

Regulatory impact on the application of Artificial Intelligence in Defence and Security

Abstract:

Artificial Intelligence (AI) is increasingly being used in defence and security, improving military strategies and operations. However, these advances also generate ethical and legal challenges regarding the privacy of the data with which these systems are trained or other issues such as biases, their autonomy and the fact that they can also be vulnerable to manipulation and attacks. This is why it is necessary to establish a regulation that guarantees the appropriate use of AI in the military environment, does not violate any fundamental rights and is safe.

Keywords:

AI, defence and security, legislation, regulation, Europe.

Cómo citar este documento:

TALAVERA RODRÍGUEZ, Emma. *Impacto de la regulación en la aplicación de Inteligencia Artificial en Defensa y Seguridad*. Documento de Opinión IEEE 70/2025. [enlace web IEEE](#) y/o [enlace bie³](#) (consultado día/mes/año).

Introducción

La Inteligencia Artificial (IA en adelante) es una herramienta tecnológica que está transformando el mundo en el que vivimos. Su rápido avance y la cantidad de datos de los que se dispone para entrenar a estos sistemas tiene un gran impacto en diferentes áreas de nuestra realidad, tanto en la parte civil como en la militar¹.

Debido a la gran capacidad y alcance que tiene, se están llevando a cabo nuevos desarrollos relacionados con vehículos autónomos, diagnósticos médicos y actividades de seguridad automatizadas, entre otros, al igual que nuevas formas de empleo en el ámbito militar². La aplicación de la IA en esta última área puede proporcionar ayuda a los comandantes para la toma de decisiones en las operaciones y estrategias militares, así como para poder anticiparse y gestionar las amenazas con la mayor inmediatez³. Un ejemplo de la influencia que está teniendo la IA en el uso militar es la Guerra de Ucrania, ya que se han estado utilizando drones y tecnologías avanzadas basadas en IA para detener el avance ruso y contraatacar⁴.

A pesar de que la IA, como se ha visto, impulsa la innovación y puede mejorar la calidad de vida del ser humano, trae consigo desafíos legales y éticos, como puede ser el sesgo o la vulneración de la privacidad⁵. Su implementación y uso debe ser responsable y garantizar el cumplimiento de los derechos fundamentales.

Se han establecido normativas, principios y códigos éticos que hacen referencia a la IA, pero la evolución de esta tecnología es más rápida que el desarrollo de la legislación y

¹ AI Task Force. (2019). *ARTIFICIAL INTELLIGENCE IN SUPPORT OF DEFENCE*. París: Ministère des Armées. Obtenido de <https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf>

² Olier, E., & Corchado, J. (2022). *Inteligencia Artificial: aplicaciones a la Defensa*. Madrid: IEEE, CESEDEN. Obtenido de https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEINV01_2022_EDUOLI_Inteligencia.pdf

³ Bossio Ballesteros, V. (26 de Octubre de 2023). *La Inteligencia Artificial en el Ámbito Militar: Una Herramienta Relevante y Útil*. Obtenido de CEEEP: <https://ceeep.mil.pe/2023/10/26/la-inteligencia-artificial-en-el-ambito-militar-una-herramienta-relevante-y-util/#post-23413-endnote-3>

⁴ Santayana, J. P. (2024). La inteligencia artificial y la guerra de Ucrania. En J. P. Santayana, *Cuaderno de estrategia 226. La inteligencia artificial en la geopolítica y los conflictos* (págs. 87-103). Madrid: IEEE - CESEDEN. Obtenido de <https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226>

⁵ Lisi, M. (2024). La IA en el espacio: un catalizador para los cambios. En M. Lisi, *Cuaderno de Estrategia 226. 'La inteligencia artificial en la geopolítica y los conflictos'* (págs. 189-217). Madrid: IEEE, CESEDEN. Obtenido de <https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226>

queda mucho por recorrer en este aspecto. Es importante mencionar lo que indica el documento “Visión de la Inteligencia Artificial en las FAS”⁶ del Ministerio de Defensa sobre las operaciones militares:

Aunque existen diversas iniciativas en marcha para certificar el uso de la IA en operaciones militares, actualmente no se dispone de legislación específica al respecto.

