque teórico

Este trabajo parte del debate estratégico sobre la creciente necesidad de autonomía militar europea y las capacidades reales de la Unión para alcanzarla. Desde esta perspectiva, se analiza cómo la Ley de IA de la UE puede influir indirectamente en la construcción de dicha autonomía, afectando a tecnologías de doble uso, la inversión en I+D y la competitividad del sector defensa. Si bien existe una amplia literatura sobre la gobernanza digital en la Unión Europea, los estudios que analizan los efectos colaterales del *AI Act* en ámbitos estratégicos como la defensa siguen siendo escasos e incompletos.

Diversos autores han analizado el rol normativo de la UE a lo largo del tiempo. En particular, Bradford (2020) introduce el concepto de *Brussels Effect* para describir la capacidad de la UE de exportar sus estándares regulatorios más allá de sus fronteras, al establecer normas que terminan adoptándose internacionalmente por su carácter vinculante para quienes operan en el mercado europeo. Sin embargo, gran parte de estos estudios se centran en los efectos internacionales de la regulación, dejando de lado su impacto interno en sectores sensibles como la defensa. En esta línea, estudios como los de Pernot-Leplay (2024) o Chun, Schroeder de Witt & Elkins (2024) subrayan cómo el enfoque ético y garantista de la UE contrasta con el pragmatismo normativo de Estados Unidos y con la planificación centralizada del modelo chino.

En el ámbito de la seguridad y la defensa, algunos trabajos recientes han advertido sobre las limitaciones que puede generar una excesiva regulación sobre la innovación estratégica. Greene (2024), desde el *Center for a New American Security*, advierte que el *AI Act* podría obstaculizar la adopción de tecnologías críticas en el sector militar europeo, mientras que Brull (2025) señala cómo las exigencias normativas han generado un fenómeno de "fuga de startups" tecnológicas hacia ecosistemas más flexibles. De forma complementaria, el informe Draghi (2024) identifica una brecha entre la ambición normativa europea y su capacidad real de innovación, especialmente en sectores altamente tecnológicos como la IA.

Sin embargo, pese al creciente interés de esta temática, aún no se ha explorado en profundidad cómo afecta la gobernanza de la IA a la proyección de poder militar europeo, ni hasta qué punto el *AI Act* puede comprometer los objetivos de autonomía estratégica definidos en documentos como la Brújula Estratégica (2022) o el *White Paper on European Defence Readiness 2030* (2025). En este sentido, el presente trabajo propone un enfoque novedoso al estudiar los efectos indirectos de la regulación sobre las capacidades militares europeas, con especial atención a tres ejes: la competitividad, la inversión en I+D y la cooperación público-privada en defensa.

1.6. Marco conceptual

Como mencionado, el presente trabajo se estructura sobre un marco conceptual que articula tres ejes fundamentales: el poder normativo europeo, la autonomía estratégica, y la gobernanza tecnológica, conceptos que permiten analizar cómo una regulación como el *AI Act* puede tener efectos indirectos en la competitividad tecnológica y las capacidades de defensa de la Unión Europea. Este enfoque es clave para comprender la tensión entre ética regulatoria y liderazgo estratégico en el contexto de una creciente rivalidad tecnológica.

En primer lugar, se retoma el concepto de poder normativo europeo (*Normative Power Europe*), desarrollado por Ian Manners (2002), que define la capacidad de la UE para ejercer influencia internacional no mediante coerción o incentivos materiales, sino a través de la exportación de normas, principios y estándares. Esta visión ha sido ampliamente adoptada en estudios sobre gobernanza global, especialmente en el ámbito digital (Ricart, 2024). En el caso del *AI Act*, esta lógica se traduce en un intento por liderar la regulación global de la IA a través de un modelo ético basado en los derechos fundamentales (Buchholz, 2025).

En segundo lugar, el concepto de autonomía estratégica, tal como lo define el Parlamento Europeo (2022), hace referencia a la capacidad de la UE para actuar de forma autónoma, apoyándose en recursos propios en sectores clave, y cooperando con terceros siempre que sea posible. Esta noción se ha ampliado recientemente para incluir no solo la defensa y la seguridad, sino también la tecnología y la economía, en respuesta a la creciente exposición europea a dependencias externas en sectores críticos (Borrell, 2020). En el ámbito del *AI Act*, la autonomía estratégica adquiere especial relevancia por el riesgo de que un marco regulatorio demasiado restrictivo limite la innovación (Espinoza, 2024) en tecnologías de doble uso, esenciales para reducir la dependencia europea de actores externos en el ámbito de la defensa (Greenacre, 2025).

Por último, se introduce el concepto de gobernanza tecnológica, entendido como el conjunto de normas, actores e instituciones que regulan el desarrollo, aplicación y supervisión de tecnologías emergentes (Costas Trascasas, 2022). Según este autor, este enfoque implica asumir que la gestión de tecnologías como la IA no puede limitarse a

criterios técnicos o de mercado, sino que requiere marcos éticos, políticos y de seguridad que garanticen la transparencia, la equidad y la protección de los derechos humanos. Desde esta perspectiva, el *AI Act* no es solo una herramienta jurídica, sino un elemento clave de la capacidad europea para definir su propio modelo de desarrollo tecnológico (Otero Iglesias, 2024).

En conjunto, estos tres conceptos permiten evaluar si el modelo regulador europeo es capaz de compatibilizar su vocación ética con sus objetivos geoestratégicos. En un escenario internacional marcado por la competencia tecnológica, las decisiones regulatorias de la UE en materia de IA no solo afectan al mercado, sino también a su posición global como actor autónomo y competitivo.

2. Inteligencia artificial en el ámbito de defensa

En la reunión anual del *World Economic Forum* (WEF), (2025), la inteligencia artificial ha sido calificada como la 5ª revolución industrial debido a su carácter revolucionario y capaz de transformar profundamente los equilibrios económicos, sociales y estratégicos globales. Según el WEF, su desarrollo se encuentra en el centro de una nueva ola de innovación impulsada por la convergencia entre los ámbitos digital, físico y biológico, que está acelerando la transformación de industrias estratégicas hacia modelos más autónomos, sostenibles y eficaces. Esta transformación se considera especialmente significativa en el ámbito de defensa, ya que la IA no solo introduce avances técnicos, sino que también redefine la manera en que se conciben, planifican y ejecutan las operaciones militares (Gray & Ertan, 2021).

La progresiva incorporación de sistemas basados en inteligencia artificial en los sectores de seguridad y defensa está generando nuevas dinámicas estratégicas, que han intensificado el debate en torno a la necesidad de establecer marcos regulatorios adecuados y a los límites que estos deberían tener (Leon Coronado, 2023). En este contexto, y antes de abordar el impacto que podría tener el *AI Act* en el ámbito de la defensa, resulta fundamental definir con precisión qué se entiende por IA en este entorno específico, así como examinar sus principales aplicaciones en escenarios militares y de seguridad.

2.1. Definición de inteligencia artificial en defensa

La inteligencia artificial se define como la capacidad de los sistemas informáticos para llevar a cabo tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, la toma de decisiones, el aprendizaje y la resolución de problemas (Russell & Norvig, 2020). En el ámbito de la defensa, esta tecnología ha cobrado una importancia estratégica debido a su capacidad de transformar las operaciones militares y las dinámicas de seguridad global (Álvarez, 2024).

La IA en defensa comprende una variedad de sistemas y aplicaciones diseñadas para procesar datos en tiempo real, identificar patrones complejos y apoyar la toma de decisiones estratégicas con un alto grado de precisión y autonomía (Las Heras, 2023). Estos sistemas incluyen plataformas de ciberseguridad avanzadas que detectan y mitigan ataques de manera proactiva, drones autónomos utilizados en misiones de reconocimiento, vigilancia y ataque, y herramientas de análisis predictivo que optimizan la logística militar y la asignación de recursos (Las Heras, 2023). Además, su capacidad de procesamiento mejora áreas críticas como la detección temprana de amenazas y la planificación de misiones militares con precisión y rapidez (Contreras Machado, 2024).

Además, la integración de la IA en los sistemas autónomos ha transformado radicalmente las capacidades de las fuerzas armadas modernas. Los sistemas autónomos, definidos por el Comité Internacional de la Cruz Roja, CICR, (2019) como "cualquier sistema de armas con autonomía en sus funciones críticas, es decir, capaz de seleccionar y atacar objetivos sin intervención humana", permiten ejecutar misiones en entornos hostiles minimizando el riesgo para el personal humano. Este tipo de tecnologías incluyen drones, vehículos terrestres no tripulados y submarinos autónomos, utilizados en misiones de vigilancia, reconocimiento y búsqueda y rescate (Guerra Huapalla, 2023).

Un ejemplo significativo de esta evolución es el programa experimental liderado por la Fuerza Aérea de los Estados Unidos a través del X-62A VISTA, una versión modificada del F-16 utilizada para probar sistemas de inteligencia artificial en vuelo (Fernández, 2024). Durante pruebas recientes, la aeronave ha sido completamente controlada por IA en distintos escenarios de combate simulado, evaluando su capacidad para operar de manera autónoma sin intervención humana (Insinna, 2023). Este desarrollo es crucial para

la integración de la IA en futuras plataformas aéreas no tripuladas, permitiendo que los sistemas autónomos cooperen con pilotos humanos en combate y asuman funciones estratégicas clave para reducir la carga operativa y optimizar la efectividad en el campo de batalla (Casem, 2021).

Otra aplicación destacable de la IA en defensa es su capacidad para fortalecer los sistemas de ciberseguridad, detectando patrones anómalos en ciberataques y respondiendo con rapidez a amenazas emergentes (Schmitt, 2023). Los sistemas de IA pueden coordinar operaciones en el ciberespacio, ofreciendo una ventaja crítica en un entorno donde las amenazas son cada vez más sofisticadas y persistentes (Goud, Kaul & Chinnegowda, 2024). La IA no solo mejora la capacidad de detección y respuesta, sino que también contribuye a la resiliencia de los sistemas militares frente a adversarios que emplean tácticas cada vez más complejas en el ciberespacio (Hierro, 2025).

2.2. Tecnologías de doble uso

Además, una de las tipologías más importantes en este campo son las denominadas tecnologías de doble uso, aquellas que, aunque desarrolladas inicialmente para fines civiles, pueden ser adaptadas y empleadas con fines militares (León Serrano, 2023). Esta doble aplicabilidad puede darse tanto a nivel de producto como de proceso: desde componentes tecnológicos integrados en sistemas militares (como sensores, algoritmos o materiales avanzados), hasta plataformas completas diseñadas para otros sectores, pero reutilizadas para defensa (Martí Sempere, 2024).

La Unión Europea define las tecnologías de doble uso como aquellas que pueden destinarse tanto a un uso civil como a uno militar, y ha elaborado una clasificación específica que incluye, entre otras, áreas como sensores y láseres, navegación, telecomunicaciones, microelectrónica, inteligencia artificial, tecnologías espaciales, robótica, materiales avanzados y biotecnología (Comisión Europea, 2021a). En efecto, estas tecnologías abarcan una gran variedad de aplicaciones que van desde la ciberseguridad hasta los sistemas de navegación, pasando por la computación cuántica, el reconocimiento facial o el procesamiento de imágenes por satélite (Quintero Morales & Salas Galindo, 2023). Además, no solo aportan eficiencia y reducción de costes

mediante economías de escala, sino que permiten acelerar el ciclo de innovación en defensa aprovechando desarrollos previos ya testeados en el mercado civil (Kosciuszko Institute & ECSO, 2024).

Un ejemplo representativo de la evolución de las tecnologías duales es el de los drones comerciales, ideados originalmente como herramientas para la recreación o la fotografía aérea (Chulilla Cano, J.L., 2023). Estos drones, concebidos para captar imágenes desde perspectivas innovadoras o realizar tareas de monitoreo ambiental, han encontrado un nuevo propósito en los conflictos bélicos. En escenarios como el de Myanmar, los drones comerciales han sido reconvertidos en instrumentos de guerra. Estos dispositivos inicialmente destinados a usos civiles han demostrado una capacidad para adaptarse a los combates contemporáneos a través de la integración de bombas improvisadas y su utilidad para misiones de vigilancia y recopilación de información en tiempo real (Banerjee, 2024). Una situación parecida ocurrió en Ucrania, donde el uso de drones comerciales se ha profesionalizado aún más, incorporando granadas y empleándose como herramienta de reconocimiento o de localización de artillería (Segura, 2023). Esta evolución demuestra cómo dispositivos desarrollados para fines civiles pueden convertirse en activos estratégicos en escenarios bélicos, especialmente cuando se integran con tecnologías avanzadas como la inteligencia artificial, maximizando su capacidad y efectividad en el campo de batalla (Lovett, 2025).

Son precisamente este tipo de tecnologías las que se verán profundamente impactadas por el *AI Act,* cuyas restricciones y exigencias no solo afectarán el uso civil de estas innovaciones, sino por ende su potencial militar, evidenciando la complejidad de regular tecnologías con aplicaciones tan amplias (Powell, 2024). Aunque el *AI Act* establece en sus consideraciones, específicamente la número 24, que los sistemas de IA empleados con fines estrictamente militares o de seguridad nacional no entran en su ámbito de aplicación (Vogiatzoglou, 2024), lo cierto es que muchas tecnologías de doble uso desarrolladas inicialmente para el mercado civil sí que se ven afectadas por estas restricciones. Esta distinción es clave, ya que cuando una tecnología, como puede ser un dron, se introduce en el mercado con fines civiles, debe cumplir con los requisitos del reglamento, incluso si posteriormente es reutilizada en contextos militares. Así lo expone el propio reglamento: «Un sistema de IA introducido en el mercado con fines civiles o de garantía del cumplimiento del Derecho que se utilice […] con fines militares, de defensa

o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento» (Reglamento (UE) 2024/1084, 2024).

No obstante, esto no implica que el sistema quede exento de regulación en su fase de desarrollo, validación o comercialización inicial, momentos en los cuales sí aplica el marco del *AI Act* si se trata de un sistema clasificado como de alto riesgo. Esta clasificación se establece en el artículo 6.2 del reglamento, que enumera una lista de usos considerados sensibles recogidos en el Anexo III (EU Artificial Intelligence Act, 2024a). A modo de ilustración, se empleará el ejemplo mencionado anteriormente de los drones comerciales equipados con IA utilizados posteriormente con fines militares en los conflictos como el de Myanmar o Ucrania. Estos drones, usados inicialmente para fines recreativos o industriales, incorporan funcionalidades como navegación autónoma, algoritmos de seguimiento o procesamiento de imágenes en tiempo real (Palmas & Andronico, 2022), que pueden entrar dentro de las categorías de alto riesgo establecidas por el reglamento. Entre los requisitos a cumplir en esta categoría, se encuentra la obligación de garantizar una supervisión humana eficaz (art. 14), establecida con el fin de asegurar que un operador pueda intervenir, corregir o detener el funcionamiento del sistema cuando sea necesario (EU Artificial Intelligence Act, 2024b). Si bien esta exigencia se alinea con la lógica de protección de derechos fundamentales en contextos civiles, puede entrar en conflicto con las necesidades del entorno militar, donde la autonomía y la rapidez de respuesta resultan esenciales (Bueso Carrasco, 2025).

Por lo tanto, aunque la reutilización militar no esté directamente regulada por el *AI Act*, el cumplimiento de estas obligaciones durante la etapa de desarrollo civil puede limitar la adaptabilidad de estas tecnologías en escenarios bélicos, al imponer sistemas menos compatibles con su aplicación militar (Greene, 2024). En consecuencia, el caso de los drones evidencia cómo el *AI Act*, aun sin dirigirse al sector defensa, influye en el potencial estratégico de determinadas tecnologías de doble uso. Además, en un entorno marcado por una creciente convergencia entre los sectores tecnológico-civil y militar, se hace cada vez más difícil trazar una línea divisoria clara entre ambos usos (Ams, 2021). Por lo que, esta tendencia refuerza la urgencia de establecer marcos normativos diferenciados y adaptativos, que reconozcan el carácter dual de ciertas tecnologías y permitan su desarrollo bajo parámetros éticos y estratégicos compatibles con los intereses de seguridad nacional (Deloitte, 2024).

2.3. Dilemas éticos y geopolíticos del uso militar de la IA

Más allá de sus implicaciones técnicas y estratégicas, la incorporación de la IA en el ámbito militar plantea a su vez una serie de desafíos éticos y geopolíticos (Moliner González, 2019) que requieren de un análisis en profundidad. A medida que estas tecnologías adquieren mayor autonomía y capacidad de decisión, no solo se transforman las dinámicas de la guerra, sino también los marcos normativos, morales y políticos que la rodean. En este contexto, los avances en inteligencia artificial aplicada al ámbito militar no deberían juzgarse únicamente en función de su rendimiento o eficacia táctica. Su creciente implementación en estos contextos ha dado lugar al desarrollo del concepto de *Responsible AI*, una aproximación que aboga por un uso ético, transparente y jurídicamente responsable de la inteligencia artificial en contextos de seguridad y defensa (Nadibaidze, 2023).

Este apartado examina, en primer lugar, los dilemas éticos derivados del desarrollo y uso de sistemas de armas autónomas letales (SAAL), centrando la atención en los desafíos relacionados con la responsabilidad, la deshumanización del conflicto y el cumplimiento del derecho internacional humanitario. En segundo lugar, se abordan los riesgos estratégicos y geopolíticos vinculados a la velocidad y autonomía de decisión de los sistemas basados en IA, especialmente en contextos de alta tensión internacional, donde las decisiones algorítmicas pueden tener consecuencias irreversibles. Ambos planos —ético y geopolítico— revelan la necesidad urgente de establecer límites normativos y explican por qué un número creciente de Estados y organizaciones internacionales están impulsando marcos regulatorios, controles técnicos y acuerdos multilaterales para abordar los riesgos asociados al uso militar de la IA (Riquelme, 2023).

Retomando esta cuestión, el despliegue de sistemas de IA en entornos militares sitúa en el centro del debate preocupaciones éticas (Klaus, 2024), al mismo tiempo que intensifica las tensiones estratégicas en un escenario marcado por aceleración tecnológica (O'Donnell, 2024). La IA, al facilitar el procesamiento autónomo de datos, la vigilancia constante y el análisis predictivo, amplía significativamente la capacidad de acción y toma de decisiones de los actores armados (Crum, 2024). Sin embargo, estas mismas capacidades también pueden aumentar el riesgo de errores operativos, interpretaciones erróneas y una mayor deshumanización de los conflictos (DeMaio, 2025).

