Cuadernos de RES PUBLICA en derecho y criminología
Nº 8 / 2026 ISSN: 2990-0697 DOI: 10.46661/respublica.13703.

El sistema jurídico ante la inteligencia artificial. Implicaciones de sus avances y retos en una sociedad algoritmizada

The legal system and artificial intelligence. Implications of its advances and challenges in an algorithm-driven society

Paola Alexandra Sierra-Zamora
Universidad Católica de Colombia. Bogotá (Colombia)
pasierra@ucatolica.edu.co
ORCID: 0000-0002-3146-7418

Giuseppe Gangi Guillen
Universidad Nebrija. Madrid. (España)
ggangi@nebrija.es
ORCID: 0000-0001-5627-3874

Resumen

La integración de la inteligencia artificial en la gobernanza pública debe evaluarse dentro de este marco constitucional. Los sistemas que automatizan la toma de decisiones en ámbitos como la asignación de prestaciones sociales, el control de la migración o la aplicación de la ley afectan directamente a las condiciones en las que las personas ejercen sus derechos y persiguen sus proyectos de vida. El presente trabajo analiza cómo la utilización de sistemas de inteligencia artificial en contextos militares afecta a los mecanismos tradicionales de imputación jurídica, prestando especial atención a la fragmentación de responsabilidades derivada de la interacción entre operadores humanos, instituciones públicas y empresas tecnológicas.

Palabras clave: Inteligencia artificial; Gobernanza algorítmica; derechos humanos; justicia automatizada; toma de decisiones militares; Derecho Internacional Humanitario.

Abstract

The integration of artificial intelligence into public governance must be assessed within this constitutional framework. Systems that automate decision-making in areas such as the allocation of social benefits, migration control or law enforcement directly affect the conditions under which people exercise their rights and pursue their life plans. This paper analyses how the use of artificial intelligence systems in military contexts affects traditional mechanisms of legal accountability, paying particular attention to the fragmentation of responsibilities arising from the interaction between human operators, public institutions and technology companies.

Keywords: Artificial intelligence; Algorithmic governance; human rights; automated justice; Military Decision-Making; International Humanitarian Law.

Cómo citar este trabajo: Sierra-Zamora, Paola Alexandra., y Gangi Guillen, Giuseppe Kodjack. (2026). El sistema jurídico ante la inteligencia artificial. Implicaciones de sus avances y retos en una sociedad algoritmizada. *Cuadernos de RES PUBLICA en derecho y criminología, (8), 01–16.* https://doi.org/10.46661/respublica.13703.

Recepción: 23.06.2026 **Aceptación:** 23.06.2026 **Publicación:** 23.06.2026

1. Introducción

La incorporación de la inteligencia artificial (IA) a los ámbitos de la seguridad y la defensa constituye una de las transformaciones tecnológicas más relevantes de las últimas décadas. Los avances en aprendizaje automático, procesamiento masivo de datos y sistemas automatizados de apoyo a la decisión han modificado profundamente la forma en que los Estados planifican, ejecutan y supervisan operaciones militares.

La inteligencia artificial ha dejado progresivamente de percibirse como un mero conjunto de técnicas computacionales diseñadas para optimizar procesos o automatizar tareas rutinarias. En cambio, cada vez más funciona como una infraestructura a través de la cual se ejerce la autoridad, se moldea el comportamiento social y se producen resultados jurídicamente relevantes. Esta transformación requiere un cambio conceptual en el análisis jurídico: pasar de considerar la inteligencia artificial como un artefacto tecnológico neutral a entenderla como generadora y mediadora de poder normativo. En este contexto, la IA debe ser comprendida no simplemente como una herramienta, sino como una infraestructura normativa capaz de reconfigurar las relaciones entre Estado, mercado y ciudadanía.

Una característica crucial de la inteligencia artificial contemporánea es la concentración del poder tecnológico y económico en un número limitado de actores privados. Las grandes empresas tecnológicas diseñan, entrenan y controlan los modelos más avanzados, a menudo operando en múltiples jurisdicciones. Como resultado, las entidades privadas configuran cada vez más las infraestructuras a través de las cuales se ejerce la autoridad pública.