A su vez, para que se autorice el empleo de un sistema de IA en las operaciones militares, éste debe ser confiable y previsible, de forma que siempre se mantenga el control sobre su resultado.

Este artículo analiza la necesidad de una regulación genérica a nivel internacional de la IA, especialmente en el ámbito militar. Es una herramienta que, además de facilitar la innovación y proporcionar grandes avances para la defensa, presenta riesgos como la privacidad y el funcionamiento autónomo en armas, lo que evidencia la relevancia de una regulación adecuada.

Para la elaboración de los siguientes apartados, se ha hecho una investigación del marco normativo actual sobre la IA, identificando en qué normas se hace mención a la defensa y seguridad y en cuáles no. También se ha estudiado cómo se pueden aplicar en este campo, junto con qué necesidades no están cubiertas.

Marco normativo

España

A continuación, se describen dos estrategias de inteligencia artificial que se desarrollaron en España y que han proporcionado un plan de actuación orientativo para la implementación de la IA.

La Estrategia Nacional de Inteligencia Artificial (ENIA) se publicó en diciembre de 2020 con el propósito de comprometerse con la Unión Europea para que esta sea líder en el

⁶ Ministerio de Defensa. *Visión de la Inteligencia Artificial en las FAS*, 2024

desarrollo de una IA ética, inclusiva y económicamente eficiente⁷. Esta estrategia no menciona explícitamente la defensa y seguridad en la redacción.

La Estrategia de Inteligencia Artificial 2024 se aprobó en España en mayo de 2024. Esta iniciativa tiene como objetivo acelerar y promover la implantación de la IA a nivel nacional, así como reforzar la ENIA⁸. En este texto tampoco se contempla la aplicación para el ámbito militar.

En cuanto a documentos específicos de defensa y seguridad nacional, existen políticas y estrategias que, aunque no se aborde en algunas de ellas de forma clara la IA, establecen distintos marcos en los que se podría incluir el uso y el desarrollo de esta herramienta de forma concreta. Además, en los documentos propios del Ministerio de Defensa, los preceptos se pueden extrapolar para establecer cierto criterio sobre la legitimidad de la aplicación de la IA.

La Estrategia de Tecnología e Innovación para la Defensa (ETID) promueve proyectos I+D+i que fortalezcan a nivel tecnológico a los grupos de investigación nacionales para participar en proyectos de defensa⁹. Es relevante porque se tratan temas de la tecnología en las armas y municiones, entre otros aspectos, aunque no se mencione la IA como tal.

En el contexto del comportamiento militar, las Reales Ordenanzas de las Fuerzas Armadas recogen las conductas militares y principios éticos conforme a la normativa jurídica¹⁰. Tampoco se hace referencia a la IA, pero se puede prever que su uso puede generar dilemas éticos tanto en el área de conflicto como en tareas de gestión¹¹.

⁷ Gobierno de España. *Estrategia Nacional de Inteligencia Artificial (ENIA)*. Gobierno de España, 2020. Disponible en: <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf>

⁸ Gobierno de España. *Estrategia de Inteligencia Artificial 2024*. Ministerio de Economía, Comercio y Empresa, 2024. Disponible en: https://portal.mineco.gob.es/es-digitalizacionIA/Documents/Estrategia_IA_2024.pdf

⁹ Ministerio de Defensa. *Estrategia de Tecnología e Innovación para la Defensa (ETID) 2020*. Ministerio de Defensa, 2020. Disponible en: https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-e-innovacion-para-la-defensa-etid-2020-libros-papel.html?__store=es

¹⁰ Ministerio de Defensa. *Reales Ordenanzas para las Fuerzas Armadas*. Real Decreto 96/2009, de 6 de febrero. Publicado en el Boletín Oficial del Estado, núm. 33, de 7 de febrero de 2009. Disponible en: https://www.defensa.gob.es/Galerias/fuerzasarmadas/realesordenanzas/RROOFAS_2009_BOE.pdf

¹¹ Escuela Militar de Estudios Jurídicos. *Revista española de derecho militar 116*. Ministerio de Defensa, 2021. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/redem_116.pdf

Así mismo, la Estrategia de Seguridad Nacional señala que se llevarán a cabo iniciativas para abordar situaciones de crisis, como aplicar tecnologías que integren la IA con la gestión del conocimiento¹².