Esta preocupación se acentúa a medida que los sistemas de IA alcanzan mayores niveles de autonomía, modificando la forma en que se toman decisiones críticas en contextos de conflicto (Crum, 2024). Delegar funciones sensibles a máquinas, especialmente en escenarios donde el tiempo de reacción es limitado, genera nuevos riesgos operativos y éticos que no siempre pueden anticiparse ni controlarse fácilmente (DeMaio, 2025). En efecto, uno de los principales dilemas éticos gira en torno al desarrollo y uso de sistemas de armas autónomas letales, capaces de identificar y atacar objetivos sin intervención humana directa (Calvo Pérez, 2020). Estos sistemas plantean preguntas críticas sobre la asignación de responsabilidad en caso de errores o daños colaterales (Aravena Flores, 2024). La ausencia de un "dedo humano en el gatillo" introduce un vacío ético que cuestiona los principios fundamentales del derecho internacional humanitario (DIH) (González, 2024). Al permitir que las máquinas tomen decisiones que pueden implicar la vida o la muerte, se corre el riesgo de deshumanizar aún más los conflictos armados y de aumentar la desconfianza en el uso de estas tecnologías (Lannquist et. al., 2020).

Un ejemplo de este tipo de sistemas es el Super aEgis II, un sistema de defensa automatizado desarrollado por la empresa surcoreana DoDAAM que cuenta con un cañón automático y sensores diseñados para proteger instalaciones estratégicas (Parkin, 2015). Según describe Parkin, su uso requiere actualmente de una orden explícita de disparo por parte de un operador humano. Sin embargo, el sistema está técnicamente capacitado para ejecutar ataques de forma totalmente autónoma si se desactiva dicha limitación de software. Esta posibilidad ha generado una fuerte controversia internacional, ya que evidencia cómo una modificación mínima en la programación podría convertir un sistema defensivo en un arma letal autónoma con capacidad de matar sin necesidad de supervisión humana directa (Human Rights Watch, 2020). Este caso pone en evidencia lo difuso que se ha vuelto el límite entre automatización y autonomía total, dado que muchos Estados ya poseen la infraestructura tecnológica para desplegar sistemas letales que no requieren de atención humana (Bieri & Dickow, 2014).

Asimismo, otro desafío ético fundamental es el riesgo de escaladas no intencionadas derivadas de estos sistemas de IA. La velocidad con la que los sistemas de IA procesan datos y toman decisiones en escenarios bélicos puede superar la capacidad de intervención humana, aumentando la probabilidad de desencadenar conflictos sin la adecuada evaluación de las consecuencias (IEEE, 2024). El poder reaccionar de manera

autónoma ante las amenazas percibidas eleva considerablemente la probabilidad de malentendidos tácticos, respuestas desproporcionadas o conflictos armados iniciados por errores algorítmicos, especialmente en escenarios tensos o de alta volatilidad geopolítica (García, 2021). El carácter impredecible de estas tecnologías, unido a la dificultad de establecer instrumentos de control eficaces, representa un serio desafío para el mantenimiento de la estabilidad y la prevención de conflictos a gran escala (Boulanin, Davison, Goussac & Peldán Carlsson, 2020).

En definitiva, estas aplicaciones de la IA en el ámbito militar implican riesgos significativos que muchos actores consideran necesario regular. Sin embargo, la ausencia de un consenso internacional claro sobre los límites aceptables del uso autónomo de la fuerza ha provocado que diversos Estados avancen de forma unilateral en el desarrollo y despliegue de este tipo de sistemas (Stockholm International Peace Research Institute, 2019). Esta falta de coordinación no solo dificulta la creación de normas jurídicas internacionales efectivas, sino que también alimenta una creciente carrera tecnológica en defensa, orientada a asegurar ventajas operativas (Bongioanni, 2024).

3. La Normativa de la UE en materia de IA

Comprender el impacto del *AI Act* en el ámbito de la defensa requiere, en primer lugar, contextualizar su origen, objetivos y fundamentos normativos. Este capítulo se centra precisamente en analizar la lógica que guía la regulación de la IA en la Unión Europea, así como su progresiva configuración como una herramienta de poder normativo. Lejos de ser una respuesta meramente técnica a los riesgos emergentes de esta tecnología, el *AI Act* debe entenderse como parte de una estrategia deliberada de posicionamiento global, en la que la UE aspira a proyectar su modelo ético y regulador más allá de sus fronteras (Šonková, 2024).

Para ello, primero se examina el proceso político y normativo que condujo a la adopción del *AI Act*, desde sus antecedentes regulatorios hasta su articulación como instrumento geopolítico. A continuación, se analizan los principios y objetivos que fundamentan esta regulación, centrados en la protección de los derechos fundamentales, la supervisión humana y la transparencia algorítmica. Por último, se estudia la tensión entre

fragmentación y unificación regulatoria dentro de la UE, así como los desafíos derivados de las diferencias normativas, técnicas y administrativas entre los Estados miembros, especialmente en sectores estratégicos como la defensa. Este análisis es clave para entender cómo un marco legal inicialmente centrado en usos civiles puede acabar condicionando el desarrollo y la aplicabilidad de tecnologías de doble uso en el ámbito militar.

3.1 Contexto de la regulación

La decisión de la Unión Europea de regular la inteligencia artificial debe entenderse dentro de un proceso más amplio de posicionamiento estratégico y político en el ámbito de la gobernanza tecnológica (Lübken, 2024). Como se ha mencionado, la inteligencia artificial se presenta en la actualidad como un catalizador tecnológico con impacto transversal en áreas críticas como la salud, la seguridad, la energía, la justicia o la defensa (OECD, 2024). Este carácter disruptivo ha llevado a la UE a considerar la IA como una cuestión estructural, vinculada tanto a su autonomía estratégica en el ámbito digital como a su capacidad de influencia normativa en el escenario internacional (European Commission, 2020a).

La regulación de las tecnologías digitales en la UE no surge de manera aislada, sino que se apoya en una serie de antecedentes que permiten anticipar la orientación normativa que esta ha adoptado frente a los desarrollos tecnológicos emergentes. Un claro ejemplo de ello es la entrada en vigor del Reglamento General de Protección de Datos (RGPD) en 2018, que marcó un punto de inflexión en la protección de los derechos fundamentales en el entorno digital europeo. Este reglamento no solo estableció un estándar global en materia de privacidad y control de datos personales, sino que también sentó las bases conceptuales y jurídicas para abordar los retos éticos y legales asociados a tecnologías como la IA (Wolford, s.f.).

A partir de estos antecedentes, la Comisión Europea comenzó a desarrollar una arquitectura normativa, orientada a promover un uso ético y responsable de la IA, fundamentado en los valores y principios defendidos por la Unión Europea (Parlamento Europeo, 2024). En este proceso, el Grupo de Expertos de Alto Nivel en Inteligencia Artificial, conocido por su acrónimo en inglés *AI HLEG* y creado en 2018, desempeñó un papel clave como órgano consultivo independiente, elaborando recomendaciones éticas,

técnicas y de política pública que servirían como base para los desarrollos regulatorios posteriores (Comisión Europea, 2018).

Uno de los primeros resultados tangibles de este enfoque fue la publicación en 2019 de las "Directrices Éticas para una IA fiable", donde se establecieron principios como la supervisión humana, la robustez técnica, la transparencia, la privacidad, la equidad y la rendición de cuentas (European Commission, 2019b). A pesar de tener un carácter no vinculante, estas directrices marcaron el inicio de una agenda normativa europea basada en valores, diferenciando el modelo de gobernanza tecnológica de la UE frente a enfoques más permisivos (Parlamento Europeo, s.f.).

El siguiente hito fue la presentación del "Libro Blanco sobre la Inteligencia Artificial" en febrero de 2020, donde la Comisión planteó un doble objetivo: por un lado, crear un entorno propicio para la innovación, y por otro, garantizar un uso ético y seguro de la IA (Rincón Andreu, 2021). En él se propuso un enfoque regulatorio basado en el riesgo, reconociendo que no todas las aplicaciones de IA presentan el mismo nivel de amenaza para los derechos o la seguridad (Comisión Europea, 2020). Este planteamiento se consolida finalmente en la propuesta oficial en el *AI Act*, aprobado por el Consejo en mayo de 2024 (EU Artificial Intelligence Act, s.f.), que a su vez ha sido posteriormente respaldada por otros documentos estratégicos como la "Brújula Digital 2030" (Comisión Europea, 2021). Asimismo, se creó la Oficina Europea de Inteligencia Artificial para supervisar la aplicación de la normativa, especialmente en lo relativo a los modelos fundacionales y los sistemas de IA de propósito general (EU Artificial Intelligence Act, 2024c).

A diferencia de otras potencias que compiten por el liderazgo en IA mediante avances tecnológicos o inversiones masivas en innovación, la Unión Europea ha optado por una vía menos habitual: liderar desde la regulación (Rodríguez Parrondo, 2024). Esta estrategia, que a primera vista puede parecer contraintuitiva, responde a una lógica profundamente arraigada en la identidad institucional de la UE como potencia normativa. El objetivo no es solo establecer reglas para su propio mercado interior, sino definir la forma en que se desarrolla y se gobierna la IA a nivel global (Maharani Hasnadim, 2024), alineándola con los valores europeos de transparencia, derechos fundamentales y supervisión democrática. Sin embargo, como explica Bradford (2020), cuando la UE se

encuentra ante distintas opciones regulatorias, tiende a escoger la más exigente o restrictiva, lo que refuerza su legitimidad normativa pero también puede limitar su margen de maniobra en sectores altamente competitivos como el de la IA.

Este enfoque encuentra su representación más clara en el denominado *Brussels Effect*, concepto que describe la capacidad de la UE para exportar sus normas más allá de sus fronteras gracias al peso de su mercado y a la legitimidad de su modelo regulador (Bradford, 2020). El *AI Act,* como primera legislación sobre IA a nivel global, representa un ejemplo paradigmático de esta lógica. Según Espinoza (2024), esta regulación no trata únicamente de proteger a los ciudadanos europeos frente a los riesgos de la IA, sino de moldear las prácticas internacionales mediante la atracción normativa del modelo europeo. Así, la UE aspira a ocupar una posición de liderazgo en la gobernanza de la inteligencia artificial, no tanto por su capacidad de innovación, sino por su capacidad de establecer los principios que orientarán su desarrollo. En este sentido, como señala Renda (2021), el *AI Act* no debe interpretarse únicamente como una política tecnológica, sino como una herramienta de proyección geopolítica, diseñada para trasladar a escala internacional los principios del Estado de derecho y el modelo regulador europeo.

En definitiva, el contexto en el que nace el *AI Act* refleja no solo una respuesta técnica ante los riesgos emergentes de la IA, sino una estrategia deliberada por parte de la UE para posicionarse como referente en la gobernanza tecnológica global. Este marco normativo, aunque centrado en usos civiles, establece principios y estándares que inevitablemente influirán en ámbitos estratégicos como la defensa, donde muchas de las tecnologías reguladas encuentran aplicaciones similares (Greene, 2024).

3.2. Principios y objetivos de la regulación

En este escenario descrito, el *AI Act* busca controlar y mitigar los riesgos significativos que estas nuevas tecnologías conllevan. Entre estos últimos destacan los sesgos algorítmicos (La Spina, 2024), las violaciones a la privacidad y la falta de transparencia en sistemas críticos (Imprivata, s.f.). Frente a estos desafíos, la UE ha adoptado un enfoque regulatorio basado en el riesgo, que clasifica los sistemas de IA en cuatro categorías principales: riesgo inaceptable, alto, limitado y mínimo (Fernhout & Michielsen, 2025). Este esquema busca establecer controles proporcionales al impacto

potencial de cada tecnología, promoviendo la ética y la seguridad sin neutralizar la innovación (EU Artificial Intelligence Act, 2024d).

Los sistemas considerados de "riesgo inaceptable" están prohibidos por su potencial para vulnerar derechos fundamentales o causar daños irreparables. Ejemplos incluyen sistemas de puntuación social o tecnologías diseñadas para manipular comportamientos humanos (Yaros et al., 2025). La normativa se fundamenta en la necesidad de proteger principios esenciales como la dignidad, la igualdad y la privacidad, subrayando que los riesgos asociados a estas tecnologías no justifican los posibles beneficios que podrían generar (European Commission, s.f.-a).

Por otro lado, los sistemas de "alto riesgo" abarcan aplicaciones críticas que, aunque no están prohibidas, requieren un cumplimiento estricto de requisitos técnicos y éticos. Estos incluyen, por ejemplo, sistemas biométricos, herramientas utilizadas en infraestructuras críticas y tecnologías empleadas en decisiones laborales o educativas (Rauer, 2024). Para garantizar su seguridad y confiabilidad, se exige a los desarrolladores la implementación de medidas como la gestión de riesgos, el uso de datos de alta calidad, la documentación exhaustiva y la supervisión humana en contextos relevantes (A&O Shearman, 2024). Estos estándares reflejan el compromiso de la UE con un modelo que prioriza la equidad y la transparencia.

En contraste, según ilustra la Comisión Europea (s.f.), los sistemas clasificados como de "riesgo limitado" presentan un menor potencial de impacto negativo, pero están sujetos a obligaciones de transparencia diseñadas para informar a los usuarios y prevenir su uso indebido. Este enfoque busca garantizar que las interacciones con sistemas de IA sean claras y accesibles, especialmente en aplicaciones de consumo masivo como los *chatbots*. Finalmente, los sistemas de "riesgo mínimo" o nulo, considerados seguros y de impacto insignificante, están exentos de restricciones específicas, fomentando así la innovación en aplicaciones no críticas (White & Case, 2025a).

Los principios fundamentales del *AI Act* incluyen el respeto a la autonomía humana, la prevención del daño, la equidad, la transparencia y la rendición de cuentas. Estos pilares no solo buscan mitigar los riesgos asociados con la IA, sino también posicionar a la UE como líder global en gobernanza ética de la tecnología (Buchholz, 2025). El *AI Act*

representa un esfuerzo sin precedentes por parte de la UE para equilibrar la innovación con la protección de los derechos fundamentales, estableciendo un estándar global para una inteligencia artificial confiable y centrada en el ser humano (Yordanova, 2022). No obstante, su éxito dependerá de la capacidad de los Estados miembros para implementar esta normativa de manera efectiva y adaptarse a los desafíos de un entorno global en rápida evolución. Como se explorará más adelante, las tensiones entre regulación y competitividad plantean preguntas clave sobre el futuro del liderazgo tecnológico europeo.

3.3. ¿Hacia una fragmentación o unificación regulatoria?

El *AI Act* nace con un claro objetivo de unificar la aproximación europea a la inteligencia artificial, estableciendo un conjunto común de criterios y obligaciones para garantizar la coherencia regulatoria entre los Estados miembros (Feldstein, 2023). Frente al riesgo de una fragmentación regulatoria que derive en 27 aproximaciones nacionales distintas, la Unión Europea plantea una arquitectura legal unificada que permita reducir las asimetrías normativas, garantizar la seguridad jurídica y promover un entorno de confianza para la adopción de la IA (Álvarez García & Tahiri Moreno, 2023). Más allá de la mera coordinación, el *AI Act* busca establecer un verdadero régimen regulador paneuropeo (Lorenzo de Olmos, s.f), con principios y obligaciones compartidas, capaz de equilibrar la promoción de la innovación con la protección de los derechos fundamentales (Marks & Trivedi, 2025). En este sentido, no solo se configura como una herramienta de integración interna, sino también como un instrumento de poder normativo externo, con el que la UE aspira a exportar sus estándares éticos y técnicos a nivel global (Espinosa de los Monteros Pérez-Brotóns & Sanz Setién, 2024).

Sin embargo, la implementación práctica del reglamento revela las tensiones persistentes entre el objetivo de armonización y la realidad fragmentada de la UE (Ricart, 2024). Como menciona Ricart, las diferencias estructurales entre Estados miembros —en términos de capacidades institucionales, cultura administrativa o disponibilidad de recursos técnicos— generan interpretaciones divergentes que amenazan con debilitar la coherencia del sistema. Esta fragmentación se manifiesta en dos niveles: las divergencias entre los Estados miembros y la coexistencia de distintas aproximaciones regulatorias a escala global (Tuset Varela, 2024), que trataremos en el siguiente punto. A pesar de los esfuerzos de la UE por regular y fomentar un desarrollo ético de la IA, esta se enfrenta a

una posible ralentización en este ámbito debido a la fragmentación normativa (El Derecho, 2024).

Uno de los elementos que podría intensificar esta fragmentación es la creación obligatoria de *regulatory sandboxes* nacionales —entornos de prueba controlados para el desarrollo de sistemas de IA—, cuya configuración y criterios varían según el país (EU Artificial Intelligence Act, 2024e). Como advierte la eurodiputada Aura Salla, esta exigencia conlleva el riesgo de generar un escenario regulatorio fragmentado que complique el cumplimiento normativo y cree incertidumbre jurídica para las empresas, debilitando así el mercado único digital europeo (Ahmed, 2025). Esta situación se agrava por la necesidad de coordinar múltiples autoridades nacionales, muchas de las cuales carecen de experiencia especializada en IA. A esto se suma la velocidad vertiginosa del desarrollo tecnológico, que amenaza con dejar obsoletas algunas disposiciones antes de que se apliquen de forma homogénea (Lebrun & Lachguer, 2025).

Asimismo, la aplicación uniforme del *AI Act* se ve obstaculizada por la complejidad de coordinar múltiples autoridades nacionales y por la rapidez con la que evoluciona la tecnología de IA (Konopczyński, 2023). La interacción del *AI Act* con otras normativas existentes, como el RGPD, añade otra capa de complejidad que podría resultar en enfoques divergentes entre los Estados miembros (ANSA, 2025). Esta situación, unida a disparidades en los recursos disponibles entre países, puede dar lugar a interpretaciones divergentes del *AI Act* y, en consecuencia, a una implementación fragmentada del marco regulatorio europeo (Bertelsmann Stiftung, s.f.).