Desde una perspectiva jurídica, este cambio tiene consecuencias relevantes. La gobernanza basada en predicciones tiende a dar prioridad a la eficiencia, la optimización y la minimización de riesgos. Si bien estos objetivos no son intrínsecamente problemáticos, resultan insuficientes como fundamentos de una autoridad pública legítima. Los ordenamientos jurídicos democráticos no se definen exclusivamente por su capacidad para producir resultados efectivos, sino por su compromiso con la equidad procesal, la transparencia y el respeto de la dignidad humana.

Este proceso plantea importantes interrogantes jurídicos y éticos. Entre ellos destaca la dificultad para determinar quién debe responder cuando una decisión apoyada o ejecutada mediante sistemas de IA ocasiona daños a personas o bienes protegidos por el Derecho Internacional Humanitario (DIH). La creciente participación de algoritmos en procesos de identificación, clasificación y priorización de objetivos introduce nuevas formas de complejidad en la atribución de responsabilidades.

En este sentido, la inteligencia artificial difumina la frontera tradicional entre el poder público y el privado. Las decisiones que afectan a los derechos fundamentales pueden verse influidas por sistemas cuya lógica interna está protegida como información privada. Esta opacidad socava la posibilidad de una impugnación significativa y debilita las condiciones para la rendición de cuentas democrática.

2. La transformación de la responsabilidad en la era digital

La responsabilidad ha constituido históricamente uno de los pilares fundamentales de los sistemas jurídicos. Tradicionalmente, la atribución de consecuencias jurídicas se basaba en la existencia de una relación identificable entre una conducta, un sujeto responsable y el resultado producido.

Sin embargo, el desarrollo de tecnologías avanzadas ha alterado este esquema clásico. Los procesos automatizados de toma de decisiones introducen nuevos actores y mecanismos de mediación que dificultan la identificación directa de quién adopta

realmente una decisión y quién debe responder por sus efectos.

En este contexto, la inteligencia artificial no actúa como un mero instrumento pasivo. Su capacidad para procesar información, establecer correlaciones y formular recomendaciones influye de manera significativa en las decisiones humanas. Como consecuencia, los modelos tradicionales de responsabilidad deben enfrentarse a escenarios en los que la causalidad y la imputación jurídica resultan menos evidentes.

3. Riesgos para la responsabilidad y control humano

La incorporación de la IA en sistemas militares plantea desafíos fundamentales para la ética, la responsabilidad y la toma de decisiones en el campo de batalla. Aunque los algoritmos pueden procesar grandes volúmenes de información y ejecutar funciones con alta velocidad, carecen de juicio moral, comprensión contextual y capacidad de ponderar adecuadamente las consecuencias jurídicas, estratégicas y humanitarias de sus acciones.

En este sentido, la doctrina contemporánea ha insistido en la necesidad de mantener un grado de supervisión humana en los sistemas de armas y apoyo a la decisión, particularmente en aquellas funciones que puedan implicar el uso de la fuerza letal. Este enfoque se conoce como human-in-the-loop, según el cual un operador humano debe permanecer integrado en el ciclo de decisión, autorizando o validando las acciones críticas del sistema.

Sin embargo, en la práctica operativa, la existencia formal de supervisión humana no garantiza necesariamente un control efectivo. La velocidad del procesamiento algorítmico, la complejidad de los modelos y la presión del entorno operativo pueden transformar la intervención humana en un acto más formal que sustantivo, debilitando la capacidad real de deliberación.

En este contexto, los riesgos asociados al uso de IA no se limitan a errores técnicos o fallos aislados, sino que se vinculan con transformaciones más profundas en la estructura de la responsabilidad:

- La Difuminación de la responsabilidad, donde la decisión final resulta de la interacción entre múltiples actores humanos y tecnológicos.
- El desplazamiento del juicio humano efectivo, cuando la supervisión se vuelve reactiva más que deliberativa.
- La confianza excesiva en sistemas automatizados, que puede llevar a la delegación implícita de decisiones críticas.
- Los desafíos de interoperabilidad en entornos multinacionales, donde sistemas heterogéneos incrementan la complejidad de atribución de errores.

En conjunto, estos elementos muestran que el problema central no es únicamente la presencia o ausencia de supervisión humana, sino la progresiva fragmentación del proceso decisional, que dificulta la identificación de un sujeto claramente responsable dentro de la cadena de acción militar

3.1. Fragmentación y dilución de la responsabilidad

Uno de los principales problemas asociados al uso de inteligencia artificial en operaciones militares es la progresiva fragmentación de la responsabilidad.