Europa

Europa fue pionera en establecer en 2024 la Ley de IA, una regulación integral sobre IA y que hace que se sitúe como referente global en este aspecto¹³. Esta normativa tiene como objetivo establecer un sistema normativo uniforme para el desarrollo y uso de sistemas de IA. Además, es el primer reglamento que regula la IA exclusivamente¹⁴. No aplica para el ámbito militar, como se indica en el apartado 3 del artículo 2:

“3. El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias.

El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.”¹⁵.

¹² Consejo de Seguridad Nacional. *Estrategia de Seguridad Nacional 2021*. Gobierno de España, 2021. Disponible en: https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20Accesible_1.pdf

¹³ Comisión Europea. *AI Act*. Comisión Europea. Recuperado el 5 de junio de 2025 de: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

¹⁴ Comisión Europea. *Ley de IA*. Comisión Europea. Recuperado el 5 de junio de 2025 de: <https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai>

¹⁵ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, 12 de julio de 2024, nº 1689.

Respecto a la protección de los datos, Europa dispone de un marco legal en el que se tratan tanto los personales como los que no lo son. Las leyes que lo componen son relevantes en este contexto ya que, al utilizar las tecnologías, incluyendo la IA, se debe hacer un uso responsable de estos datos.

En este sentido, destaca el RGPD (Reglamento General de Protección de Datos) de 2016, que protege los datos personales de las personas físicas y al igual que su tratamiento. Este reglamento excluye la seguridad nacional de su ámbito de aplicación el artículo 2.2:

“2. El presente Reglamento no se aplica al tratamiento de datos personales:

- a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
- b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
- c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
- d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.”¹⁶.

Para facilitar la disponibilidad e intercambio de datos entre países de la UE y beneficiar así tanto a los ciudadanos como a las empresas, está en vigor desde 2022 la DGA (Ley de Gobernanza de Datos). A diferencia del RGPD, la DGA trata tanto los datos personales como los no personales¹⁷, pero tampoco aplica para defensa y seguridad nacional como indica el artículo 1.5:

¹⁶ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, de 4 de mayo de 2016, nº119.

¹⁷ Comisión Europea. *Una estrategia europea para los datos*. Comisión Europea. Recuperado el 5 de junio de 2025 de: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>

“5. El presente Reglamento se entenderá sin perjuicio de las competencias de los Estados miembros respecto a las actividades relativas a la seguridad pública, la defensa y la seguridad nacional.”¹⁸.

Por último, también es relevante mencionar la regulación europea en temas de ciberseguridad, entre las que destacan la Directiva NIS2 y el Reglamento DORA, ambas de 2022. La primera establece medidas para lograr una mayor ciberseguridad en la Unión Europea y mejorar el mercado interior¹⁹. La segunda refuerza la ciberseguridad de entidades financieras. Ninguna de las dos aplica para las funciones de defensa y seguridad nacional, como se expresa en el artículo 2.7 de la Directiva NIS2:

“7. La presente Directiva no se aplicará a las entidades de la Administración pública que lleven a cabo sus actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley, incluidas la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales.”

y en el considerando 17 del Reglamento DORA: “De conformidad con el artículo 4, apartado 2, del Tratado de la Unión Europea, y sin perjuicio del control judicial por parte del Tribunal de Justicia, el presente Reglamento no debe afectar a la responsabilidad de los Estados miembros relativa a las funciones esenciales del Estado que afectan a la seguridad pública, la defensa y la salvaguardia de la seguridad nacional, por ejemplo en casos en los que facilitar información sería contrario a la salvaguardia de la seguridad nacional.”²⁰

¹⁸ Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). *Diario Oficial de la Unión Europea*, de 3 de junio de 2022, nº152.