Consciente de los riesgos que plantea una aplicación fragmentada de las políticas de inteligencia artificial, la Comisión Europea puso en marcha en 2018 el Plan Coordinado sobre Inteligencia Artificial, actualizado en 2021, con el objetivo de alinear las estrategias nacionales, acelerar las inversiones y evitar una proliferación de enfoques dispares entre los Estados miembros (Comisión Europea, 2018). Este plan sirvió como base para el posterior desarrollo del *AI Act*, proporcionando un marco político de referencia que impulsó la necesidad de una legislación vinculante y armonizada (Cancela-Outeda, 2024). En coherencia con esta lógica de convergencia, el propio *AI Act* ha creado estructuras supranacionales específicas, como la ya mencionada Oficina Europea de Inteligencia Artificial y la Junta Europea de Inteligencia Artificial (European Commission, s.f.-b),

concebidas para reforzar la cooperación entre autoridades nacionales, emitir directrices interpretativas comunes y garantizar la interoperabilidad de los sistemas de supervisión (Comisión Europea, s.f.). No obstante, estos mecanismos se encuentran aún en una etapa inicial, y su eficacia dependerá en última instancia de la voluntad política de los Estados miembros para ceder parte de su flexibilidad normativa en favor de una gobernanza verdaderamente supranacional (Senter & Bruton, 2025).

Esta implementación fragmentada del *AI Act*, aplicada al sector de defensa, podría obstaculizar significativamente la cooperación entre los Estados miembros. Diferencias en la aplicación de la normativa pueden dificultar la interoperabilidad de los sistemas de defensa y limitar la eficacia de proyectos conjuntos dentro de la UE (Lawrenson & Sabatino, 2024). Esto es especialmente relevante en tecnologías de doble uso, como la IA aplicada a sistemas autónomos o de vigilancia, que requieren una coordinación estrecha para garantizar su desarrollo ético y seguro (Monaghan, 2023). Además, la falta de armonización regulatoria puede ralentizar el desarrollo de capacidades comunes en defensa, objetivo clave de iniciativas como la Cooperación Estructurada Permanente (Lamela Gallego, s.f.) y el Fondo Europeo de Defensa (Euro Funding, s.f.). En comparación con potencias como Estados Unidos, que adoptan marcos regulatorios más centralizados, la UE corre el riesgo de quedar rezagada en términos de integración militar si no logra establecer una regulación común y clara (Greene, 2024).

3.4. Marco regulatorio internacional en IA

Analizar los marcos regulatorios desarrollados por otras potencias permite situar el *AI Act* en un contexto geopolítico más amplio y entender cómo distintas concepciones sobre la gestión del riesgo derivado del uso de la IA pueden tener consecuencias directas sobre su aplicación en defensa. Aunque, como se ha señalado, el enfoque de la Unión Europea ha priorizado la protección de derechos fundamentales y la gobernanza ética, otros modelos, como el estadounidense o el chino, responden a lógicas estratégicas distintas, centradas en la competitividad, la innovación o la integración directa con capacidades militares (Pernot-Leplay, 2024). Esta comparación permite comprender mejor las implicaciones que tienen los distintos enfoques regulatorios sobre el desarrollo y aplicación de tecnologías emergentes en ámbitos estratégicos como la defensa. Al contrastar el enfoque

europeo con los modelos adoptados por otras potencias, se evidencian diferencias regulatorias que influyen en el desarrollo y la eficacia operativa en el ámbito militar, especialmente en un contexto marcado por la irrupción de tecnologías disruptivas y las crecientes tensiones geopolíticas (Chun, Schroeder de Witt & Elkins, 2024).

Como mencionábamos, la gobernanza de la IA se ha convertido en un elemento central de gobernanza tecnológica global. Como afirmó Vladimir Putin en 2017, "quien controle la IA, controlará el mundo" (Gigova, 2017). Si bien la Unión Europea ha optado por una regulación basada en valores y en la protección de derechos fundamentales (Torres Jarrín, 2021), otras potencias como Estados Unidos y China han desarrollado marcos regulatorios adaptados a sus prioridades nacionales, con un foco especial en la adopción rápida de capacidades militares y tecnológicas avanzadas (Tovar, 2025). Esta diversidad de enfoques no solo evidencia las distintas concepciones sobre el papel del Estado y la gestión del riesgo tecnológico, sino que también genera desequilibrios en el desarrollo de sistemas de IA (Fritz & Giardini, 2024), cuyas consecuencias serán analizadas en el siguiente capítulo.

Estados Unidos

Por un lado, Estados Unidos ha adoptado un enfoque descentralizado y orientado a la innovación (Observatorio de Inteligencia Artificial, 2025). En lugar de establecer un marco normativo exhaustivo, ha optado por una combinación de directrices sectoriales, recomendaciones no vinculantes y órdenes ejecutivas de alcance limitado (White & Case, 2025b). Entre las principales iniciativas destacan la *American AI Initiative* (Parker, 2020) y la *Executive Order on Safe*, *Secure, and Trustworthy Artificial Intelligence* de 2023 (Neenan & Sayler, 2023), que establecen prioridades estratégicas en materia de investigación, seguridad y colaboración público-privada, sin imponer obligaciones regulatorias estrictas.

Este modelo busca crear un entorno altamente competitivo en el que los actores privados —particularmente las grandes tecnológicas— lideren el desarrollo de soluciones de IA sin barreras normativas que obstaculicen la experimentación y la escalabilidad de estas tecnologías (Busquets Carretero, 2024). En el ámbito de defensa, esta lógica se ha institucionalizado con la creación, en 2022, del *Chief Digital and Artificial Intelligence*

Office, *CDAO* por sus siglas en inglés, que absorbió al anterior *Joint Artificial Intelligence Center*, *JAIC*, y consolidó otras estructuras dedicadas a la transformación digital del Pentágono (Gill, 2022). El CDAO actúa como núcleo central de gobernanza tecnológica, coordinando desde la adopción de sistemas autónomos y capacidades de ciberdefensa, hasta el uso de análisis predictivos y estándares éticos aplicables a tecnologías emergentes como la IA generativa (CDAO, s.f.).

Como menciona Busquets Carretero (2024), este enfoque se posiciona en una visión ideológica impulsada desde *Silicon Valley*, donde se promueve el concepto de *longtermism*: la idea de que una élite tecnológica debe liderar las decisiones estratégicas para resolver problemas globales a gran escala y asegurar la supervivencia futura de la humanidad (Barrett & Schmidt, 2022). Esta lógica refuerza el papel central de las grandes corporaciones en el desarrollo de tecnologías críticas, particularmente en el ámbito de defensa (Krauss, 2024). Asimismo, al no imponer restricciones regulatorias excesivas, se favorece la agilidad del ecosistema tecnológico y se estimula el liderazgo en innovación (Vereckey, 2023), especialmente en sectores como el de defensa. Sin embargo, esta misma flexibilidad ha dado lugar a una fragmentación normativa entre Estados y agencias, lo que dificulta la coordinación institucional, debilita la supervisión sobre el uso de estas tecnologías y plantea problemas de coherencia estratégica a nivel federal (Stone, 2020).

Aunque este enfoque ha permitido a Estados Unidos consolidarse como referente en innovación tecnológica, especialmente en defensa (Fierro Rodríguez, 2024), también pone en evidencia limitaciones estructurales significativas. La ausencia de una legislación federal integral en materia de IA ha dado lugar a un entorno regulatorio fragmentado, caracterizado por marcos dispares entre estados y organismos federales (ICEX, 2024). Según el informe del ICEX, esta dispersión normativa no solo dificulta la coordinación institucional y la implementación de estándares éticos homogéneos, sino que también obstaculiza la formulación de una estrategia nacional coherente. En un contexto de competencia geopolítica intensificada, esta falta de armonización puede debilitar la capacidad del país para definir una posición unificada y eficaz sobre el desarrollo, la gobernanza y el uso estratégico de la IA en defensa (Kumayama, Levi & Ridgway, 2025).

China

Por otro lado, China ha desarrollado un modelo altamente centralizado, basado en una estrategia de la "*intelligentization*" de la guerra, entendida como la transformación del ámbito militar mediante la integración de inteligencia artificial, *big data* y sistemas autónomos en todas las fases del conflicto (Baughman, 2024). A través de la política de fusión militar-civil, el gobierno chino coordina de manera estratégica la colaboración entre sectores civiles, militares e industriales para incorporar las últimas tecnologías en su planificación y operaciones militares (Ruiz, 2025). Esta estrategia se traduce, según Ruiz, en la implicación directa de empresas tecnológicas como Huawei o Baidu en proyectos vinculados al Ejército Popular de Liberación (EPL), lo que facilita la transferencia de innovaciones del sector civil al ámbito militar. Además, en el ámbito de defensa, este modelo implica una doctrina cada vez más dependiente de tecnologías disruptivas. Bajo el concepto de "*intelligentized warfare*", el EPL busca integrar IA en la toma de decisiones operativas, la guerra electrónica, los sistemas de misiles autónomos, el reconocimiento avanzado y las operaciones cibernéticas ofensivas (Takagi, 2022).

En el plano normativo, China ha optado por un enfoque regulador basado en directrices emitidas por el Consejo de Estado, el Ministerio de Ciencia y Tecnología y la Administración del Ciberespacio de China (CAC) (White & Case, 2025c). En lugar de una ley única como el *AI Act* europeo, el gobierno chino regula la IA a través de múltiples normativas sectoriales y mecanismos de control previos al lanzamiento. Entre ellas destacan las medidas sobre algoritmos de recomendación (2022) y los servicios de IA generativa (2023), que establecen requisitos de registro, transparencia y alineación con los valores socialistas para las empresas tecnológicas (Fernández, 2023).

Este modelo presenta beneficios como la capacidad del Estado chino para coordinar eficazmente a universidades, empresas tecnológicas y organismos militares, lo cual facilita una implementación rápida y estratégica de soluciones de IA en operaciones militares (Lacort, 2025). Sin embargo, este avance se ve limitado por restricciones externas, como las impuestas por Estados Unidos a la exportación de semiconductores avanzados, lo que afecta a la autosuficiencia tecnológica de China y podría obstaculizar su liderazgo global en IA (Parolari, 2025).

Estos distintos enfoques internacionales en la regulación de la IA reflejan una gran desigualdad tanto en el plano normativo como en el tecnológico, ya que cada potencia prioriza sus propios intereses estratégicos (Wu & Liu, 2023). Mientras que la UE se centra en los valores y derechos, Estados Unidos apuesta por la innovación, y China lo integra como parte de su estrategia de defensa. Esta falta de coordinación global dificulta la colaboración entre países, especialmente cuando no existen reglas comunes claras (Variengien & Martinet, 2024). Además, el dominio tecnológico de Estados Unidos y China puede generar situaciones de dependencia para otros países que no tienen capacidad para desarrollar o controlar sus propios sistemas (Cuenca, 2020). Es por ello que, uno de los grandes retos actuales es encontrar espacios de cooperación internacional que garanticen un desarrollo más equilibrado y seguro de la IA (Rodríguez, 2025).

4. El impacto del *AI Act* en la competitividad europea

Tras haber analizado el contexto normativo y estratégico del *AI Act*, es pertinente examinar cómo esta regulación puede afectar a la competitividad europea, especialmente en el ámbito de la defensa. Este capítulo analiza cómo la normativa impulsada por la UE influye tanto en su posicionamiento tecnológico como en su autonomía estratégica. En particular, se examina hasta qué punto el liderazgo normativo europeo puede constituir una ventaja competitiva para la UE.

Para ello, se abordarán tres dimensiones clave. Primero, se ofrece una definición amplia de competitividad y ventaja competitiva, estableciendo los marcos teóricos necesarios para evaluar el rendimiento europeo en relación con otras potencias. Después, se analiza en qué medida el liderazgo regulatorio europeo en inteligencia artificial puede considerarse una fuente de ventaja competitiva estratégica, reforzando la legitimidad internacional de la UE y su poder de atracción normativa. Por último, se examinan los desafíos que esta estrategia plantea para la autonomía tecnológica y militar, señalando las posibles limitaciones del modelo europeo frente a potencias que priorizan una integración directa entre innovación e industria militar. Con ello, este apartado busca poner en perspectiva la hipótesis inicialmente planteada: cómo afecta el *AI Act* en la capacidad de Europa para mantenerse como actor competitivo, autónomo y relevante en un escenario global marcado por la aceleración tecnológica y las crecientes tensiones geopolíticas.

4.1. Definición de competitividad y ventaja competitiva

Para entender el impacto del *AI Act* en la competitividad militar es esencial definir este concepto y su composición. La competitividad global se entiende como la capacidad de una economía para alcanzar niveles sostenidos de crecimiento económico que generen bienestar a largo plazo para su población (Schwab, 2016). Asimismo, según el WEF (2016), la competitividad se define como "el conjunto de instituciones, políticas y factores que determinan el nivel de productividad de un país". La productividad, en este sentido, no solo marca el nivel de ingresos que un país puede alcanzar, sino que también determina su capacidad para innovar, generar empleo de calidad y mantener una posición sólida en el sistema internacional (Organización Internacional del Trabajo, 2020). En este sentido, Porter (2004) define la competitividad como la capacidad de una nación para producir bienes y servicios que resulten exitosos en los mercados internacionales, al tiempo que aseguran niveles crecientes de prosperidad para su población. Esta definición integra dimensiones tanto económicas como sociales, y en el contexto actual, incluye también criterios de sostenibilidad, gobernanza digital y liderazgo en tecnologías emergentes.

El WEF estructura esta competitividad en torno a 12 pilares fundamentales que permiten evaluar el rendimiento de un país en múltiples dimensiones. Estos pilares son: 1) instituciones, 2) infraestructuras, 3) entorno macroeconómico, 4) salud y educación primaria, 5) educación superior y formación, 6) eficiencia del mercado de bienes, 7) eficiencia del mercado laboral, 8) desarrollo del mercado financiero, 9) preparación tecnológica, 10) tamaño del mercado, 11) sofisticación empresarial y 12) capacidad de innovación (WEF, 2016, p. 4). Este enfoque integral permite considerar no solo factores económicos objetivos, sino también elementos institucionales, sociales y tecnológicos esenciales para el posicionamiento estratégico de los países. En el contexto del presente trabajo, y dada la naturaleza tecnológica, estratégica y regulatoria del tema tratado, se prestará especial atención a tres pilares clave del análisis del WEF: la capacidad de innovación, como indicador directo del liderazgo tecnológico; la preparación tecnológica, que permite evaluar el grado de adopción e integración de tecnologías emergentes; y las instituciones, cuyo diseño e implementación regulatoria son determinantes para orientar o restringir el desarrollo de sectores como la IA aplicada a defensa.

Adicionalmente, el concepto de ventaja competitiva permite complementar este análisis al centrarse en los elementos que permiten a un país o región diferenciarse de forma sostenible en un entorno internacional altamente dinámico (Porter, 1990). Según Porter (1990), esta ventaja no se deriva únicamente del acceso a recursos o de la reducción de costes, sino de la capacidad para innovar, desarrollar capacidades especializadas y aprovechar eficazmente su entorno institucional y productivo. En otras palabras, una nación posee una ventaja competitiva cuando es capaz de generar un valor superior mediante productos o servicios difíciles de replicar, sosteniendo dicha posición en el tiempo gracias a factores como la calidad de sus instituciones, su entorno regulador, su capital humano o su infraestructura tecnológica (Dunning, 1992).

En el contexto de la IA aplicada a defensa, la noción de competitividad adquiere una dimensión estratégica especialmente compleja y multifacética. No se trata únicamente de poseer capacidades tecnológicas avanzadas, sino de poder implementarlas dentro de entornos científicos, industriales y regulatorios lo suficientemente sólidos como para garantizar una integración efectiva y segura en las estrategias de defensa (Mikhailov, 2023). La ventaja competitiva, por tanto, no se construye solo sobre el nivel de desarrollo técnico, sino sobre la capacidad de implementar, adaptar y escalar estas soluciones dentro de marcos que respondan tanto a los intereses estratégicos nacionales como a los valores que los sustentan (Instituto Español de Estudios Estratégicos, 2015). Sin embargo, en la práctica, resulta complejo evaluar el nivel de integración y cumplimiento equitativo de todos estos pilares. Por ello, al retomar el enfoque propuesto por el WEF, se observa que en función del eje que se priorice, cada una de las principales potencias tecnológicas —Estados Unidos, China y la Unión Europea— ha desarrollado una ventaja competitiva diferenciada en el ámbito de la IA aplicada a defensa. Estados Unidos, por ejemplo, destaca en los pilares de capacidad de innovación y sofisticación empresarial, gracias a un ecosistema dinámico liderado por empresas tecnológicas con fuerte capacidad de inversión, experimentación y crecimiento (O'Brien, 2024). Este dinamismo permite un despliegue ágil de tecnologías disruptivas, incluso en sectores como el militar. China, por su parte, ha logrado fortalecer su ventaja competitiva en base a pilares como la preparación tecnológica y la infraestructura, integrando la IA dentro de su estrategia de "*intelligentized warfare*" mediante una planificación centralizada y una estrecha coordinación entre el sector civil y el institucional, el EPL (Baughman, 2024). Esta

sinergia le permite movilizar rápidamente sus recursos para el desarrollo y despliegue de tecnologías emergentes en el ámbito militar.

Por su lado, la UE ha centrado su estrategia en el pilar institucional y en el desarrollo de un marco normativo ético, convirtiéndose en referente mundial en gobernanza tecnológica. Su fortaleza reside en la capacidad de establecer estándares regulatorios exigentes que protegen los derechos fundamentales y promueven la transparencia y la rendición de cuentas (European Comission, 2024). No obstante, este liderazgo normativo plantea retos específicos para la competitividad operativa de la Unión Europea en sectores estratégicos como la defensa, donde el equilibrio entre innovación tecnológica, seguridad y principios éticos resulta especialmente complejo (Paniagua, 2023). En los siguientes apartados se examinará hasta qué punto este enfoque regulatorio puede constituir una ventaja competitiva para la UE —al posicionarla como referente global en gobernanza tecnológica— y, al mismo tiempo, cómo puede suponer una desventaja frente a potencias que priorizan la rapidez innovadora y la integración directa de la IA en sus capacidades militares, afectando así a su autonomía.

4.2. Liderazgo regulatorio como ventaja competitiva

El liderazgo normativo que ejerce la Unión Europea en el ámbito de la inteligencia artificial no es casual ni reciente, sino que responde a una lógica estructural propia de su modelo de integración (Cancela-Outeda, 2024). En efecto, según explica Manners (2002), la UE ha construido históricamente su influencia internacional a través del derecho, la regulación y la promoción de valores democráticos, en lugar de recurrir a instrumentos de *hard power* como la coerción militar o la supremacía económica. Esta tradición normativa se ha consolidado en lo que se conoce como "*regulatory power Europe*" clasificando a la UE de potencia reguladora debido a su enfoque basado en la creación de estándares globales —ya sean medioambientales, digitales o tecnológicos— que definen indirectamente las reglas del juego a nivel mundial (Hadjiyianni 2021).