En los sistemas convencionales, la cadena de decisión suele ser relativamente clara: una persona adopta una decisión y asume las consecuencias derivadas de ella. Sin embargo, cuando intervienen sistemas algorítmicos complejos, el proceso se distribuye entre múltiples actores.

Desarrolladores de software, proveedores de infraestructura tecnológica, responsables políticos, mandos militares y operadores finales participan de forma conjunta en la generación del resultado. Esta estructura

dificulta determinar qué grado de responsabilidad corresponde a cada uno de ellos cuando se producen errores o daños.

La consecuencia es la aparición de lo que diversos autores denominan "dilución algorítmica de la responsabilidad", fenómeno por el cual la responsabilidad se dispersa entre numerosos participantes hasta hacer más difícil su identificación individual.

La utilización de sistemas de inteligencia artificial en ámbitos sensibles de la actividad humana ha reabierto el debate sobre la capacidad del derecho para anticipar y gestionar riesgos derivados de tecnologías emergentes. Aunque la inteligencia artificial suele presentarse como una herramienta orientada a optimizar procesos de toma de decisiones y aumentar los niveles de eficiencia, su creciente incorporación en sectores críticos demuestra que los beneficios potenciales coexisten con riesgos cuya magnitud aún no ha sido completamente determinada.

La preocupación por estos riesgos ha llevado a diversos organismos internacionales y reguladores a desarrollar modelos normativos basados en la clasificación de sistemas según su nivel de peligrosidad. La aproximación regulatoria más notable es el Reglamento de Inteligencia Artificial de la Unión Europea (AI Act), instrumento que adopta un modelo escalonado basado en la gestión del riesgo y distingue entre sistemas de riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo. Este modelo parte de una premisa fundamental: no toda inteligencia artificial genera las mismas consecuencias jurídicas ni requiere idénticos niveles de control regulatorio.

La categoría de alto riesgo resulta especialmente relevante para el presente estudio debido a que comprende sistemas capaces de producir afectaciones significativas sobre derechos fundamentales, seguridad pública, infraestructuras críticas y procesos decisorios de especial sensibilidad. En estos casos, la regulación jurídica no se fundamenta exclusivamente en los daños ya producidos, sino en la existencia de una probabilidad razonable de afectación futura que justifica la adopción de medidas preventivas.

Desde esta perspectiva, los conceptos de riesgo, amenaza, peligro y daño adquieren una especial utilidad para el análisis jurídico de la inteligencia artificial militar. Para efectos del presente escrito, el riesgo algorítmico[1] puede entenderse como la posibilidad abstracta de que un sistema de inteligencia artificial produzca decisiones, recomendaciones o acciones capaces de afectar bienes jurídicos protegidos como consecuencia de errores de diseño, sesgos de entrenamiento, deficiencias en los datos utilizados o limitaciones inherentes al funcionamiento del propio sistema.

En esta fase inicial, la afectación todavía no se ha materializado. Sin embargo, la mera existencia de una probabilidad significativa de daño resulta suficiente para justificar mecanismos de supervisión y control. El derecho contemporáneo ha abandonado progresivamente la lógica reactiva que exigía la producción efectiva del perjuicio para activar consecuencias jurídicas. En su lugar, se ha consolidado una visión preventiva orientada a intervenir antes de que el daño ocurra.

La amenaza aparece cuando el riesgo deja de ser una hipótesis abstracta y se convierte en una posibilidad concreta de afectación. En el ámbito militar, ello podría ocurrir cuando un sistema de inteligencia artificial presenta fallos identificados que comprometen la correcta selección de objetivos, generan

[1] La definición propuesta se construye a partir de la teoría de la sociedad del riesgo desarrollada por Beck (1998), de los enfoques regulatorios basados en riesgo adoptados por el Reglamento Europeo de Inteligencia Artificial (AI Act) y de la literatura contemporánea sobre riesgos asociados a sistemas algorítmicos.

errores sistemáticos en la identificación de combatientes o incrementan significativamente la probabilidad de afectación a la población civil. En tales circunstancias, el riesgo adquiere una dimensión tangible que exige respuestas inmediatas por parte de las autoridades competentes.