¹⁹ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). *Diario Oficial de la Unión Europea*, 27 de diciembre de 2022, nº333.

²⁰ Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011. *Diario Oficial de la Unión Europea*, 27 de diciembre de 2022, nº333.

Compromisos

Una vez revisados algunos de los documentos normativos y en vigor actualmente en España y Europa, se procede a ver otro tipo de documentos que aplican únicamente a los países que se adscriban a ellos, como es el caso de OECD AI Principles de 2019. Se trata del primer estándar intergubernamental y fomenta una IA fiable e innovadora que respeta los derechos humanos²¹, pero no se hace mención del ámbito militar. Países como Estados Unidos, España, Japón y Reino Unido se han adherido a estos principios²².

De forma similar, está la Convención sobre Ciertas Armas Convencionales (CCAC) de 1980. Esta se basa en los principios de otras normas para prohibir y restringir el uso de armas para proteger a civiles y que no se causen daños graves al medio ambiente²³. Es relevante porque establece límites en el empleo de armamento en conflictos con el fin de causar el menor daño posible a los grupos mencionados.

Para finalizar con este tipo de documentos, el Proceso de IA de Hiroshima consta de un conjunto de principios rectores a seguir por las organizaciones que desarrollan IA para promover una IA segura y confiable a nivel mundial²⁴. Estos principios no excluyen expresamente la defensa y la seguridad nacional, pero tampoco la mencionan. En una parte del texto, traducido al español, dice “Estos principios deben aplicarse a todos los actores de la IA, cuando y como sea aplicable para cubrir el diseño, desarrollo, despliegue y uso de sistemas avanzados de IA.

²¹ OECD. *AI principles*. OECD. Recuperado el 5 de junio de 2025, de: <https://www.oecd.org/en/topics/ai-principles.html>

²² OECD. *OECD Legal Instruments*. OECD. Recuperado el 5 de junio de 2025 de: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents>

²³ Sandoz, Y. *Convención de 10 de octubre de 1980 sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados (convención de 10 de octubre de 1980)*. United Nations, 2010. Disponible en: https://legal.un.org/avl/pdf/ha/cprccc/cprccc_s.pdf

²⁴ Comisión Europea. *Declaración de los dirigentes del G-7 sobre el proceso de la IA de Hiroshima*. Comisión Europea, 2023. Recuperado el 5 de junio de 2025, de: <https://digital-strategy.ec.europa.eu/es/library/g7-leaders-statement-hiroshima-ai-process>

Esperamos seguir desarrollando estos principios como parte del marco político global, con aportaciones de otras naciones y de partes interesadas más amplias del mundo académico, empresarial y de la sociedad civil.”²⁵.

Otros

Entre otros documentos relacionados con la IA, hay muchos países que han elaborado sus códigos éticos sobre el uso de esta herramienta, como China o India. Estos documentos se pueden tomar como referencia, pero no imponen medidas sancionadoras. Además, en vez de disponer de reglamentos específicos sobre la IA, cuentan con leyes que abarcan de una forma más general la ciberseguridad, sin centrarse en tecnologías concretas.

En contraste con la aproximación occidental hacia el uso de la IA, en China se está implantado con paso acelerado el uso de IA con fines incluso de evaluación de la población que, con la legislación aplicable aquí, sería imposible trasladar. Considerando que incluso el ámbito civil se ve limitado en este sentido, resulta menos viable que se tenga en cuenta el mundo militar.

Por otro lado, existen organizaciones y congresos que reúnen a investigadores y académicos de diferentes territorios para tratar temas referentes a la IA, como, por ejemplo, la asociación Iberamia, cuyo objetivo es impulsar las actividades científicas y tecnológicas que implican el uso de la IA en los países Iberoamericanos y de habla española y portuguesa²⁶. Así mismo, en el contexto europeo está la AI HLEG (High-Level Expert Group on Artificial Intelligence), que cuenta con más de 4000 miembros pertenecientes a la Unión Europea²⁷. Otro ejemplo de reunión global es la cumbre REAIM (Responsible AI in the Military domain Summit) cuyo objetivo es tratar el uso responsable de la IA en el contexto militar²⁸.