A menudo se repite que "Estados Unidos innova, China fabrica y Europa regula" (García Paudo, 2025). Esta fórmula refleja la estrategia diferenciada que caracteriza a las tres grandes potencias tecnológicas. A diferencia de la UE, Estados Unidos se apoya en una

competitividad tecnológica basada en la agilidad del sector privado (Innobasque, 2024), mientras que China integra el desarrollo tecnológico en su doctrina de seguridad nacional (Antonio, 2023). En el caso europeo, la regulación se ha convertido en una herramienta de proyección geopolítica que permite ampliar su esfera de influencia sin necesidad de recurrir a la competencia militar o a subsidios masivos a la industria. Tal como sugiere Colomina (2023), este liderazgo normativo puede considerarse una forma de *soft power* competitivo, especialmente cuando se logra que actores externos adopten regulaciones europeas como condición para acceder a su mercado, reforzando así el *Brussels Effect* ya descrito anteriormente.

Este enfoque se ha visto reflejado en múltiples precedentes regulatorios, como el Reglamento General de Protección de Datos (RGPD) o la Ley de Servicios Digitales, que han servido para proyectar los valores europeos en la gobernanza digital (Daturex, 2024). En esta línea, el *AI Act* constituye un claro ejemplo del liderazgo normativo europeo. Si bien ya se han abordado anteriormente los contenidos del reglamento, es importante destacar que la capacidad de establecer reglas claras, predecibles y alineadas con principios éticos constituye en sí misma una ventaja competitiva para Europa (Otero Iglesias, 2024). En un entorno internacional marcado por la fragmentación regulatoria y la creciente desconfianza tecnológica, la UE ofrece un marco institucional que proporciona seguridad jurídica y estabilidad a los actores del ecosistema tecnológico (Chalom, 2024). Como ha señalado la Comisión Europea en el *White Paper for European Defence Readiness 2030* (2025), el objetivo de una defensa robusta e innovadora no puede desvincularse de la creación de un ecosistema regulatorio eficiente que proporcione "predictibilidad industrial" y facilite "el desarrollo tecnológico responsable" (European Commission, 2025). En este sentido, el marco normativo europeo no solo actúa como un mecanismo de control, sino también como una palanca para orientar el desarrollo de tecnologías duales hacia objetivos estratégicos compartidos, reforzando al mismo tiempo la soberanía tecnológica de la Unión.

Pero más allá del mercado, este enfoque se ha trasladado explícitamente al terreno estratégico. La creación de la Vicepresidencia Ejecutiva para la Soberanía Tecnológica, la Seguridad y la Democracia, otorgada a Henna Virkkunen para el periodo 2024–2029, sitúa la política tecnológica en el núcleo de la competitividad europea (Stannard, Agius & Szewczyk, 2025). Como se recoge en este nuevo mandato, el objetivo es convertir la

IA en un eje estratégico para la autonomía tecnológica de Europa, articulando una gobernanza normativa que asegure tanto la protección de derechos como la resiliencia del ecosistema industrial (Agenzia Nova, 2025). Además, este liderazgo normativo permite a la UE marcar la agenda internacional en foros multilaterales como la OCDE, el G7 o Naciones Unidas, proyectando su modelo ético de IA en debates sobre autonomía tecnológica y usos militares (Maremonti, 2024).

Por lo tanto, y como ya se adelantaba en el apartado anterior, este tipo de liderazgo regulatorio puede considerarse una ventaja competitiva en sí misma. No solo permite a la UE situarse como referente ético y jurídico en un contexto tecnológico incierto (Colomina, 2023), sino que también le otorga capacidad para moldear el mercado internacional desde su propia visión estratégica, maximizando su influencia a través del derecho en lugar de la fuerza (Euronews, 2023). Sin embargo, en el siguiente apartado se examinará hasta qué punto este posicionamiento constituye una ventaja competitiva o un estancamiento en materia de seguridad europea (Quarles Van Ufford, 2025).

4.3. Desafíos regulatorios para la autonomía tecnológica estratégica

Si bien el liderazgo normativo ha sido durante años una de las herramientas más distintivas del poder europeo, sus efectos en el ámbito tecnológico plantean desafíos importantes cuando se confronta con objetivos de autonomía estratégica. En sectores altamente dinámicos como el de IA aplicada a la defensa, la velocidad de desarrollo, la escalabilidad y la capacidad de adaptación tecnológica se convierten en elementos esenciales para preservar ventajas operativas frente a potencias rivales.

La preferencia de la UE por garantizar un uso ético de la inteligencia artificial, aunque legítima, presenta una aplicación excesivamente rígida en el ámbito de las tecnologías duales, lo que puede ralentizar de forma sustancial el ciclo de innovación (Gehrke, 2025). Tal como señala el *White Paper on European Defence Readiness 2030* (2025), el ecosistema industrial europeo no está preparado para responder a la aceleración tecnológica global, en parte debido a la ausencia de un mercado interior plenamente funcional y a la fragmentación de marcos regulatorios entre Estados miembros.

En paralelo, el informe Draghi (2024) identifica la complejidad administrativa, la escasa coordinación institucional y el exceso de cautela normativa como factores estructurales que dificultan la consolidación de una base tecnológica autónoma. A pesar de las inversiones anunciadas, Europa mantiene una posición rezagada en componentes críticos como semiconductores o software de defensa (Cordero, 2024). La situación es especialmente grave en el ámbito de las tecnologías duales, donde la falta de un ecosistema sólido de transferencia de conocimiento y la ausencia de una política industrial paneuropea han frenado la conversión del conocimiento científico en aplicaciones tecnológicas estratégicas (Martí Sempere, 2024).

Este desfase normativo se refleja también en la pérdida de competitividad de startups tecnológicas europeas (Politico, 2024). Las exigencias del *AI Act* han incrementado hasta un 35 % los costes operativos para estas empresas —en particular, por el cumplimiento de requisitos de transparencia algorítmica—, lo que ha llevado a muchas a trasladar sus centros de desarrollo a entornos más favorables como Estados Unidos o Israel (Greene, 2024). Esta fuga de talento y capital, unida a la creciente dependencia de chips asiáticos y software estadounidense (Hernández,2024), compromete directamente los márgenes de maniobra de Europa en un escenario internacional cada vez más volátil.

Como advierte la Comisión Europea (2025), la consolidación de un verdadero mercado interior de defensa pasa necesariamente por una profunda simplificación regulatoria, una armonización de los procesos de certificación y una estrategia compartida de inversión en tecnologías críticas. Sin esta coordinación efectiva, la UE difícilmente podrá garantizar el acceso seguro a capacidades clave ni resistir presiones externas sobre sus cadenas de suministro (Comisión Europea, 2025). La interrupción del acceso a componentes estratégicos —por ejemplo, ante una posible escalada en el estrecho de Taiwán— evidenciaría la vulnerabilidad europea frente a tensiones geopolíticas (Hyeon Choi, 2025).

En última instancia, el equilibrio entre protección de derechos fundamentales e impulso a la innovación exige un replanteamiento estratégico del marco normativo vigente. Como se señala en el informe Draghi (2024), la soberanía tecnológica no se construye únicamente desde la regulación, sino también desde la capacidad real de desarrollar, producir y desplegar tecnologías propias en condiciones de competitividad global. A

medida que la carrera por el liderazgo en defensa inteligente se intensifica, será imprescindible dotar a los valores normativos europeos de operatividad estratégica, asegurando que no se conviertan en freno para la autonomía que se pretende defender (Tuma, 2025).

5. Implicaciones del *AI Act* en defensa

El presente capítulo examina de forma detallada las implicaciones que el *AI Act* genera en el ámbito de la defensa, no tanto por su aplicación directa —ya que el reglamento excluye expresamente los usos militares—, sino por sus efectos indirectos sobre tecnologías de doble uso, procesos de innovación y dinámicas económicas estratégicas. Estas implicaciones permiten comprobar si la normativa europea, aunque formulada con fines éticos y civiles, está introduciendo obstáculos que afectan a la capacidad de la Unión Europea para desarrollar una base tecnológica autónoma en defensa.

Para ello, se abordan tres dimensiones interconectadas: las implicaciones estratégicas, centradas en la autonomía militar europea; las implicaciones en I+D, clave para entender las barreras a la innovación aplicada; y las implicaciones económicas, que permiten observar cómo el entorno regulatorio afecta a la competitividad industrial frente a otras potencias. Este enfoque transversal permite evaluar si, como plantea la hipótesis de este trabajo, el *AI Act* limita la proyección tecnológica y defensiva de la UE al restringir indirectamente el desarrollo de capacidades críticas en un entorno internacional marcado por la aceleración tecnológica y la creciente militarización de la inteligencia artificial.

5.1. Implicaciones Estratégicas: autonomía militar europea

En el campo de las Relaciones Internacionales, el concepto de "estrategia" ha evolucionado desde una acepción puramente militar —centrada en el empleo coordinado de medios para alcanzar objetivos bélicos— hacia una dimensión más amplia, que integra elementos políticos, económicos, tecnológicos y normativos en la formulación de objetivos de poder e influencia (Freedman, 2017). Según Gray (1999), la estrategia puede definirse como "el puente que conecta los fines políticos con los medios disponibles", es decir, como el proceso mediante el cual se alinean decisiones y recursos con el objetivo

de proteger y promover los intereses nacionales en un entorno competitivo. Esta expansión del concepto ha dado lugar a la división de las estrategias en función del recurso —como la estrategia energética, digital o industrial— que, aunque no están ligadas directamente al uso de la fuerza, condicionan la posición relativa de los Estados en el sistema internacional (Freedman, 2017).

A pesar de la amplitud de enfoques que recoge la estrategia, este trabajo se centrará particularmente en la dimensión militar de la estrategia, entendida por von Clausewitz (1989) como el diseño y despliegue de capacidades destinadas a garantizar la defensa y la disuasión frente a amenazas externas. Tal como señala el *White Paper for European Defence Readiness 2030* (European Commission, 2025), esta estrategia debe adaptarse a un entorno geopolítico marcado por una mayor inestabilidad, una creciente fragmentación del orden multilateral y una carrera tecnológica que redefine los parámetros tradicionales de la seguridad. En este contexto, la IA aparece como un potenciador de capacidades estratégicas, con posibles aplicaciones en todos los sectores. Por ello, el *AI Act* no puede analizarse únicamente desde una lógica legal o ética, sino también como un elemento que condiciona la autonomía militar de la UE (Perotto, 2023).

En este contexto, la posición regulatoria adoptada por la UE debe, asimismo, analizarse desde una perspectiva de "autonomía estratégica militar", definido como la capacidad de una entidad política —en este caso la UE— para actuar militarmente de forma independiente, sin depender de alianzas externas como, en su caso, la OTAN (Council of the European Union, 2016). Este objetivo, recogido en documentos clave como la Brújula Estratégica de 2022 (Consejo de la Unión Europea, 2022) o el Plan de Acción Europeo de Defensa (Comisión Europea, 2016), se ha intensificado en los últimos años como consecuencia de varios factores geopolíticos.

Entre ellos, la retirada de Estados Unidos de determinados escenarios europeos —como la retirada en la guerra de Ucrania desde la administración Trump (BBC News Mundo, 2025)— puso en evidencia la fragilidad europea en defensa dentro de la OTAN (Dello Iacono, 2025). Esta vulnerabilidad se hizo especialmente evidente tras el estallido de la guerra en Ucrania en 2022, cuando quedó claro que los Estados miembros dependían en gran medida del apoyo logístico, tecnológico y operativo de Estados Unidos para responder una amenaza de tal calibre (Aymerich, 2022). Además, bajo el mandato de

Trump, la atención estratégica de EE. UU. se ha desplazado hacia la región del Indo-Pacífico, considerada como un punto estratégico en la competencia con China (Schulenburg, 2025). Esta reorientación responde a la necesidad de contener el posicionamiento de China como potencia militar y dicho objetivo se ha visto reflejado en documentos como el *U.S. National Defense Strategy*, donde China es identificado como el "*pacing challenge*", es decir, el principal competidor estratégico que marca el ritmo del desarrollo militar estadounidense (US Department of Defense, 2022).

Este giro ha implicado un reajuste en el despliegue de recursos militares de EE. UU., priorizando su liderazgo militar frente a otras potencias y reduciendo su implicación en la seguridad europea (Sabbagh, 2025). En este sentido, las declaraciones aislacionistas de Trump —quien ha exigido que los países de la OTAN eleven su gasto en defensa hasta el 5% del PIB— intensifican la percepción europea de una creciente vulnerabilidad estratégica (Rizzi, 2025). Este escenario ha puesto en evidencia la vulnerabilidad estratégica de la UE en materia de defensa, al poner en cuestión el apoyo militar estadounidense y la capacidad de la UE en hacer frente a estos conflictos por cuenta propia (Beneyto, 2025). Esto ha intensificado el debate interno sobre la necesidad de reforzar la autonomía estratégica europea (Equipo Europa, 2023), así como reequilibrar las capacidades armamentísticas europeas. Tal como señala el *European Council on Foreign Relations* (Moscoso del Prado, 2023), sin una base industrial y tecnológica robusta, la autonomía europea seguirá siendo más un discurso que una realidad operativa. En este contexto, el desarrollo y control autónomo de tecnologías clave —como la IA aplicada a defensa— se ha convertido en un componente crítico no solo de modernización militar, sino de supervivencia geopolítica (Humble, 2024).

A pesar de la intención de la Unión Europea de garantizar un uso ético de las tecnologías de IA a través del *AI Act*, este marco regulatorio podría limitar la capacidad europea para integrar rápidamente tecnologías críticas en su sistema militar. El impacto abordado anteriormente de esta regulación en las tecnologías de doble uso condiciona la rapidez de innovación, la escalabilidad y la adaptabilidad de estas tecnologías necesarias para la defensa europea (Greene, 2024). En contraste, otras potencias como Estados Unidos y China han adoptado enfoques más flexibles que facilitan la rápida incorporación de la IA en sus sistemas de defensa. Este enfoque ágil les permite avanzar en capacidades militares basadas en IA sin las restricciones normativas que enfrenta la UE (Álvarez-Aragonés,

2024). Como resultado, la UE corre el riesgo de quedar "fuera de juego" en el ámbito militar debido a la rigidez de su gobernanza tecnológica, lo que limita su margen de maniobra estratégico frente a actores que alinean eficazmente sus prioridades normativas con objetivos geopolíticos de poder y disuasión (Pugnet & Kölsch, 2025). Esta situación plantea desafíos para el objetivo de la UE de lograr una autonomía estratégica en defensa. La insistencia en regular, aunque bien intencionada, podría obstaculizar la posición de Europa como líder en IA y poner de manifiesto su retraso militar en un escenario donde el desarrollo tecnológico es cada vez más crítico y fundamental (Torreblanca & Verdi, 2024).

5.2. Implicaciones en I+D

En el contexto de la IA aplicada a defensa, la investigación y el desarrollo (I+D) desempeñan un papel clave para garantizar la innovación tecnológica necesaria para mantener capacidades militares actualizadas y eficaces (Daniels, 2019). El I+D puede definirse, según la OCDE (2015), como el «conjunto de actividades creativas y sistemáticas realizadas para aumentar el caudal de conocimientos —incluido el conocimiento del ser humano, la cultura y la sociedad— y para idear nuevas aplicaciones de los conocimientos disponibles». Esta definición incluye tanto la investigación básica como la investigación aplicada y el desarrollo experimental. En defensa, estas actividades no solo permiten anticiparse a nuevas amenazas, sino que también son esenciales para transformar el conocimiento científico en soluciones concretas —como sistemas autónomos, herramientas de ciberdefensa o capacidades de reconocimiento— adaptadas a entornos complejos como el militar (Ahmedoğlu, 2024).

En este marco, el *AI Act* introduce ciertas brechas con los objetivos europeos de reforzar su base industrial en defensa, al imponer requisitos normativos que pueden obstaculizar la agilidad del proceso innovador (CMS, 2025). A pesar de que el Reglamento contempla excepciones para actividades de investigación científica no destinadas directamente al mercado, según recoge el art. 2 y el 25 (Diario Oficial de la Unión Europea, 2024), estas exclusiones no se aplican al desarrollo experimental ni a las fases de validación tecnológica, etapas críticas en el ámbito de la defensa (Hickman, Lorenz, Teetzmann & Jha, 2024). Esta limitación ha generado un fenómeno de "fuga de innovación", en el que

startups y centros tecnológicos trasladan sus actividades a regiones con marcos más flexibles para evitar la incertidumbre asociada al cumplimiento del *AI Act* (Keslassy, 2025). Esta tendencia responde a una dinámica ya observada tras el estallido de la guerra en Ucrania, cuando el fuerte incremento en los costes energéticos llevó a numerosas startups a trasladarse a entornos más estables y competitivos, tanto en términos regulatorios como operativos, como el de EE. UU. (Zachová, 2023). Además de la pérdida de competitividad tecnológica que esta fuga conlleva, también se ve limitado al acceso a estas tecnologías innovadoras el sector de defensa (Brull, 2025).

En este contexto, el impacto del *AI Act* adquiere una relevancia particular, dado que su carga regulatoria limita la libre innovación en IA que resulta especialmente necesario para el rearme europeo (Quarles Van Ufford, 2025). A diferencia de otras potencias que apuestan por una inversión pública sostenida en capacidades militares, la Unión Europea presenta un gasto en innovación en defensa muy limitado (Tidey, 2025). Según datos de Lakeside Ventures, los gobiernos europeos destinan apenas un 4% de sus presupuestos de defensa a actividades de I+D, frente al 14% en el caso de Estados Unidos (Sahbaz, 2025). Esta brecha se traduce también en la financiación de startups tecnológicas. Según indica Shabaz, en 2024, las nuevas empresas del sector en Estados Unidos captaron 3.500 millones de dólares, mientras que sus homólogas europeas solo alcanzaron los 800 millones. En este escenario de inversión pública insuficiente, son precisamente las empresas tecnológicas con soluciones de doble uso las que han potenciado el desarrollo de capacidades innovadoras en defensa (McKinsey & Company, 2025a). Por ello, si la regulación europea no se adapta a las especificidades de estos actores —en particular las exigencias del *AI Act* en fases como el desarrollo experimental—, se corre el riesgo de acabar con uno de los pocos motores reales de modernización militar europea (Roberts, 2025).