El peligro constituye un grado de concreción aún más avanzado dentro de esta secuencia conceptual. Se configura cuando la posibilidad de afectación alcanza niveles de proximidad que hacen razonablemente previsible la producción del daño. En operaciones militares apoyadas por inteligencia artificial, el peligro podría manifestarse durante la ejecución de ataques en los cuales la información procesada por el sistema resulta insuficiente, desactualizada o incompatible con las condiciones reales del entorno operacional.

Finalmente, el daño representa la materialización efectiva de la afectación. En contextos de conflicto armado, dicho daño puede traducirse en pérdidas de vidas humanas, lesiones a personas protegidas, destrucción de bienes civiles, ataques indiscriminados o vulneraciones de derechos fundamentales. En estos casos, las consecuencias jurídicas ya no se limitan al ámbito preventivo, sino que involucran cuestiones relativas a responsabilidad estatal, responsabilidad individual y reparación de las víctimas.

La importancia de esta secuencia radica en que permite comprender que el riesgo algorítmico no surge exclusivamente en el momento en que se ejecuta una operación militar. Por el contrario, puede originarse mucho antes, durante las fases de diseño, programación, entrenamiento, validación y despliegue de los sistemas de inteligencia artificial. Esta circunstancia posee profundas implicaciones jurídicas, pues desplaza parcialmente la atención desde la respuesta frente al daño consumado hacia la identificación temprana de riesgos previsibles.

En consecuencia, la regulación de los sistemas de inteligencia artificial de alto riesgo no puede limitarse a evaluar los resultados producidos por la tecnología. Resulta igualmente necesario examinar las condiciones bajo las cuales dicha tecnología fue concebida, desarrollada y autorizada para su utilización. Desde esta perspectiva, la respuesta anticipatoria jurídica a la inteligencia artificial exige una aproximación preventiva basada en la gestión integral del riesgo, especialmente cuando los sistemas son empleados en escenarios de conflicto armado donde los márgenes de error pueden traducirse en consecuencias irreparables para la vida, la integridad y la dignidad humana

3.2. Casos ilustrativos y dificultades de atribución

La dilución algorítmica de la responsabilidad puede observarse en distintos tipos de situaciones donde la interacción entre sistemas automatizados, decisiones humanas y estructuras institucionales dificulta la identificación de un responsable claro.

En contextos operativos militares, se han documentado incidentes en los que el uso de sistemas de apoyo a decisiones o plataformas automatizadas de identificación de objetivos ha contribuido a errores con consecuencias civiles significativas. En estos casos, la dificultad no radica únicamente en determinar si existió una falla técnica o humana, sino en reconstruir el grado de influencia que ejercieron los sistemas algorítmicos en la decisión final, especialmente cuando la información procesada proviene de múltiples fuentes automatizadas y supervisadas de manera parcial.

La problemática descrita puede observarse en numerosos escenarios contemporáneos. En el ámbito militar se han documentado situaciones en las que sistemas automatizados de análisis de información o identificación de objetivos han contribuido a decisiones erróneas con consecuencias graves para la población civil. En estos casos resulta especialmente complejo determinar si el origen del problema se encuentra en una deficiencia técnica, en una interpretación

humana incorrecta o en una combinación de ambos factores.

Paralelamente, han surgido debates públicos relacionados con la participación de empresas tecnológicas en proyectos de defensa. La colaboración entre compañías especializadas en inteligencia artificial y organismos militares plantea interrogantes acerca de la distribución de responsabilidades éticas, jurídicas y políticas derivadas del uso de estas tecnologías.

Ambos ejemplos reflejan una misma realidad: la dificultad creciente para identificar un responsable único cuando las decisiones son producto de la interacción entre algoritmos, personas e instituciones.

Los sistemas de IA dependen de manera estructural de los datos que reciben para generar recomendaciones, clasificaciones o decisiones automatizadas. El rendimiento de un sistema algorítmico está fuertemente condicionado por la calidad, estructura y representatividad de la información con la que es entrenado y alimentado. En el ámbito militar, estos datos incluyen fuentes heterogéneas como imágenes satelitales, inteligencia de señales, reportes operativos, bases de datos históricas y flujos de información en tiempo real. Sin embargo, estos insumos no constituyen únicamente un soporte técnico neutral, sino que forman parte de un proceso de construcción de la realidad operativa sobre la cual se toman decisiones estratégicas.