²⁵ Comisión Europea. *Principios rectores internacionales del proceso de Hiroshima para un sistema avanzado de IA*. Comisión Europea, 2023. Recuperado el 5 de junio de 2025, de: <https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-guiding-principles-advanced-ai-system>

²⁶ Iberamia. *Información institucional*. Iberamia. Recuperado el 5 de junio de 2025, de <https://www.iberamia.org/iberamia/informacion-institucional/>

²⁷ Comisión Europea. *Grupo de expertos de alto nivel sobre inteligencia artificial*. Comisión Europea. Recuperado el 5 de junio de 2025, de: <https://digital-strategy.ec.europa.eu/es/policies/expert-group-ai>

²⁸ REAIM. *REAIM Summit 2024*. REAIM. Recuperado el 5 de junio de 2025, de: <https://www.reaim2024.kr/reaimeng/index.do>

Aplicación de las normativas

Como se ha observado en el punto anterior, existen diversas normativas que tratan el ámbito tecnológico a nivel nacional, europeo e internacional; pero en la mayoría de ellas se excluye su uso para la defensa y la seguridad nacional. Por ello, aunque Europa es pionera en desarrollar una ley específica que aborda la implementación y el uso de la IA, no se puede considerar como un referente en el ámbito militar, a no ser que, como especifica la propia Ley, los sistemas de IA desarrollados en ese ámbito se utilizaran temporal o permanentemente para otros fines, como el civil o humanitario²⁹.

Entonces, realmente, ¿cuál es el impacto de estas regulaciones en defensa y seguridad? ¿Cómo se podrían aplicar estas regulaciones en defensa y seguridad? ¿Qué desafíos éticos y legales surgen dentro del marco normativo actual al respecto?

La IA cada vez va adquiriendo un papel de mayor importancia en la defensa y seguridad nacional, lo que plantea cuestiones normativas y éticas que es fundamental gestionar, ya sea mediante la creación de nuevas normativas o modificando las existentes, incluyendo los apartados pertinentes.

En este sentido, un ejemplo es la aplicación de la IA en los enjambres de drones. Estos drones se coordinan entre sí y, en muchas ocasiones, no es necesaria la intervención humana. Son más efectivos que los drones individuales ya que, en este caso, son capaces de realizar diferentes tareas y su actividad puede continuar si uno de ellos tuviera algún problema o estuviera inoperativo. A su vez, algunos métodos de enjambre de drones se basan en algoritmos muy sofisticados que se inspiran en el comportamiento colectivo de aves o insectos y que, además, hacen posible que respondan ante nuevas situaciones gracias a la IA. Se puede aplicar esta tecnología para la búsqueda de personas desaparecidas, por ejemplo³⁰. Estados Unidos está trabajando en diferentes proyectos relacionados con este funcionamiento de los drones, como el programa

²⁹ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, 12 de julio de 2024, nº 1689.

³⁰ U.S. Government Account Office. *Science & Tech Spotlight: Drone Swarm Technologies*. U.S. Government Account Office, 14 de septiembre de 2023. Recuperado el 5 de junio de 2025 de: <https://www.gao.gov/products/gao-23-106930>

Gremlins de UAV (*Unmanned Air Vehicle*) y CICADA (*Close In Covert Autonomous Disposable Aircraft*)³¹.

Este es solo uno de los muchos casos en los que se puede aplicar la IA en el contexto militar, lo que implica que esta herramienta se está integrando progresivamente en este ámbito, formando ya parte de estrategias y herramientas operativas. La ausencia de un marco normativo aplicable a esta materia proporciona una mayor libertad a los Estados a la hora de implementar y utilizar sistemas basados en IA. Sin embargo, esta libertad, a su vez, motiva el planteamiento de los límites éticos y legales.

En este contexto, depende de cada Estado el seguir una serie de medidas y principios éticos, que no deja de ser una cuestión subjetiva, y que genera, como ya se ha expuesto previamente en este artículo, una desalineación de códigos éticos y normativas.