Esta problemática se ve agravada por un dilema estructural más profundo denominado como "*innovation gap*" en el que la brecha entre la excelencia investigadora europea en IA y su poca capacidad para traducir ese conocimiento en desarrollos tecnológicos es cada vez más grande (Soete, 2025). Este fenómeno se traduce en una menor productividad en comparación con otras potencias, que sí logran canalizar con agilidad su producción científica hacia aplicaciones militares, lo que pone de manifiesto las dificultades de la UE para escalar sus avances tecnológicos (Giordano et al., 2024). Como argumenta Draghi

en su informe sobre la competitividad europea (2024), esta desconexión entre investigación y aplicación se debe, en gran medida, a la falta de mecanismos eficaces de transferencia de conocimiento y a la ausencia de una estrategia industrial paneuropea coherente. Incluso iniciativas ambiciosas como *NextGenerationEU*, que movilizó más de 800.000 millones de euros para la recuperación y la transformación digital, han evidenciado importantes fallos de absorción. Como destaca Draghi (2024), las empresas no han aprovechado estos fondos al ritmo esperado, debido a obstáculos como la complejidad administrativa, la fragmentación institucional y la incertidumbre sobre el retorno de la inversión en sectores regulados como el de IA.

En consecuencia, el ciclo de innovación en defensa —que requiere agilidad, escalabilidad y visión estratégica a largo plazo (McKinsey & Company, 2025b)— se ve interrumpido en sus fases más críticas. En este contexto, un marco regulatorio como el del *AI Act*, que añade nuevas exigencias, puede convertirse en un factor que intensifique esta brecha, afectando directamente a la soberanía tecnológica de la UE y su capacidad para responder con rapidez a los desafíos emergentes (Van Oirsouw, 2024). Como respuesta, la Comisión Europea ha puesto en marcha iniciativas como las *AI Factories*, concebidas como nodos de innovación que conecten centros de supercomputación, universidades, industria y capital inversor (Bertuzzi, 2024). Con un fondo inicial de 1.500 millones de euros y participación de 15 Estados miembros, estas fábricas de IA buscan fomentar un ecosistema más dinámico que acelere el desarrollo tecnológico (Stannard, Agius & Szewczyk, 2025). No obstante, su alcance aún es limitado y no aborda plenamente los desequilibrios del sistema europeo de I+D en defensa (Torreblanca & Verdi, 2024).

En definitiva, el impacto del *AI Act* sobre la I+D en defensa revela una contradicción entre la ambición regulatoria de la Unión Europea y su capacidad real de innovación estratégica (Espinoza, 2024). Los efectos colaterales que tendrá en el ecosistema de innovación —especialmente en un contexto de inversión pública limitada, fuga de startups y fragmentación institucional— pueden comprometer los objetivos de soberanía tecnológica y rearme militar (Mundell, 2023; Martens, 2024). Sin un entorno más favorable para la transferencia de conocimiento y la inversión en startups de defensa, la UE corre el riesgo de quedarse atrás en la carrera por el liderazgo en defensa inteligente, precisamente cuando más necesita reforzar sus capacidades autónomas ante un orden internacional en transformación (Spasov, 2023).

5.3. Implicaciones Económicas

En un contexto de creciente rivalidad estratégica, las principales potencias han intensificado su inversión en tecnologías duales que combinan innovación civil con aplicaciones militares (SIPRI, 2024). La Unión Europea, a través del plan *ReArm Europe* —que prevé movilizar 800.000 millones de euros hasta 2030 (European Commission, 2025)—, busca reforzar sus capacidades defensivas. Sin embargo, esta apuesta por el refuerzo militar europeo se ve limitada por el aumento de los costes operativos derivados del marco regulatorio en materia de IA (KPMG, s.f), lo que ha ralentizado el desarrollo tecnológico en sectores clave y ha contribuido a una fuga innovación hacia ecosistemas más favorables (Whittaker, 2023). Mientras Estados Unidos y China avanzan con marcos regulatorios más flexibles e integradores, el principal riesgo para la Unión Europea reside en que su enfoque sobrerregulado no solo limite su autonomía tecnológica, sino que también comprometa su capacidad operativa en materia de defensa (Engler, 2023).

5.3.1. Presupuestos y proyecciones de gasto en defensa: Estados Unidos, China y la Unión Europea (2025-2030)

Como mencionábamos, la escalada geopolítica global ha intensificado las inversiones militares de las principales potencias, con estrategias que combinan modernización tecnológica, expansión de capacidades y cooperación regional (Baldor, 2024). Para analizar las implicaciones económicas del *AI Act,* se ha realizado un análisis, basado en datos oficiales y reportes recientes que comparan las tendencias presupuestarias de Estados Unidos, China y la Unión Europea. Este contexto es esencial para entender las implicaciones que esta regulación presenta en materia de defensa.

Estados Unidos: Consolidación del liderazgo militar

Por un lado, según el *U.S. Senate Committee on Appropriations* (2025) el presupuesto de defensa propuesto en EE. UU. para 2025 asciende a 852.200 millones de dólares, un 3,3% más que en 2024. Tal como se detalla en la Comisión de Asignaciones del Senado de EE. UU. (2025), el presupuesto de defensa para 2025 contempla asignaciones específicas destinadas a fortalecer capacidades clave, entre ellas, una inversión adicional de 280

millones de dólares para el desarrollo del sistema de propulsión adaptativa de la Fuerza Aérea (Lee Harpley, 2024), y 200 millones destinados a mitigar riesgos industriales dentro del programa de disuasión estratégica terrestre (Liang, 2025).

Asimismo, la Oficina Presupuestaria del Congreso (CBO) de EE. UU. (2024) estima que el gasto anual en defensa podría ascender a 965.000 millones de dólares en 2039, impulsado principalmente por un aumento del 64% en los costes operativos y del 32% en los programas de adquisición. No obstante, el informe advierte que estas proyecciones podrían resultar conservadoras: si los costes evolucionan conforme a las tendencias históricas, el gasto real acumulado entre 2025 y 2039 podría superar en un 5% las previsiones actuales, lo que obligaría a realizar ajustes presupuestarios adicionales o a solicitar fondos extraordinarios.

China: Crecimiento sostenido con foco tecnológico

Por otro lado, según datos del *Central People's Government of China* (2025), el presupuesto de defensa del país aumentará un 7,2% en 2025, alcanzando los 1,78 billones de yuanes —aproximadamente 249.000 millones de dólares—. Este incremento, que mantiene el gasto militar en torno al 1,4% del PIB, consolida a China como el segundo mayor inversor en defensa a nivel mundial (Lei, 2025). Su estrategia de modernización militar prioriza el desarrollo de capacidades avanzadas, con un énfasis particular en dos ámbitos estratégicos: los sistemas de misiles de alcance medio y largo —como el *Conventional Prompt Strike*, diseñado para realizar ataques de alta precisión en tiempos mínimos (Campbell, 2021)—, y el refuerzo de su flota naval, tanto en términos de volumen como de sofisticación tecnológica (China Power, 2018). Esta última se traduce en una expansión significativa de destructores de nueva generación, submarinos nucleares y portaaviones, con el objetivo de proyectar poder en el mar de China Meridional y más allá (China Daily, 2025). Estas inversiones forman parte de una estrategia de seguridad más amplia, centrada en la "*intelligentization*", que busca integrar IA, automatización y capacidades cibernéticas en la planificación y ejecución de operaciones militares, consolidando así una postura disuasoria creíble frente a rivales regionales y globales (Kania, 2019).

Unión Europea: Rearme colectivo ante nuevas amenazas

Por su lado, en marzo de 2025, la Comisión Europea presentó el plan *ReArm Europe*, una ambiciosa estrategia destinada a reforzar la base industrial y tecnológica de defensa de la UE mediante la movilización de hasta 800.000 millones de euros hasta 2030 (European Parliament, 2025). Según menciona Ruitenberg (2025), el plan contempla, entre otras medidas, la concesión de préstamos por valor de 150.000 millones de euros para adquisiciones conjuntas, la flexibilización del Pacto de Estabilidad —permitiendo déficits públicos de hasta el 3,5% del PIB si se destinan a inversiones en defensa—, así como incentivos fiscales específicos para impulsar sectores estratégicos como los drones, la ciberdefensa o la movilidad militar. El objetivo es elevar progresivamente el gasto agregado en defensa hasta el 2,5% del PIB, frente al 1,9% registrado actualmente (Statista, 2025). Según ha señalado Tidey (2025), las prioridades del programa se centran en fortalecer capacidades críticas como la defensa aérea, la artillería y la producción de municiones, promoviendo al mismo tiempo la reducción de la dependencia externa mediante un enfoque coordinado de compras intracomunitarias.

Tabla 1: Comparativa de presupuestos

País/Región	**Presupuesto 2025 (USD)**	**% PIB 2025**	**Proyección 2030 (USD)**
Estados Unidos	852.200 millones	3.5%	965.000 millones
China	249.000 millones	~1.4%	No Disponible
Unión Europea *	326.000 millones	2.5%	800.000 millones

Fuente: Elaboración propia con datos extraídos de Insinna (2024); Congressional Budget Office (2024); Central People's Government of China (2025); European Council (2025).

*Estimación basada en proyecciones de gasto agregado de los Estados miembros.

5.3.2. Relación entre los sectores público y privado en defensa

Asimismo, conviene entender la relación entre los sectores público y privado en el desarrollo de tecnologías duales con IA ya que varía significativamente entre las tres

principales potencias —Estados Unidos, China y la Unión Europea— reflejando así modelos económicos y prioridades estratégicas divergentes (Ilaria, Marsh & Reichberg, 2022).

Estados Unidos: Colaboración pragmática con controles estratégicos

En el caso de Estados Unidos, el modelo de desarrollo en tecnologías de IA aplicadas a defensa se basa en una estrecha colaboración público-privada, marcada por una regulación flexible (Kennedy, 2025). Como expone Tucker (2024), esta relación se articula en torno a tres pilares principales. En primer lugar, destaca la promoción de iniciativas conjuntas entre el Departamento de Defensa y empresas tecnológicas como Anduril, que han integrado herramientas desarrolladas por *OpenAI* en su plataforma Lattice para optimizar la detección y respuesta ante amenazas mediante drones autónomos. Este tipo de alianzas busca acelerar la innovación manteniendo estándares básicos de seguridad (Albon, 2024). En segundo lugar, bajo la nueva administración Trump, el enfoque regulatorio estadounidense continúa priorizando el control de exportaciones estratégicas —especialmente en lo relativo a tecnologías críticas de IA— como medida para limitar el acceso de países considerados como adversarios geopolíticos (Prensa EC, 2025). Sin embargo, a nivel interno, se mantiene una línea desreguladora en materia de investigación y desarrollo, con el objetivo de preservar la competitividad tecnológica nacional y evitar obstáculos normativos que ralenticen la innovación en sectores clave como la IA en defensa (France 24, 2025). En tercer lugar, este enfoque ha contribuido a consolidar un ecosistema innovador y competitivo: se estima que alrededor del 70% de las startups estadounidenses en defensa con aplicaciones de IA reciban financiación federal, y sectores como la ciberseguridad o los sistemas autónomos registran tasas de crecimiento cercanas al 12% anual (Tucker, 2024). Este modelo evidencia cómo un entorno normativo estratégico, combinado con inversión pública focalizada, puede fortalecer la autonomía tecnológica y el dinamismo innovador en sectores sensibles.

China: Fusión militar-civil obligatoria

Por otro lado, China aplica una estrategia de integración vertical basada en el principio de fusión militar-civil, que busca eliminar las barreras entre los sectores tecnológico,

industrial y de defensa (Pompeo, s.f.). En primer lugar, las directrices estatales establecen obligaciones explícitas de colaboración entre empresas privadas y el Ejército Popular de Liberación (EPL). Según la Comisión Europea (2024), compañías como Huawei, DJI o Hikvision están sujetas a marcos regulatorios que les obligan a transferir avances tecnológicos al sector militar; en este sentido, se estima que más del 90% de los sistemas de vigilancia desarrollados por Hikvision son utilizados en instalaciones del EPL. En segundo lugar, esta estrategia se apoya en una potente inversión pública: el programa *Made in China (MIC)* 2025 ha destinado más de 150.000 millones de dólares a tecnologías de uso dual, con prioridad en capacidades como enjambres de drones autónomos o sistemas avanzados de reconocimiento facial (Kowalski, 2025). Este programa estratégico —lanzado en 2015 por el Consejo de Estado chino— tiene como objetivo reducir la dependencia tecnológica del exterior y convertir a China en una superpotencia industrial en sectores clave como la robótica, los semiconductores, la IA y la defensa inteligente (Zamorin, 2023). A través de incentivos fiscales, subsidios y control estatal de la innovación, el MIC 2025 ha acelerado la fusión militar-civil, consolidando una base industrial capaz de traducir la investigación civil en capacidades operativas avanzadas para el Ejército Popular de Liberación (Sohail, 2024). Finalmente, a pesar de que este modelo ha impulsado el dinamismo innovador —con un crecimiento anual del 8% en patentes relacionadas con tecnologías duales (Chun, Schroeder de Witt & Elkins, 2024)—, su falta de transparencia en materia ética y normativa ha suscitado una creciente preocupación internacional respecto a los riesgos de militarización opaca de la IA (Buirrun, 2024).

Unión Europea: Equilibrio entre innovación y precaución

Sin embargo, la UE articula su estrategia en tecnologías de doble uso combinando instrumentos de financiación con un enfoque regulatorio particularmente estricto como es el *AI Act*. En primer lugar, según visto anteriormente, el plan *ReArm Europe* (2025) prevé movilizar hasta 800.000 millones de euros hasta el año 2030 con el fin de fomentar proyectos duales estratégicos, como el despliegue de drones autónomos para patrullas fronterizas con capacidades de IA (European Commission, 2025). En segundo lugar, la calificación según riesgos del *AI Act* conlleva exigencias adicionales, como certificaciones éticas obligatorias, evaluaciones de conformidad y auditorías externas, lo cual ralentiza significativamente los tiempos de desarrollo y despliegue (European

Institute, 2024). Finalmente, los efectos concretos de este enfoque regulatorio presentan resultados ambivalentes. Aunque países como Alemania o Francia han experimentado un incremento del 6 % en la adjudicación de contratos vinculados a tecnologías duales, múltiples actores del ecosistema de innovación —en particular las pymes— advierten que la complejidad administrativa impuesta por el marco normativo europeo dificulta su participación efectiva (Comunale & Manera, 2024). Esta burocracia excesiva no solo retrasa los procesos de validación y despliegue tecnológico, sino que también desincentiva la implicación de nuevos agentes en proyectos estratégicos (Monaghan, 2023)

A diferencia de Estados Unidos y China, que han optado por modelos de innovación acelerada en los que prima la rapidez en el desarrollo y la implementación de nuevas tecnologías, la Unión Europea continúa apostando por un enfoque más proteccionista, en el que la exigencia de altos estándares éticos y regulatorios constituye una prioridad central. Sin embargo, esta estrategia, acarrea importantes costes en términos de agilidad e impacto tecnológico en defensa, lo que limita su competitividad en un entorno global altamente dinámico (Sekine, 2024). Por lo tanto, Europa se enfrenta a dificultades económicas para conciliar su ambición normativa con las exigencias operativas de un ecosistema innovador cada vez más competitivo (Fuest et al., 2024).

6. Conclusiones

La regulación de la inteligencia artificial en Europa representa un intento ambicioso de establecer valores éticos, derechos fundamentales y liderazgo normativo. Sin embargo, cuando se analiza su impacto sobre sectores estratégicos como la defensa, surgen importantes tensiones entre los principios que sustentan dicha regulación y las exigencias de un entorno geopolítico cada vez más competitivo y tecnológico (Baldor, 2024). A lo largo de este trabajo se ha analizado en profundidad cómo la estructura y los efectos indirectos del *AI Act* —pese a su exclusión formal de los usos militares— afectan a tecnologías de doble uso, a la inversión en I+D y, en última instancia, a la competitividad y autonomía estratégica de la Unión Europea.

A partir de este análisis, pueden extraerse las siguientes conclusiones clave:

I. La estrategia regulatoria europea fortalece su poder normativo, pero pone en riesgo su posición en defensa: El *AI Act* proyecta a la Unión Europea como referente global en gobernanza ética de la IA, reforzando su reputación como "potencia reguladora" (Bradford, 2020). No obstante, su aplicación rígida y transversal —incluso sobre tecnologías potencialmente reutilizables en defensa— ralentiza la capacidad de innovación, reduce la escalabilidad de sistemas autónomos y limita la soberanía operativa europea frente a actores más flexibles como Estados Unidos o China (Buchholz, 2025; Greene, 2024).

II. Las tecnologías de doble uso se ven desproporcionadamente afectadas, creando una brecha en su aplicación militar: Los requisitos impuestos a los sistemas de alto riesgo —como la transparencia algorítmica o la supervisión humana— dificultan la adaptación de tecnologías civiles a usos estratégicos, especialmente en contextos donde la autonomía y la velocidad de respuesta son críticas (Boulanin et al., 2020). Esto entorpece la lógica del *dual use*, pilar fundamental para el rearme tecnológico europeo (Kosciuszko Institute & ECSO, 2024).

III. La fragmentación regulatoria dentro de la UE pone en peligro la interoperabilidad y la cooperación militar: La implementación nacional del *AI Act* ha resaltado divergencias institucionales y técnicas entre Estados miembros, debilitando proyectos conjuntos de defensa e impidiendo una respuesta cohesionada a desafíos tecnológicos compartidos (Lawrenson & Sabatino, 2024). Esta falta de armonización contrasta con modelos más centralizados como el estadounidense, donde agencias como el *Chief Digital and AI Office* coordinan la gobernanza tecnológica de defensa (Gill, 2022).

IV. El entorno normativo actual establecido por el *AI Act* desincentiva la inversión privada y favorece la fuga de startups tecnológicas: El incremento de costes regulatorios, la incertidumbre jurídica y la lentitud administrativa han provocado que muchas empresas europeas de IA trasladen su actividad a ecosistemas más flexibles (Whittaker, 2023). Esta dinámica compromete el desarrollo de una base industrial de defensa europea autosuficiente e intensifica la dependencia externa en sectores estratégicos (Draghi, 2024).

V. El liderazgo ético europeo puede ser una ventaja normativa, pero no garantiza competitividad operativa: Si bien la UE ha sabido posicionarse como defensor de un desarrollo responsable de la IA, este *soft power* regulatorio solo se traduce en ventaja competitiva si se acompaña de políticas industriales eficaces, inversión sostenida en I+D y capacidad de despliegue rápido de nuevas tecnologías (Fuest et al., 2024). En defensa, donde la innovación es un factor de supervivencia geopolítica, la regulación no puede actuar como freno.