En este sentido, la cuestión relevante no es únicamente la precisión técnica de los datos, sino también su selección, clasificación y jerarquización, ya que estos procesos determinan qué información es considerada relevante, qué se excluye del análisis y qué patrones se consideran significativos. De esta manera, los datos no solo alimentan el sistema, sino que contribuyen a estructurar el marco dentro del cual la IA interpreta el entorno.

Cuando los datos son incompletos, desactualizados o sesgados, los sistemas pueden producir resultados que afectan directamente principios fundamentales del derecho internacional humanitario, como la distinción, la proporcionalidad y la necesidad militar. Sin embargo, el problema no se limita al error técnico en la salida del sistema, sino que se extiende al origen mismo de la información utilizada para entrenarlo o activarlo.

En escenarios operativos, por ejemplo, una clasificación errónea de patrones de actividad o de imágenes satelitales puede derivar en la identificación incorrecta de objetivos. No obstante, la dificultad principal no radica únicamente en el resultado final, sino en la dificultad de determinar con precisión si el error provino del algoritmo, de la calidad del dato o de las decisiones humanas que determinaron qué información fue incorporada al sistema y bajo qué criterios

4. Concepto y funcionamiento de la inteligencia artificial en el ámbito militar

La inteligencia artificial puede definirse como un conjunto de métodos computacionales orientados a reproducir determinadas capacidades asociadas al razonamiento humano, como el reconocimiento de patrones, la clasificación de información o la formulación de predicciones.

La IA ha pasado de ser un instrumento de apoyo a convertirse en un componente estratégico de la guerra contemporánea. Su aplicación no solo transforma la manera en que se recopila y procesa la información, sino que también altera la dinámica de la toma de decisiones, los riesgos operativos y la naturaleza misma de la responsabilidad. Este capítulo explora cómo la IA se inserta en el ámbito militar, sus ventajas, riesgos y la manera en que los principales actores internacionales la integran en sus estrategias.

La IA no introduce únicamente eficiencia en la guerra, sino una reconfiguración estructural de la responsabilidad mediante la fragmentación del proceso decisional. Su funcionamiento se basa fundamentalmente

en tres elementos: los datos utilizados para entrenar los modelos, los algoritmos encargados de procesarlos y la infraestructura tecnológica necesaria para ejecutar dichos procesos.

En el ámbito de la defensa, estas herramientas se utilizan en actividades de vigilancia, reconocimiento, inteligencia y apoyo a la toma de decisiones. Entre sus aplicaciones más habituales destacan el análisis automatizado de imágenes, la detección de objetivos potenciales, la predicción de movimientos estratégicos y la gestión de grandes volúmenes de información operativa.

Aunque formalmente las decisiones continúan siendo adoptadas por personas, la inteligencia artificial influye de manera significativa en la forma en que esas decisiones se construyen y justifican.

La inteligencia artificial puede entenderse como un conjunto de técnicas computacionales diseñadas para permitir que sistemas digitales realicen tareas que, en condiciones normales, requieren capacidades cognitivas humanas, tales como el reconocimiento de patrones, la clasificación de información, la predicción de comportamientos y la generación de recomendaciones a partir del análisis de grandes volúmenes de datos.

En términos operativos, la IA no constituye una forma de "inteligencia" autónoma en sentido humano, sino un sistema estadístico avanzado que identifica correlaciones dentro de conjuntos de datos y produce resultados probabilísticos a partir de ellos. Su funcionamiento depende de tres elementos fundamentales: los datos que alimentan el sistema, los algoritmos que los procesan y la capacidad computacional que permite ejecutar dicho procesamiento a gran escala.

En el ámbito militar, estos sistemas se integran en procesos de inteligencia, vigilancia, reconocimiento y apoyo a la decisión. Entre sus aplicaciones más comunes se encuentran el análisis de imágenes satelitales y de drones para la detección de objetivos, la predicción de posibles movimientos de fuerzas adversarias, la simulación de escenarios de conflicto y la priorización automatizada de información relevante para la toma de decisiones operativas. En este sentido, la IA no sustituye formalmente la decisión militar, pero sí influye de manera directa en la forma en que esa decisión se construye, al seleccionar, jerarquizar y presentar la información disponible a los actores humanos.