“La gobernanza de la IA es un problema global, no solo nacional. Una gobernanza eficaz de los sistemas de IA requiere cooperación internacional, ya que los sistemas de IA y sus efectos no respetan las fronteras nacionales. Los países deben colaborar para establecer estándares y normas globales de uso de la IA”³².

La realidad es que el desarrollo de armamento y herramientas continuará evolucionando en consecuencia al avance constante de las nuevas tecnologías y, en este caso de la IA, generando nuevas situaciones que continuarán con el planteamiento de los mismos dilemas mencionados anteriormente.

De inicio, pueden surgir las preguntas: ¿quién es el responsable de los actos de la IA? ¿Cómo se puede garantizar que no tomarán decisiones basándose en sesgos? ¿Qué tipo de datos se utilizan para entrenar estos sistemas? ¿Se respeta la privacidad de los ciudadanos?

El marco legal actual no da respuestas claras a estas preguntas.

³¹ Gómez de Ágreda, Á. *La inteligencia artificial en el campo de batalla*. En Ministerio de Defensa (Ed.), *Usos militares de la Inteligencia Artificial, la automatización y la robótica (IAA&R)*. 2020. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf

³² Marwala, T. . *Militarization of AI Has Severe Implications for Global Security and Warfare*. UNU, 24 de Julio de 2023. Recuperado el 5 de junio de 2025, de: <https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare>

La OTAN, en 2021, especificó un marco en el que se aprobaron seis principios de uso responsable para la IA en Defensa: “Legalidad, Responsabilidad y Rendición de Cuentas, Explicabilidad y Trazabilidad, Fiabilidad, Gobernabilidad y Mitigación de Sesgos.”³³.

Estos principios, por ejemplo, se podrían tener en cuenta para el entrenamiento de la IA. Los seres humanos toman decisiones según sus sesgos y prejuicios, aunque pueda ser de forma inconsciente. La IA tomará sus decisiones en función de los datos con los que sea entrenada, por consiguiente, la imparcialidad y la diversidad en ellos son cruciales para asegurar resultados de calidad y justos. Pero ¿cómo se regula el uso de estos datos? Existen diferentes normativas que regulan y sancionan la violación de la protección de datos, como el RGPD en Europa, pero se excluye de su ámbito de aplicación el entorno militar.

Aunque la IA pretende mejorar el desempeño humano, no dispone todavía de habilidad respecto a la interacción social y, por lo tanto, de forma de identificar y de entender comportamientos complejos que se dan o son necesarios en el campo de batalla³⁴.

En los siguientes párrafos se expondrán dos casos ilustrativos, sin que ello suponga una crítica en relación a ellos, que reflejan la falta de normativa de la IA.

El primer ejemplo, es el uso que ha dado el gobierno de China a esta tecnología en la provincia de Xinjiang. Se implementaron sistemas de reconocimiento facial y vigilancia genómica, y se estima que se ha detenido a entre el 10% y el 20% de los uigures³⁵, un grupo étnico de ascendencia turca y practicante del islam que se encuentra en esta

³³ OTAN. *Summary of NATO's revised Artificial Intelligence (AI) strategy*. OTAN, 2024. Recuperado el 5 de junio de 2025, de:

https://www.nato.int/cps/en/natohq/official_texts_227237.htm#:~:text=Within%20the%20AI%20Strategy%2C%20Allies,Reliability%2C%20Governability%20and%20Bias%20Mitigation.

³⁴ Las Heras, P. *El reto de la inteligencia artificial para la seguridad y defensa*. Universidad de Navarra, 18 de Octubre de 2023. Recuperado el 5 de junio de 2025, de: <https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa>

³⁵ Feldstein, S. *La vigilancia de alta tecnología de China impulsa la opresión de los uigures*. Bulletin of the Atomic Scientists, 27 de Octubre de 2022. Recuperado el 5 de junio de 2025, de: <https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/>

provincia china³⁶. Según Amnistía Internacional, China, para establecer este control, compró sistemas de vigilancia digital a empresas de Francia, Suecia y Países Bajos³⁷.