VI. La desconexión entre regulación e innovación acentúa el "*innovation gap*" europeo: El desequilibrio entre producción científica y capacidad de escalado es especialmente visible en la UE, donde se generan avances en investigación que no se transforman en aplicaciones estratégicas debido a la rigidez normativa y la fragmentación institucional (Soete, 2025). Este desfase compromete las ambiciones de autonomía tecnológica europea y la posiciona en desventaja frente a potencias más ágiles.

VII. Es urgente una revisión adaptativa del marco regulador europeo para tecnologías estratégicas: Los retos que plantea el *AI Act* en defensa invitan a replantear el equilibrio entre ética y operatividad. La UE necesita un modelo más ágil, con regulaciones diferenciadas para tecnologías de doble uso, procesos de certificación acelerados y mecanismos de gobernanza adaptativa que permitan innovar sin renunciar a principios democráticos (Sekine, 2024). Sin este giro estratégico, la brecha entre los objetivos normativos de la UE y su realidad geopolítica seguirá ampliándose.

En este contexto, la Unión Europea ha comenzado a reconocer las limitaciones de su enfoque regulatorio actual. Prueba de ello es el *White Paper on European Defence Readiness 2030* (2025), que propone una estrategia integral para reforzar la autonomía estratégica del bloque, subrayando la importancia de la innovación tecnológica —en particular de la inteligencia artificial— para la seguridad europea (Rengel, 2025). El documento plantea medidas como compras conjuntas por valor de 150.000 millones de euros y una mayor flexibilidad fiscal orientada a fomentar el gasto en I+D militar. Paralelamente, el proceso legislativo del *AI Act* ha evolucionado hacia una lógica más pragmática. Según Haeck (2025), se han introducido ajustes normativos orientados a

reducir las cargas regulatorias sobre los modelos fundacionales y los sistemas de propósito general, acompañados de mecanismos de co-regulación y de previsión de revisión futura del reglamento. Estas iniciativas, impulsadas por la presión de varios Estados miembros y del sector tecnológico, reflejan una mayor concienciación sobre los efectos limitadores de la regulación en sectores estratégicos como la defensa. Si bien estos ajustes aún no constituyen una reforma sustantiva, permiten avanzar hacia una gobernanza más adaptativa, capaz de coordinar los valores fundacionales de la UE con las exigencias del entorno geopolítico y tecnológico actual.

Bibliografía

A&O Shearman. (2024). *Zooming in on AI – #10: EU AI Act – What are the obligations for "high-risk AI systems"?*. https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-10-eu-ai-act-what-are-the-obligations-for-high-risk-ai-systems

Academia de las Ciencias y las Artes Militares. (2024). *Impacto de la IA en el sector de la Defensa y Seguridad.* https://www.acami.es/noticia/impacto-de-la-ia-en-el-sector-de-la-defensa-y-seguridad/

Agenzia Nova. (2025). *UE: El Comisario Virkkunen dice que un plan nos hará más competitivos y seguros*. https://www.agenzianova.com/es/news/ue-commissaria-ue-virkkunen-piano-ia-ci-rendera-piu-competitivi-e-sicuri/

Ahmed, M. (2025). Transcript: Tech in 2025 — The EU vs Big Tech. Murad Ahmed speaks to Aura Salla, MEP in Brussels and former lobbyist for Meta. *Financial Times*. https://www.ft.com/content/8b43a2ae-fc02-4bfd-bfc2-15b05918f692

Ahmedoğlu, M. (2024). *Technological innovation in military R&D: perspectives between Mowery, Kaempffert, and Milward*. Medium. https://muminahmedoglu.medium.com/technological-innovation-in-military-r-d-perspectives-between-mowery-kaempffert-and-milward-

Albon, C. (2024). Anduril, OpenAI partner to boost counter-drone tech for bases, troops. *Defense News*. https://www.defensenews.com/pentagon/2024/12/05/anduril-openai-join-to-boost-counter-drone-tech-for-us-bases-troops/

Álvarez, R. (2024). *Inteligencia Artificial y Defensa: explorando las fronteras de la tecnología militar*. Defensa. Grupo Edefa. *ISSN: 3045-5170.*

Álvarez-Aragonés, P., (2024). *The New Arms Race in Dual-Use Technologies.* IE Insights. https://www.ie.edu/insights/articles/the-new-arms-race-in-dual-use-technologies/

Álvarez García, V. & Tahiri Moreno, J. (2023). La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque. *Revista General de Derecho Administrativo*, 63. https://laadministracionaldia.inap.es/noticia.asp?id=1514080

Ams, S. (2021). Blurred lines: the convergence of military and civilian uses of AI & data use and its impact on liberal democracy. *International Politics, 60*, 879 - 896. DOI:10.1057/s41311-021-00351-y

ANSA, (2025). *Interaction between AI Act and GDPR risks legal uncertainty*. ANSA. https://www.ansa.it/english/news/science_tecnology/

Antonio, A. (2023). La Doctrina De Xi Para Ganar Las Guerras Futuras. *Le Grand Continent.* https://legrandcontinent.eu/es/2023/06/11/la-doctrina-de-xi-para-ganar-las-guerras-futuras/

Aravena Flores, M. A. (2024). Dilemas derivados del uso de sistemas autónomos de armas letales en el derecho internacional humanitario. *Justicia*, ISSN 0124-7441, 29, 45. DOI: 0.17081/just.29.45.7143

Aymerich, R. (2022). Ucrania, la debilidad de Europa. *La Vanguardia*. https://www.lavanguardia.com/internacional/20220123/8005538/ucrania-debilidad-europa.html

Baldor, L.C. (2024). China has expanded its nuclear force and strengthened ties to Russia, the Pentagon says. *AP News*. https://apnews.com/article/china-military-taiwan-corruption-defense-9c1f0e145a250f2b8bd7f6f3dd4b7083

Banerjee, S. (2024). *Drone warfare in Myanmar: Strategic implications*. Observer Research Foundation. https://www.orfonline.org/expert-speak/drone-warfare-in-myanmar-strategic-implications

Beneyto, J. M. (2025). La vulnerabilidad de Europa es extrema sin el paraguas nuclear y militar de Estados Unidos. *La Razón*. https://www.larazon.es/internacional/vulnerabilidad-europa-extrema-paraguas-nuclear-militar-estados-unidos

Bertelsmann Stiftung, (s.f.). Implementation of the AI Act: numerous tensions with existing regulations. *Bertelsmann Stiftung.* https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/implementation-of-the-ai-act-numerous-tensions-with-existing-regulations

Bertuzzi, L. (2024). LEAK: EU Commission prepares 'strategic framework' to boost AI start-ups, generative AI uptake. *Euractiv*. https://www.euractiv.com/section/tech/news/leak-eu-commission-prepares-strategic-framework-to-boost-ai-start-ups-generative-ai-uptake/

Bieri, M. & Dickow, M. (2014). Lethal Autonomous Weapons Systems: Future Challenges. *CSS Analyses in Security Policy* 164, 3. https://doi.org/10.3929/ethz-a-010273874

Boulanin, V., Davison, N., Goussac, N. & Peldán Carlsson, M. (2020). Limits on Autonomy in Weapon Systems. *Stockholm International Peace Research Institute*, 23. https://www.sipri.org/sites/default/files/2020-06/2006_limits_of_autonomy_0.pdf

Bongioanni, M. (2024). *La carrera armamentista también pasa por la inteligencia artificial.* Valor Social. https://valorsocial.info/la-carrera-armamentista-tambien-pasa-por-la-inteligencia-artificial/

Borrell, J. (2020). *Por qué es importante la autonomía estratégica europea*. Servicio Europeo de Acción Exterior. https://www.eeas.europa.eu/eeas/por-qué-es-importante-la-autonomía-estratégica-europea_es

Bradford, A. (2020). *The brussels effect: how the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Brull, R. (2025). *Opinion: To close Europe's defence tech gap, governments must support startups.* The Next Web. https://thenextweb.com/news/european-governments-must-support-startups-close-defence-tech-gap

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., ... & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. https://arxiv.org/abs/1802.07228

Bueso Carrasco, E. (2025). ¿Cómo ha evolucionado la guerra con drones autónomos?. *Geopol 21*. https://geopol21.com/como-ha-evolucionado-la-guerra-con-drones-autonomos/

Buchholz, L. (2025). *BCG: The EU AI Act is a 'wake up call' for leaders to assess AI readiness. Here's what HR needs to know.* Unleash. https://www.unleash.ai/risk-compliance-regulation/bcg-the-eu-ai-act-is-a-wake-up-call-for-leaders-to-assess-ai-readiness-heres-what-hr-needs-to-know/

Buirrun, A. (2024). China tiene una IA comandante militar 'enjaulada' y dedicada a realizar simulacros de guerra. *La Razón*. https://www.larazon.es/tecnologia/china-tiene-comandante-militar-enjaulada-dedicada-realizar-simulacros-guerra

Busquets Carretero, X. (2024). *Trump y la tecnología: Silicon Valley toma el poder*. Computer World. https://www.computerworld.es/article/3611897/trump-y-la-tecnologia-silicon-valley-toma-el-poder.html

Calvo Pérez, J. L. (2020). *El debate sobre los sistemas de armas autónomos letales: perspectivas en el sistema internacional*. Ministerio de defensa, 5, 459. https://armada.defensa.gob.es/archivo/rgm/2020/04/rgmabril20cap5.pdf

Campbell, C. (2021). *China's military: The People's Liberation Army (PLA)* (CRS Report No. R46808). Congressional Research Service. https://www.congress.gov/crs-product/R46808

Cancela-Outeda, C. (2024). The EU's AI act: A framework for collaborative governance. *Internet of Things*, 27, 101291, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101291

Casem, G. (2021). *NF-16D VISTA becomes X-62ª.* Edwards Air Force Base. https://www.edwards.af.mil/News/Article/2714183/nf-16d-vista-becomes-x-62a/

CDAO. (s.f.). *Organization.* https://www.ai.mil/About/Organization/

Chalom, T. (2024). *The Global Race for AI Regulation.* NJI. https://www.njimedia.com/the-global-race-for-ai-regulation/

China Daily. (2025). *China to increase defense budget by 7.2 percent in 2025*. https://www.chinadaily.com.cn/a/

Chulilla Cano, J.L. (2023). Presente y futuro de los drones comerciales letalizados. *Revista general de marina*, ISSN 0034-9569, 284, 4, 673-684. https://armada.defensa.gob.es/archivo/rgm/2023/05/RGMMayo2023Parte05.pdf

Chun, J., Schroeder de Witt, C. & Elkins, E. (2024). *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US.* Oxford University. https://arxiv.org/pdf/2410.21279

CMS. (2025). *AI and IP in Defense sector.* CMS Law. https://cms.law/en/int/publication/ai-and-ip-in-defense-sector

Colomina, C. (2023). *Una IA ética: la UE y la gobernanza algorítmica.* CIBOD. https://www.cidob.org/publicaciones/una-ia-etica-la-ue-y-la-gobernanza-algoritmica

Comité Internacional de la Cruz Roja (CICR). (2019). *International humanitarian law and the challenges of contemporary armed conflicts: Recommitting to protection in armed conflict on the 70th anniversary of the Geneva Conventions*. https://international-review.icrc.org/es/articulos/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados-0

Comisión Europea. (2016). *Plan de Acción Europeo de Defensa.* https://ec.europa.eu/commission/presscorner/api/files/attachment/493161/factsheet_defence_action_plan_ES.pdf

Comisión Europea. (2018). *Plan coordinado sobre la inteligencia artificial. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM(2018) 795.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías & Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji. (2019). *Directrices éticas para una IA fiable.* Oficina de Publicaciones. https://data.europa.eu/doi/10.2759/14078

Comisión Europea. (2020). *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* COM(2020), 65, 5. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

Comisión Europea. (2021a). *Reglamento (UE) 2021/821 del Parlamento Europeo y Del Consejo*. Diario oficial de la UE. https://www.boe.es/doue/2021/206/L00001-00461.pdf

Comisión Europea. (2021b). *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*. https://espanadigital.gob.es/Brújula Digital 2030.pdf

Comisión Europea. (2025). *White Paper On options for enhancing support for research and development involving technologies with dual-use potential. COM(2024) 27 final*. https://research-and-innovation.ec.europa.eu/white-paper-dual-use-potential.pdf

Comisión Europea. (s.f.). *Junta de IA*. Configurar el futuro digital de Europa. https://digital-strategy.ec.europa.eu/es/policies/ai-board

Comunale, M. & Manera, A. (2024). *The Economic Impacts and the Regulation of AI: A Review of the Academic Literature and Policy Actions.* International Monetary Fund, 2024/65, 9798400268588. https://www.imf.org/-/media/Files/Publications/WP/2024/English/

Congressional Budget Office. (2024). *Long-Term Implications of the 2025 Future Years Defense Program*. https://www.cbo.gov/publication/61017

Consejo de la Unión Europea. (2022). *Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE en el próximo decenio*. https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

Consejo de la Unión Europea. (2025). *Reglamento de Inteligencia Artificial* https://www.consilium.europa.eu/es/policies/artificial-intelligence/

Contreras Machado, J. L. (2024). Toma de decisiones estratégicas en la Defensa Nacional: Un abordaje desde la Inteligencia artificial. *Revista Científica De La Escuela Superior De Guerra Del Ejército*, *3*(2), 57-70. https://doi.org/10.60029/rcesge.v3i2arti5

Cordero, D. (2024). Europa se queda sin autonomía en campos clave: "Para defender la soberanía, antes hay que tenerla". *El País.* https://elpais.com/economia/europa-se-queda-sin-autonomia-en-campos-clave-para-defender-la-soberania-antes-hay-que-tenerla

Costas Trascasas, M. (2022). La gobernanza tecnológica como nuevo paradigma de la seguridad internacional. *Revista de Estudios en Seguridad Internacional,* 8(2), 89–108. https://dialnet.unirioja.es/servlet/articulo

Council of the European Union. (2016). *Council Conclusions On Implementing The EU Global Strategy In The Area Of Security And Defence*. Foreign Affairs Council, 14149/16. https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf

Crum, D. (2024). *AI's Role in Defense – Accelerating Decision Dominance in the Next Era of Warfare.* OWL Cyber Defense. https://owlcyberdefense.com/blog/ai-role-in-defense-accelerating-decision-dominance/

Cuenca, A. (2020). El problema de Europa: la dependencia tecnológica de Estados Unidos y China. *El Orden Mundial*. https://elordenmundial.com/dependencia-tecnologica-union-europea/

Daniels, M. P. (2019). *Artificial Intelligence Research and Development*. U.S. Department of Defence. https://www.defense.gov/News/artificial-intelligence-research-and-development/

Daturex. (2024). *IA y GDPR: Los proteccionistas de datos de la UE acuerdan las normas*. https://externer-datenschutzbeauftragter-dresden.de/es/proteccion-de-datos/protectores-de-datos-de-la-ue-acuerdan-normas/

Dello Iacono, F. (2025). *Europe's Defense Shift: Strategic Autonomy In The Wake Of Trump's Return*. Instituto Analisi Relazioni Internazionali, IARI. https://iari.site/2025/02/19/europes-defense-shift-strategic-autonomy-in-the-wake-of-trumps-return/

Deloitte. (2024). Dual-Use Technology – Cross-Sector Cooperation in the Cyber Security Sector. *Third Policy Brief, Cybersec Expo & Fo- Rum,* Poland, p.6. https://cybersecforum.eu/wp-content/Dual-use-technology-cross-sector-cooperation-in-the-cyber-security-sector.pdf

DeMaio, K. (2025). *The Dehumanization of ISR: Israel's Use of Artificial Intelligence In Warfare.* Georgetown Security Studies Review. https://georgetownsecuritystudiesreview.org/2025/01/09/the-dehumanization-of-isr-israels-use-of-artificial-intelligence-in-warfare/

Diario Oficial de la Unión Europea. (2024). *Reglamento (UE) 2024/1084 Del Parlamento Europeo Y Del Consejo, Consideración nº24*. http://data.europa.eu/eli/reg/2024/1689/oj

Draghi, M. (2024). *The Future of European Competitiveness: Part B: In-depth Analysis and Recommendations*, 29-30. https://commission.europa.eu/document/

Dunning, J. H. (1992). The competitive advantage of countries and the activities of transnational corporations. https://unctad.org/system/files/official-document/

Equipo Europa. (2023). La Autonomía Estratégica de la Unión Europea: Fortaleciendo su Rol Global en un Mundo Multipolar. https://equipoeuropa.org/la-autonomia-estrategica-de-la-union-europea-fortaleciendo-su-rol-global-en-un-mundo-multipolar

El Derecho. (2024). *La regulación fragmentada hace que la UE corra el riesgo de perderse la era de la IA.* El Derecho. https://elderecho.com/la-regulacion-fragmentada-hace-que-la-ue-corra-el-riesgo-de-perderse-la-era-de-la-ia

Engler, A. (2023). *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment.* Brookings. https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/

Espinosa de los Monteros Pérez-Brotóns, S. & Sanz Setién, G. (2024). El Reglamento de IA: El Primer Paso del Camino hacia una Regulación Completa de la Inteligencia Artificial. *Actualidad Jurídica Uría Menéndez*, 65, octubre 2024, 180-196. https://www.uria.com/documentos/publicacionesAJUM-65

Espinoza, J. (2024). Europe's rushed attempt to set the rules for AI. *Financial Times*. https://www.ft.com/content/

EU Artificial Intelligence Act. (s.f.). *Cronología histórica*. EU Artificial Intelligence Act. https://artificialintelligenceact.eu/es/avances/

EU Artificial Intelligence Act. (2024a). *Annex III: High-Risk AI Systems Referred to in Article 6(2)*. https://artificialintelligenceact.eu/annex/3/

EU Artificial Intelligence Act. (2024b). *Artículo 14: Supervisión humana*. https://artificialintelligenceact.eu/es/article/14/

EU Artificial Intelligence Act. (2024c). *La Oficina de Inteligencia Artificial: ¿Qué es y cómo funciona?*. EU Artificial Intelligence Act. https://artificialintelligenceact.eu/es/the-ai-office-summary/

EU Artificial Intelligence Act. (2024d). *High-level summary of the AI Act*. https://artificialintelligenceact.eu/high-level-summary/

EU Artificial Intelligence Act. (2024e). *Article 57: AI Regulatory Sandboxes*. https://artificialintelligenceact.eu/article/57/

Euro Funding. (s.f.). Fondo Europeo de Defensa. https://euro-funding.com/es/blog/fondo-europeo-de-defensa/

Euronews. (2023). *Así es la ley de la UE para regular la IA: pionera en el mundo para proteger de los riesgos de la IA.* https://es.euronews.com/asi-es-la-ley-de-la-ue-para-regular-la-ia-pionera-en-el-mundo-para-proteger-de-los-riesgos

European Commission. (2018). *A definition of AI: main capabilities and disciplines*: *Independent High-Level Expert Group on Artificial Intelligence.* https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf

European Commission. (2025). *Joint White Paper for European Defence Readiness 2030*. JOIN (2025) 120 final, 5. https://defence-industry-space.ec.europa.eu/WhitePaper.pdf

European Commission. (s.f.-a). *IA Act: Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (s.f.-b). *European AI Office*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/ai-office

European Council. (2025). *EU defence in numbers*. https://www.consilium.europa.eu/en/policies/defence-numbers/

European Institute. (2024). *The EU AI Act: Key Impacts for the Public Sector*. EU Online Academy. https://www.eu-online-academy.org/The AI Act Key impacts for the Public Sector.pdf

European Parliament. (2022). *EU strategic autonomy 2013-2023*. European Parliamentary Research Service. https://www.europarl.europa.eu/

European Parliament. (2023). *EU AI Act: first regulation on artificial intelligence.* https://www.europarl.europa.eu/topics/en/eu-ai-act-first-regulation-on-artificial-intelligence

European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council. *Official Journal of the European Union*, 2024/1689, 1-2. https://eur-lex.europa.eu/legal-content/EN/

European Parliament. (2025). *ReArm Europe Plan/Readiness 2030*. European Parliamentary Research Service. https://www.europarl.europa.eu/EN.pdf

Feldstein, S. (2023). Evaluating Europe's push to enact AI regulations: how will this influence global norms? *Democratization*, 31(5), 1049–1066. https://doi.org/10.1080/13510347.2023.2196068

Fernández, C. B. (2023). China aprueba una regulación de la inteligencia artificial y de la inteligencia artificial generativa. *Diario La Ley*. https://diariolaley.laleynext.es/china-aprueba-una-regulacion-de-la-inteligencia-artificial-y-de-la-inteligencia-artificial-generativa

Fernández, M. (2024). El caza F-16 controlado por IA de EEUU se enfrenta a un piloto humano: así fue la primera prueba de combate. *El Español*. https://www.elespanol.com/omicrono/defensa-y-espacio/caza-f-16-controlado-ia-eeuu-enfrenta-piloto-humano-primera-prueba-combate/

Fernhout, F. & Michielsen, C. (2025). *The Current Status of the AI Act: Navigating the Future of AI Regulation in the EU.* Stibbe. https://www.stibbe.com/publications-and-insights/the-current-status-of-the-ai-act-navigating-the-future-of-ai-regulation

Fierro Rodríguez, D. (2024). La inteligencia artificial como asunto de seguridad nacional en Estados Unidos. *Diario La Ley.* https://diariolaley.laleynext.es/la-inteligencia-artificial-como-asunto-de-seguridad-nacional-en-estados-unidos

France 24. (2025). *Trump's call for AI deregulation gets strong backing from Big Tech*. https://www.france24.com/en/trump-s-call-for-ai-deregulation-gets-strong-backing-from-big-tech

Freedman, L. (2017). The Meaning Of Strategy: Part I:The Origin Story. *Texas National Security Review*, 1, 1. https://doi.org/10.15781/T2WH2DX5J

Fritz, J. & Giardini, T. (2024). *Why Global Coordination is Necessary for Regulating AI.* Promarket. https://www.promarket.org/2024/09/11/why-global-coordination-is-necessary-for-regulating-ai/

Fuest, C., Gros, D., Mengel, P. L., Presidente, G. & Tirole, J. (2024). *EU Innovation Policy: How To Escape The Middle Technology.* European Policy Analysis Group. https://www.econpol.eu/sites/Report EU Innovation Policy.pdf

García, E.V. (2021). *Killed by algorithms: Do autonomous weapons reduce risks?.* Beyond the Horizons. https://behorizon.org/killed-by-algorithms-do-autonomous-weapons-reduce-risks/

García Paudo, D. (2025). DeepSeek: EEUU innova, China copia y Europa regula. *El Economista*. https://www.eleconomista.es/opinion/deepseek-eeuu-innova-china-copia-y-europa-regula.html

Garrigues. (2023). *Así está regulando la IA la UE, EE.UU. y la OCDE.* https://www.garrigues.com/es_ES/garrigues-digital/asi-esta-regulando-ia-ue-eeuu-ocde-dificil-equilibrio-seguridad-fomento

Gehrke, T. (2025). *Brussels hold'em: European cards against Trumpian coercion.* European Council on Foreign Relations. https://ecfr.eu/publication/brussels-holdem-european-cards-against-trumpian-coercion/

Gigova, R. (2017). Who Vladimir Putin thinks will rule the world. *CNN.* https://edition.cnn.com/world/putin-artificial-intelligence-will-rule-world

Gill, J. (2022). Say goodbye to JAIC and DDS, as offices cease to exist as independent bodies June 1. *Breaking Defense.* https://breakingdefense.com/2022/05/say-goodbye-to-jaic-and-dds-as-offices-cease-to-exist-as-independent-bodies-june-1/

Giordano, M., Hieronimus, S., Smit, S., de la Chevasnerie, M. A., Mischke, J., Koulouridi, E., Dagorret, G. & Brunetti, N. (2024). *Accelerating Europe: Competitiveness for a new era*. McKinsey Global Institute. https://www.mckinsey.com/mgi/our-research/accelerating-europe-competitiveness-for-a-new-era

González, I. (2021). Los cazas sin piloto, más cerca: así es Skyborg, el santo grial del pilotaje autónomo, *El Español*, tecnología. https://www.elespanol.com/omicrono/tecnologia/cazas-sin-piloto-cerca-skyborg-pilotaje-autonomo/

González, M. (2024). Cuando el gatillo lo dispara un algoritmo. *El País*. https://elpais.com/tecnologia/branded/inteligencia-artificial/cuando-el-gatillo-lo-dispara-un-algoritmo

Goud, S., Kaul, H., Chinnegowda H. (2024). The Rise of AI and Autonomous Systems: Transforming Industries and Navigating Ethical Challenges. *International Journal for Research in Applied*

Science & Engineering Technology (IJRASET) ISSN: 2321-9653, 12, 2. https://www.ijraset.com/best-journal/the-rise-of-ai-and-autonomous-systems-transforming-industries-and-navigating-ethical-challenges

Gray, C.S., (1999). *Modern Strategy*. Oxford University Press, 17. https://www.uni-frankfurt.de/Modern_Strategy

Gray, M. & Ertan, A. (2021). *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*. NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), 17. https://ccdcoe.org/Strategies_and_Deployment_A4.pdf

Greenacre, M. (2025). EIC will invest in dual-use start-ups, Commission says. *Science Business*. https://sciencebusiness.net/news/european-innovation-council/eic-will-invest-dual-use-start-ups-commission-says

Greene, N. (2024). The EU AI Act could hurt military innovation in Europe. *Center for a New American Security*. https://www.cnas.org/publications/commentary/the-eu-ai-act-could-hurt-military-innovation-in-europe

Guerra Huapalla, G. M. (2023). Inteligencia artificial en la carrera de las potencias: desafíos y oportunidades para el equilibrio de poder internacional. *Política Internacional*, (134), 94–112, 6. https://doi.org/10.61249/pi.vi134.92

Hadjiyianni, I. (2021). The European Union as a Global Regulatory Power. *Oxford Journal of Legal Studies*, 41, 1, 243–264. https://doi.org/10.1093/ojls/gqaa042

Haeck, P. (2025). EU opens door to reworking AI rulebook. *Politico*. https://www.politico.eu/article/how-eu-did-full-180-artificial-intelligence-rules/

Hernández, N. (2024). Europa a punto de perder la carrera de los chips: la inacción de Bruselas nos deja vendidos ante China y Estados Unidos. *El Español*. https://www.elespanol.com/invertia/disruptores/politica-digital/europa/europa-punto-perder-carrera-chips-inaccion-bruselas-deja-vendidos-china-unidos/

Hierro, L. (2025). La guerra cibernética entre Ucrania y Rusia se intensifica en paralelo al conflicto militar, *El País*. https://elpais.com/internacional/la-guerra-cibernetica-entre-ucrania-y-rusia-se-intensifica-en-paralelo-al-conflicto-militar

Human Rights Watch. (2020). Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control. *Human Rights Watch*. https://www.hrw.org/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

Humble, K. (2024). War, Artificial Intelligence, and the Future of Conflict. *Georgetown Journal of International Affairs*. https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/

Hyeon Choi, S. (2025). EU defence white paper says China's military action risks 'major disruption' for Europe. *South China Morning Post*. https://www.scmp.com/news/china/eu-defence-white-paper-says-chinas-military-action-risks-major-disruption-europe

ICEX. (2024). *La Inteligencia Artificial (IA) en Estados Unidos.* Oficina Económica y Comercial de la Embajada de España en Chicago, 37. https://www.icex.es/content/OD_Inteligencia Artificial en Estados Unidos.pdf

Imprivata. (s.f.). *The 6 principles of AI and data protection: how the AI act ensures data is safe.* https://www.imprivata.com/sites/Whitepaper-6-AI-Principles_Allison Schuh.pdf

Instituto Español de Estudios Estratégicos. (2024). *La inteligencia artificial en la geopolítica y los conflictos*. Cuadernos de Estrategias 226. ISBN 978-84-9091-933-0. https://publicaciones.defensa.gob.es/media/downloadable/files/links/l/a/la_inteligencia_artificial_en_la_geopol_tica_y_los_conflictos_ce_226.pdf

Insinna, V. (2023). Inside the special F-16 the Air Force is using to test out AI. *Breaking Defense*. https://breakingdefense.com/2023/01/inside-the-special-f-16-the-air-force-is-using-to-test-out-ai/

Insinna, V. (2024). SAC passes $852B defense bill, adding $21B and teeing up budget fight. *Breaking Defense*. https://breakingdefense.com/2024/08/sac-passes-852b-defense-bill-breaking-budget-caps-and-teeing-up-budget-fight/

Innobasque. (2024). *Europa y Estados Unidos: una brecha de competitividad que exige transformación*. https://www.innobasque.eus/tendencias/europa-y-estados-unidos-una-brecha-de-competitividad-que-exige-transformacion/

Imbalzano, G. (2025). *Eu's AI Dilemma: Balancing Regulation, Competitiveness, and Global Pressures*. IARI, Instituto Analisi Relazioni Internazionali. https://iari.site/2025/03/07/eus-ai-dilemma-balancing-regulation-competitiveness-and-global-pressures/

Ilaria, C., Marsh, N. & Reichberg, G. M. (2022). Dual-Use AI Technology in China, the US and the EU: Strategic Implications for the Balance of Power. *PRIO Paper*. https://www.nb.no/

Kania, E. B. (2019). *Chinese Military Innovation in Artificial Intelligence*. CNAS. https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence

Kennedy, M. (2025). *A Strategic Vision for US AI Leadership: Supporting Security, Innovation, Democracy and Global Prosperity*. Wilson Center. https://www.wilsoncenter.org/article/strategic-vision-us-ai-leadership-supporting-security-innovation-democracy-and-global

Keslassy, E. (2025). OpenAI and Other Tech Companies Battle Transparency Obligation in Europe's AI Act as Creatives Push Back: 'We Know You're Harvesting Us'. *Variety*. https://variety.com/2025/digital/global/ai-companies-battle-europe-ai-act-creatives-push-back

Klaus, M. (2024). *Transcending weapon systems: the ethical challenges of AI in military decision support systems.* Humanitarian Law & Policy. https://blogs.icrc.org/app/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems

Konopczyński, F. (2023). *One Act to Rule Them All.* Verfassungsblog. https://verfassungsblog.de/one-act-to-rule-them-all/

Kowalski, B. (2025). *The AI dual-use dilemma using the example of China*. Allegro Blog Tech. https://blog.allegro.tech/2025/02/the-ai-dual-use-dilemma-using-the-example-of-china.html

KPMG. (s.f.). *The rising importance of AI regulation.* KPMG Switzerland. https://kpmg.com/ch/en/insights/artificial-intelligence/eu-ai-act.html

Krauss, J. (2024). *Tapping the United States' greatest weapon: innovation*. JP Morgan. https://www.jpmorgan.com/insights/investing/investment-trends/defense-tech-innovation-and-the-role-of-startups

Kumayama, K. D., Levi, S. D. &Ridgway, W. E. (2025). *US Federal Regulation of AI is likely to be lighter, but States may fill the void.* Skadden. https://www.skadden.com/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter

Lacort, J. (2025). *China tiene un ambicioso plan para superar a Occidente en tecnología. Y ya ha elegido a sus 18 empresas para conseguirlo*. Xataka. https://www.xataka.com/empresas-y-economia/quien-quien-nueva-china-tecnologica-estas-18-empresas-que-xi-jinping-ha-elegido-para-competir-occidente

Lamela Gallego, M. (s.f.). La revitalización de la defensa europea: PESCO. *Universidad de Navarra, Global Affairs*. https://www.unav.edu/web/global-affairs/detalle/-/blogs/la-revitalizacion-de-la-defensa-europea-pesco

Lannquist, Y., Loke, J., Miailhe, N., Hodes, C. & Yampolskiy, R. (2020). *The Intersection and Governance of Artificial Intelligence and Cybersecurity.* https://www.researchgate.net/The_Intersection_and_Governance_of_Artificial_Intelligence_and_Cybersecurity

La Spina, E. (2024). La regulación europea de la IA ante los sesgos y riesgos de discriminación algorítmica en contextos migratorios. *Revista CIDOB d'Afers Internacionals,* 138, 171-194. https://www.cidob.org/sites/

Las Heras, P. (2023). *El reto de la inteligencia artificial para la seguridad y defensa*. Global Affairs. Universidad de Navarra. https://www.unav.edu/en-GB/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa

Lawrenson, T. & Sabatino, E. (2024). *The Impact of the European Defence Fund on Cooperation with Third-country Entities.* IISS. https://www.iiss.org/research-paper/2024/10/the-impact-of-the-european-defence-fund-on-cooperation-with-third-country-entities/

Lebrun, B. & Lachguer, W. (2025). *The EU AI Act and National AI Standards: Risk of Fragmentation of the Internal Market.* Chambers & Partners. https://chambers.com/legal-trends/eu-ai-acts-goals

Lee Harpley, U. (2024). *Senate Committee Adds More Fighters, Boosts USAF and USSF Budget*. Air & Space Forces. https://www.airandspaceforces.com/senate-fighters-usaf-ussf-budget/

Lei, Z. (2025). Proposed defense budget calls for 7.2 percent rise in spending. *China Daily*. https://www.chinadaily.com.cn/

Leon Coronado, C. (2023). La carrera por la regulación de la inteligencia artificial. *Revista Latinoamericana de Economía y Sociedad Digital*, 4, 7. https://doi.org/10.53857/RLESD.04.2023.05/

León Serrano, G. (2023). El papel dual de la inteligencia artificial en una era de conflictos híbridos. *Academia de las Ciencias y las Artes Militares Sección Prospectiva de la Tecnología Militar*, 6. https://www.acami.es/wp-content/uploads/2023/12/El-papel-dual-de-la-inteligencia-artificial-web.pdf

Liang, X. (2025). *Defense Policy Bill Sets Stage for Nuclear Expansion*. Arms Control Association. https://www.armscontrol.org/act/2025-01/news/defense-policy-bill-sets-stage-nuclear-expansion

López Vicente, P. (2009). Tecnologías Disruptivas. Mirando el futuro Tecnológico. *En Boletín de Observación Tecnológica en Defensa* no 25, 16-19. https://www.tecnologiaeinnovacion.defensa.gob.es/

Lorenzo de Olmos, A. (s.f.). *El movimiento Pan Europeo*. Córdoba Global. https://cbaglobal.com.ar/el-movimiento-pan-europeo/

Lovett, L. (2025). Los drones cambian la dinámica de la guerra en Myanmar. *El País*. https://elpais.com/planeta-futuro/los-drones-cambian-la-dinamica-de-la-guerra-en-myanmar

Lübken, J. (2024). The EU's Artificial Intelligence Act: A golden opportunity for global AI regulation. *European Leadership Network, ELN.* https://europeanleadershipnetwork.org/commentary/the-eus-artificial-intelligence-act-a-golden-opportunity-for-global-ai-regulation/

Madariaga, B. (2024). Unión Europea, Estados Unidos y China: tres modelos diferentes de regulación de la IA. *Director TIC*. https://directortic.es/estrategia-it/union-europea-estados-unidos-y-china-tres-modelos-diferentes-de-regulacion-de-la-ia

Maharani Hasnadim, D. (2024). *Doubting a "Brussels Effect 2.0": Can the European Union's AI Act Foster Legitimacy?.* Modern Diplomacy. https://moderndiplomacy.eu/2024/12/24/doubting-a-brussels-effect-2-0-can-the-european-unions-ai-act-foster-legitimacy/

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms?. *Journal of Common Market Studies*, 40, 2, 235-58. https://www.princeton.edu/~amoravcs/library/mannersnormativepower.pdf

Maremonti, F. (2024). *The G7 and AI Governance: Towards a Deeper and Broader Agenda*. Istituto Affari Internazionali (IAI). http://www.jstor.org/stable/resrep65207

Marks, D. S. & Trivedi, S. (2025). *European Union Artificial Intelligence Act: An Overview*. Benesch. https://www.beneschlaw.com/resources/european-union-artificial-intelligence-act-an-overview-part-2.html

Martens, B. (2024). *Catch-up with the US or prosper below the tech frontier? An EU artificial intelligence strategy.* Bruegel. https://www.bruegel.org/policy-brief/catch-us-or-prosper-below-tech-frontier-eu-artificial-intelligence-strategy

Martí Sempere, C. (2024). Estrategias industriales de defensa y tecnologías duales. *Real Instituto El Cano*, ARI 137/2024, 3. https://media.realinstitutoelcano.org/wp-content/uploads/-martisempere-estrategias-industriales-de-defensa-y-tecnologias-duales

McKinsey & Company. (2025a). *European defense tech start-ups: In it for the long run?*. McKinsey & Company, Aerospace & Defence. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-tech-start-ups-in-it-for-the-long-run

McKinsey & Company. (2025b). *Shaping resilience: Defend. Secure. Innovate*. McKinsey & Company, Aerospace & Defence Practice. https://www.mckinsey.com/~/media/mckinsey/industries/aerospace and defense/