En este caso, se puede apreciar tanto la responsabilidad de China por el incumplimiento de los Derechos Humanos, como la de estas empresas que, aunque indirectamente, estarían implicadas en las medidas tomadas por esta gran potencia³⁸.

El segundo ejemplo es la utilización de drones STM Kargu-2 de fabricación turca en Libia en el año 2020 que, según describe un informe del Consejo de Seguridad de las Naciones Unidas, se trata de drones autónomos que se utilizaron para ir tras los soldados en retirada³⁹. No hubo víctimas, pero podrían haber sido atacados de forma autónoma y en el informe se confirma que, aunque se haya intentado prohibir este tipo de armas, se utilizaron igualmente estos drones⁴⁰.

Conclusiones

El marco normativo actual en el que se regula el desarrollo y aplicación de la IA, ya sea nacional, europeo o internacional, en el ámbito de defensa y seguridad nacional, plantea retos éticos y jurídicos, como se ha evidenciado a lo largo de este documento.

Por un lado, está el problema ya señalado en la introducción: la legislación va mucho más lenta que el avance de las tecnologías de forma general, no solo que el avance de la IA. Esto es un obstáculo a la hora de establecer normativas actualizadas y claras para tratar las nuevas tecnologías.

³⁶ Fernández Aparicio, P. *Los uigures y el dragón chino en la encrucijada (reedición)*. IEEE-CESEDEN, 2024.

Disponible en:

<https://www.defensa.gob.es/documents/2073105/2265107/Los+uigures+y+el+drag%C3%B3n+chino+en+la+encrucijada+%28reedici%C3%B3n%29.pdf/56606714-9d21-b311-b1b9-4bdb021136da?t=1732097514224>

³⁷ Amnistía Internacional. *EU companies selling surveillance tools to China's human rights abusers*. Amnistía Internacional, 21 de Septiembre de 2020. Recuperado el 5 de junio de 2025, de:

<https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/>

³⁸ Ídem

³⁹ Colegio oficial de Ingenieros Castilla-La Mancha. *Un dron ha atacado a personas de forma totalmente autónoma por primera vez*. Colegio oficial de Ingenieros Castilla-La Mancha, 21 de Septiembre de 2020. Recuperado el 5 de junio de 2025 de: <https://coiiclm.org/un-dron-ha-atacado-a-personas-de-forma-totalmente-autonoma-por-primera-vez/>

⁴⁰ AS. *Un dron ataca a humanos sin habérselo ordenado: Su IA autónoma decidió el ataque*. AS, 2021. Recuperado el 5 de junio de 2025, de: https://as.com/meristation/2021/05/28/betech/1622234551_710916.html

Por otro lado, las normativas actuales que sí que tienen en cuenta estas herramientas, excluyen de su ámbito de aplicación o no mencionan directamente la defensa y seguridad en sus textos, lo que supone una incertidumbre jurídica sobre a qué reglamentos debe estar sujeto el desarrollo y uso de sistemas militares basados en IA, así como los límites legales y éticos. Además, se añade la dificultad de que en el ámbito militar muchas de las decisiones se apoyan en criterios confidenciales y en intereses estratégicos nacionales.

Concluyendo, la falta de regulación de la IA en defensa y seguridad representa un riesgo tanto para el ámbito militar como para el civil debido al uso indebido que se le puede dar a la herramienta. Es por ello por lo que es necesaria una colaboración internacional, con el fin de desarrollar una normativa que contemple todos los ámbitos y aspectos de la IA, especialmente en el entorno de defensa y seguridad. Aunque esto limitaría en parte la innovación, su objetivo principal sería contar con un conjunto de normas comunes que se podrían alinear con la legislación actual y facilitaría el tratamiento y el uso responsable de la IA en este ámbito.

*Emma Talavera Rodríguez**

Estudiante en prácticas en el IEEE
Alumna del Máster en Ciberdelincuencia Universidad Nebrija