Mikhailov, D. I. (2023). *Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration.* IEEE. https://arxiv.org/abs/2305.13927

Moliner González, J. A. (2019). *Desafíos éticos en el uso militar de la inteligencia artificial.* La inteligencia artificial, aplicada a la defensa, 127-152. https://dialnet.unirioja.es/descarga/libro/731297.pdf

Monaghan, S. (2023). *Solving Europe's Defense Dilemma*. CSIS. https://csis-website-Monaghan_Defense_Dilemma

Moscoso del Prado, J. (2025*). Combine to survive: The European defence sector on the threshold.* European Council on Foreign Relations. https://ecfr.eu/article/combine-to-survive-the-european-defence-sector-on-the-threshold/

Mundell, I. (2023). The Ecosystem: sprawling AI Act may deprive European start-ups of investment. *Science Business*. https://sciencebusiness.net/news/ecosystem-sprawling-ai-act-may-deprive-european-start-ups-investment -

Nadibaidze, A. (2023). *'Responsible AI' in the Military Domain: Implications for Regulation.* Opinio Juris. http://opiniojuris.org/2023/03/31/responsible-ai-in-the-military-domain-implications-for-regulation/

Neenan, A. G. & Sayler, K. M. (2023). *The AI Executive Order and Its Potential Implications for DOD.* Congressional Research Service. https://www.congress.gov/crs-product/IN12286

Observatorio de Inteligencia Artificial. (2025). *Reino Unido y EE. UU. alinean sus regulaciones de IA*. https://observatorio-ia.com/reino-unido-y-ee-uu-alinean-sus-regulaciones-de-ia

O'Brien, M. (2024). *EEUU encabeza innovación de IA, superando ampliamente a China en nuevo ranking de Stanford. Independent.* https://www.independentespanol.com/tecnologia/eeuu-encabeza-innovacion-de-ia-superando-ampliamente-a-china-en-nuevo-ranking-de-stanford

O'Donnell, J. (2024). *La IA llega al campo de batalla para redefinir la toma de decisiones en la guerra moderna.* MIT Technology Review. https://technologyreview.es/article/la-ia-llega-al-campo-de-batalla-para-redefinir-la-toma-de-decisiones-en-la-guerra-moderna/

OECD. (2024). *Artificial intelligence.* OECD Policy Issue. https://www.oecd.org/en/topics/artificial-intelligence.html#context

Organización Internacional del Trabajo. (2020). *Impulsando la Productividad.* https://www.ilo.org/sites/default/

Otero Iglesias, M. (2024). *En busca de una ventaja competitiva: la reforma del marco reglamentario de la UE*. Real Instituto El Cano. https://www.realinstitutoelcano.org/documento-de-trabajo/en-busca-de-una-ventaja-competitiva-la-reforma-del-marco-reglamentario-de-la-ue/

Palmas, A. & Andronico, P. (2022). *Deep Learning Computer Vision Algorithms for Real-time UAVs On-board Camera Image Processing*. NATO AVT-353 Research Workshop "Artificial Intelligence in Cockpits for UAVs". https://doi.org/10.48550/arXiv.2211.01037

Paniagua, E. (2023). Cinco retos de la ley de IA. *El Español*. https://www.elespanol.com/disruptores-innovadores/retos-ley-ia/

Parker, L. (2020). *The American AI Initiative: The U.S. strategy for leadership in artificial intelligence*. OECD AI, Policy Observatory. https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-rtificial-intelligence

Parkin, S. (2015). Killer robots: The soldiers that never sleep. *BBC.* https://www.bbc.com/future/article/20150715-killer-robots-the-soldiers-that-never-sleep

Parlamento Europeo. (s.f.). *Una Agenda Digital para Europa*. Fichas temáticas sobre la Unión Europea. https://www.europarl.europa.eu/factsheets/es/sheet/64/una-agenda-digital-para-europa

Parolari, M. N. (2025). ¿Un cambio que sacudirá la tecnología? Lo que se trama tras los aranceles a los chips propuestos por Trump. *Diario Gizmodo*. https://es.gizmodo.com/un-cambio-que-sacudira-la-tecnologia-lo-que-se-trama-tras-los-aranceles-a-los-chips-propuestos-por-trump

Perotto, G. (2023). The Legal Framework of the EU Defence Industry and the Pursuit of Strategic Autonomy. *European Papers*, 8, 1, 475-486. DOI: 10.15166/2499-8249/668

Pernot-Leplay, E. (2024). *The AI Dilemma: AI Regulation In China, EU & The U.S.* Emmanuel Pernot-Leplay, Global AI & Tech Policies. https://pernot-leplay.com/ai-regulation-china-eu-us-comparison/

Politico. (2024). *Europe jumps into 'incredibly costly' AI supercomputing race.* https://www.politico.eu/article/europe-costly-artificial-intelligence-race-supercomputer-startups/

Pompeo, M. R. (s.f.). *The Chinese Communist Party's Military-Civil Fusion Policy. U.S. Department of State*. https://2017-2021.state.gov/military-civil-fusion/

Porter, M. E. (1990). The Competitive Advantage of Nations. *Havard Business Review*. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Porter, M. E. (2004). *Ser competitivo: Estrategias, tácticas y tecnologías para la competencia*. Ediciones Deusto. https://proassetspdlcom.com/libros_contenido/arxius/Ser_competitivo.pdf

Powell, R. (August 2024). *The EU AI Act: National Security Implications*. CETaS Explainers. https://cetas.turing.ac.uk/the_eu_ai_act_national_security_implications.pdf

Prensa EC. (2025). *La estrategia de Trump en el comercio global: ¿Un nuevo orden económico en formación?* https://prensa.ec/la-estrategia-de-trump-en-el-comercio-global-un-nuevo-orden-economico-en-formacion/

Pugnet, A. & Kölsch, D. (2025). Europe's new military paradigm – going solo without US backup. *Euractiv*. https://www.euractiv.com/section/defence/news/europes-new-military-paradigm-going-solo-without-us-backup/

Quarles Van Ufford, H. (2025). Regulate or stagnate: Why the EU must lead on AI. *Euractiv*. https://ecfr.eu/article/regulate-or-stagnate-why-the-eu-must-lead-on-ai/

Quintero Morales, G., & Salas Galindo, O. L. (2023). Aplicaciones de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa nacional. *Revista Ciberespacio, Tecnología e Innovación*, 2(3), 57-80. https://doi.org/10.25062/2955-0270.4772

Rauer, N. (2024). *A guide to high-risk AI systems under the EU AI Act.* Pinsent Masons. https://www.pinsentmasons.com/guides/guide-to-high-risk-ai-systems-under-the-eu-ai-act

Renda, A. (2019). Artificial Intelligence: Ethics, Governance and Policy Challenges. *CEPS Task Force Report*, ISBN 978-94-6138-716-5, 43-47. https://ssrn.com/abstract=3420810

Rengel, C. (2025). Claves del Libro Blanco de la Defensa UE: dinero de todos para un rearme forzado por la amenaza rusa. *El Huff Post*. https://www.huffingtonpost.es/global/claves-libro-blanco-defensa-ue-dinero-todos-rearme-forzado-amenaza-rusa.html

Ricart, R. J. (2024). El reto digital de la Unión Europea. *Política Exterior,* 220. https://www.politicaexterior.com/articulo/el-reto-digital-de-la-union-europea/

Riquelme, R. (2023). Países aceleran regulación de Inteligencia Artificial y México es uno de ellos. *El Economista*. https://www.eleconomista.com.mx/tecnologia/Paises-aceleran-regulacion-de-Inteligencia-Artificial-y-Mexico-es-uno-de-ellos

Rincón Andreu, G. (2021). Libro Blanco de la Comisión Europea sobre Inteligencia Artificial. Un enfoque europeo hacia la excelencia y la confianza. *Ius et Praxis*, 27(1), 264-270, 264. https://dx.doi.org/10.4067/S0718-00122021000100264

Rizzi, A. (2025). Trump pide a los países de la OTAN que eleven su gasto en defensa al 5% del PIB y acusa a la UE de tratar "muy mal" a EE UU. *El País*. https://elpais.com/trump-pide-a-los-paises-de-la-otan-que-eleven-su-gasto-en-defensa-y-acusa-a-la-ue-de-tratar-muy-mal-a-ee-uu

Roberts, O. (2025). *EU AI Act's Burdensome Regulations Could Impair AI Innovation.* Bloomberg Law. https://news.bloomberglaw.com/us-law-week/eu-ai-acts-burdensome-regulations-could-impair-ai-innovation

Rodríguez, H. (2025). *La ONU alerta sobre la desigualdad en IA y propone regulación global.* La Ecuación Digital. https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/la-onu-alerta-sobre-la-desigualdad-en-ia-y-propone-regulacion-global/

Rodríguez Parrondo, J. (2024). Europa busca liderar la regulación de la inteligencia artificial. *Cinco Días*. https://cincodias.elpais.com/europa-busca-liderar-la-regulacion-de-la-inteligencia-artificial

Ruitenberg, R. (2025). EU pitches plan to free up €800 billion for defense spending. *Defense News.* https://www.defensenews.com/eu-pitches-plan-to-free-up-800-billion-for-defense-spending/

Russell, S., Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*. ISBN -10 0134610997. https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

Sabbagh, D. (2025). US no longer 'primarily focused' on Europe's security, says Pete Hegseth. *The Guardian.* https://www.theguardian.com/us-news/2025/feb/12/us-no-longer-primarily-focused-on-europes-security-says-pete-hegseth

Sahbaz, U. (2025). *Europe's defense spending should focus on innovation.* TechEU. https://tech.eu/2025/03/05/europes-defense-spending-should-focus-on-innovation/

Schwab, K. (2016). The Global Competitiveness Report 2016–2017. *World Economic Forum*, 4. https://www3.weforum.org/docs/TheGlobalCompetitivenessReport

Schechner, S. & Meichtry, S. (2025). Vance Warns U.S. Allies to Keep AI Regulation Light. *The Wall Street Journal. https://www.wsj.com/tech/ai/vance-warns-u-s-allies-to-keep-ai-regulation-light*

Schmitt, M. (2023). *Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection*. arXiv:2401.01342

Schulenburg, R. (2025). *Reinforcement and redistribution: evolving US posture in the Indo-Pacific*. IISS. https://www.iiss.org/online-analysis/military-balance/2025/03/reinforcement-and-redistribution-evolving-us-posture-in-the-indo-pacific/

Segura, C. (2023). La guerra en Ucrania revoluciona el uso de los drones civiles como arma para matar. *El País.* https://elpais.com/la-guerra-en-ucrania-revoluciona-el-uso-de-los-drones-civiles-como-arma-para-matar

Sekine, T. (2024). EU's AI Regulation and International Economic Law: The Complex Impact of the EU AI Act on Global Economic Governance. *SSU Working Paper*, University of Tokyo, http://dx.doi.org/10.2139/ssrn.4997043

Senter, D. & Bruton, H. (2025). The Future of AI Compliance—Preparing for New Global and State Laws. *Smith Anderson*. https://www.smithlaw.com/printpilot-publication-the-future-of-ai-compliance-preparing-for-new-global-and-state-laws

Soete, L. (2025). How to break Europe's innovation stasis. *Social Europe*. https://www.socialeurope.eu/how-to-break-europes-innovation-stasis

Sohail, K. (2024). *The Military-Civil Fusion Strategy of the Chinese Communist Party & the Concerned America.* Paradigm Shift. https://www.paradigmshift.com.pk/military-civil-fusion/

Šonková, M. (2024). Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act. College of Europe. *EU Diplomacy Papers,* 4/2024. https://www.coleurope.eu/Sonkova

Spasov, S. (2023). The power of pragmatism: Nuclear energy, technological innovation, and the green transition. *Euractiv*. https://ecfr.eu/article/the-power-of-pragmatism-nuclear-energy-technological-innovation-and-the-green-transition/

Stannard, A., Agius, P. & Szewczyk, B. (2025). *What Does the New European Commission Mean for EU Tech Policy?*. Global Policy Watch. https://www.globalpolicywatch.com/what-does-the-new-european-commission-mean-for-eu-tech-policy/

Statista. (2025). *Chart: ReArm Europe: The EU's €800-Billion Defense Plan*. https://www.statista.com/chart/34051/eu-plan-to-boost-defense-spending/

Stockholm International Peace Research Institute. (2019). The Impact Of Artificial Intelligence On Strategic Stability And Nuclear Risk. *Euro-Atlantic Perspectives*, I. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf

Stone, P. (2020). La estrategia política en IA en los Estados Unidos. *Revista Idees*. https://revistaidees.cat/es/un-resum-de-lestrategia-politica-en-ia-als-eua/

Takagi, K. (2022). *New Tech, New Concepts: China's Plans for AI and Cognitive Warfare*. War on the Rocks. https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/

The Central People's Government of China. (2025). *China to increase defense budget by 7.2 percent in 2025*. https://english.www.gov.cn/news/202503/05/content_WS67c7ba5dc6d0868f4e8f05cf.html

The White House. (2019). *Maintaining American leadership in artificial intelligence.* Federal Register. https://www.federalregister.gov/maintaining-american-leadership-in-artificial-intelligence

Tidey, A. (2025). La UE quiere aumentar su capacidad de Defensa: necesita invertir 500.000 millones. *Euronews*. https://es.euronews.com/my-europe/2025/02/04/los-lideres-de-la-ue-debaten-sobre-el-gasto-comun-en-defensa

Torres Jarrín, M. (2021). La UE & la gobernanza ética de la inteligencia artificial. *Cuadernos salmantinos de filosofía*, ISSN 0210-4857, 48, 213-234. https://summa.upsa.es/

Torreblanca, J.I. & Verdi, G. (2024). Control-Alt-Distribuir: Una gran estrategia digital para la Unión Europea. *European Council on Foreign Relations*. https://ecfr.eu/no/publication/control-alt-distribuir-una-gran-estrategia-digital-para-la-union-europea/

Tovar, M. (2025). China le está ganando a EEUU la primera guerra por la IA armamentística con una fecha en mente para el cambio de paradigma. *Diario AS*. https://as.com/china-le-esta-ganando-a-eeuu-la-primera-guerra-por-la-ia-armamentistica-con-una-fecha-en-mente-para-el-cambio-de-paradigma-n/

Tucker, P. (2024). *Can OpenAI power military drone defenses? New partnership with Anduril offers clues.* Defence One. https://www.defenseone.com/business/2024/12/can-openai-power-military-drone-defenses-new-partnership-anduril-offers-clues/401446/

Tuma, P. (2025). *The EU just released a roadmap to defend Europe. Will member states follow it?*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-eu-just-released-a-roadmap-to-defend-europe-will-member-states-follow-it/

Tuset Varela, D. (2024). La fragmentación del derecho de la Inteligencia Artificial: análisis crítico de un reto normativo global. *Diario La Ley*. https://diariolaley.laley/la-fragmentacion-del-derecho-de-la-inteligencia-artificial-analisis-critico-de-un-reto-normativo-global

U.S. Department of Defence. (2022). *National Defence Strategy of the United States of America*. https://media.defense.gov/2022/Oct/NATIONAL-DEFENSE-STRATEGY.pdf

U.S. Senate Committee on Appropriations. (2025). *BILL SUMMARY: Defense Fiscal Year 2025 Appropriations Bill.* https://www.appropriations.senate.gov/news/majority/bill-summary-defense-fiscal-year-2025-appropriations-bill

Van Oirsouw, T. (2024). *AI, Digital Sovereignty, and the EU's Path Forward: A Case for Mission-Oriented Industrial Policy.* Harvard Kennedy School, ASH Center for Democratic Governance and Innovation. https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/

Variengien, A. & Martinet, C. (2024). *AI Safety Institutes: Can countries meet the challenge?*. OECD Policy Observatory. https://oecd.ai/en/wonk/ai-safety-institutes-challenge

Vereckey, B. (2023). *Does regulation hurt innovation? This study says yes*. MIT Sloan School. https://mitsloan.mit.edu/ideas-made-to-matter/does-regulation-hurt-innovation-study-says-yes

Vogiatzoglou, P. (2024). *The AI Act National Security Exception.* Verfassungsblog. https://verfassungsblog.de/the-ai-act-national-security-exception/

Von Clausewitz, C. (1989). *On War*. Princeton University Press, 25. https://www.usmcu.edu/

White & Case. (2025a). *AI Watch: Global regulatory tracker - European Union*. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union

White & Case. (2025b). *AI Watch: Global regulatory tracker - United States*. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

White & Case. (2025c). *AI Watch: Global regulatory tracker – China*. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china

Whittaker, T. (2023). *EU AI Act: how will startups be impacted?* Burges Salmon. https://www.burges-salmon.com/articles/102i4ct/eu-ai-act-how-will-startups-be-impacted/

Wolford, B. (s.f.). *What is GDPR, the EU's new data protection law?*. GDPR, European Union. https://gdpr.eu/what-is-gdpr/

World Economic Forum. (2025). *Technology convergence is leading the way for the fifth industrial revolution*. World Economic Forum Annual Meeting. https://www.weforum.org/stories/2025/01/technology-convergence-is-leading-the-way-for-accelerated-innovation-in-emerging-technology-areas/

Wu, W. & Liu, S. (2023). *A Comprehensive Review and Systematic Analysis of Artificial Intelligence Regulation Policies*. https://arxiv.org/pdf/2307.12218

Yaros, O., Kourinian, A., Hadnes Bruder, A., Randall, R., Hajda, O., Hepworth, E. & Maher, A. (2025). *EU AI Act: Ban on Certain AI Practices and Requirements for AI Literacy come into Effect.* Mayer Brown. https://onenorth.com/pdfrenderer.svc

Yordanova, K. (2022). The EU AI Act – Balancing Human Rights and Innovation Through Regulatory Sandboxes and Standardization. *Competition Policy International*. https://www.competitionpolicyinternational.com/The-EU-AI-Act-Balancing-Human-Rights-and-Innovation-Through-Regulatory-Sandboxes-and-Standardization-Katerina-Yordanova

Zachová, A. (2023). Companies switching from Europe to US amid high energy costs. *Euractiv.* https://www.euractiv.com/section/politics/news/companies-switching-from-europe-to-us-amid-high-energy-costs/

Zamorin, V. A. (2023). Contribution of the Chinese Military-Industrial Complex to the "Made in China 2025" State Plan. *Far Eastern Affairs*, 51, 2, 130-152 https://dx.doi.org/10.21557/FEA.86159334