Esta mediación algorítmica tiene implicaciones relevantes para la conducción de operaciones militares. En primer lugar, introduce una dependencia estructural de los datos: la calidad de la decisión depende directamente de la calidad, integridad y representatividad de la información utilizada para entrenar y alimentar los sistemas. En segundo lugar, incorpora el riesgo de sesgos algorítmicos, ya sea por limitaciones en los datos de entrenamiento, por decisiones de diseño o por condiciones operativas cambiantes que no fueron previstas en el modelo. En tercer lugar, puede generar una percepción de objetividad técnica que no necesariamente corresponde con la complejidad normativa y contextual de las decisiones militares, especialmente aquellas que implican la aplicación del Derecho Internacional Humanitario.

4.1. Dependencia de los datos y riesgos asociados

La eficacia de los sistemas de inteligencia artificial depende directamente de la calidad de los datos que utilizan.

Información incompleta, sesgada o desactualizada puede generar resultados incorrectos y afectar negativamente a los procesos de decisión. Asimismo, los algoritmos pueden incorporar sesgos derivados tanto de los datos empleados como de las decisiones adoptadas durante su diseño.

Otro problema relevante es la tendencia a atribuir a los sistemas tecnológicos una apariencia de objetividad que no siempre se

corresponde con la realidad. Las recomendaciones generadas por algoritmos continúan siendo el resultado de elecciones humanas previas y, por tanto, pueden contener limitaciones similares a las presentes en otros procesos de decisión.

4.2. Sistemas semi-autónomos y control humano significativo

En la actualidad, la mayoría de las aplicaciones militares de inteligencia artificial se desarrollan bajo modelos semi-autónomos. En estos sistemas, la tecnología asiste al operador humano proporcionando análisis, clasificaciones o recomendaciones, mientras que la decisión final permanece formalmente bajo control humano.

Este modelo se apoya en el principio de "control humano significativo", según el cual las decisiones con consecuencias potencialmente letales deben estar sujetas a supervisión efectiva por parte de personas.

No obstante, la creciente velocidad de procesamiento y la complejidad de los sistemas pueden reducir la capacidad real de supervisión. Cuanto más rápido opera un sistema automatizado, más difícil resulta para el operador analizar críticamente la información antes de actuar.

Por otro lado, los sistemas plenamente autónomos representan un escenario distinto, en el que la tecnología podría seleccionar y ejecutar acciones sin intervención humana directa. Aunque su utilización sigue siendo limitada, constituyen una cuestión central en los debates actuales sobre regulación internacional.

5. La opacidad algorítmica

Uno de los mayores desafíos asociados a la inteligencia artificial es la falta de transparencia de muchos de sus procesos internos. Numerosos sistemas basados en aprendizaje automático funcionan como auténticas "cajas negras", capaces de generar resultados complejos sin ofrecer explicaciones claras sobre cómo se alcanzan.

La opacidad constituye uno de los rasgos más problemáticos de la incorporación de IA en la toma de decisiones militares. Muchos de los sistemas utilizados, especialmente aquellos basados en aprendizaje automático, operan como "cajas negras": procesan grandes volúmenes de datos y generan recomendaciones o clasificaciones sin que los propios usuarios —e incluso en ocasiones los desarrolladores— puedan explicar con precisión cómo se alcanzó ese resultado.

En la práctica, esta opacidad se manifiesta en situaciones concretas. Por ejemplo, un sistema de inteligencia puede procesar imágenes satelitales, patrones de comportamiento y datos de comunicaciones para clasificar un objetivo como "amenaza de alto valor". El operador recibe esa conclusión con un nivel de confianza estadística, pero no necesariamente con una explicación comprensible de qué variables fueron determinantes ni cómo se ponderaron. En consecuencia, la decisión final —aunque formalmente humana— se apoya en un proceso que no es plenamente transparente ni verificable en tiempo real.

Esta limitación no solo dificulta la supervisión, sino también la reconstrucción posterior de los hechos. En caso de error —por ejemplo, un ataque contra un objetivo incorrecto— resulta complejo determinar si la falla provino de los datos, del diseño del algoritmo, de su entrenamiento o de la interpretación humana del resultado.

En un entorno en el que la rendición de cuentas depende de la capacidad de explicar y justificar las decisiones, esta falta de trazabilidad representa un desafío significativo. La imposibilidad de comprender plenamente cómo se ha llegado a un resultado limita la atribución de responsabilidad y debilita los mecanismos de control.

De este modo, la opacidad no es un problema meramente técnico, sino un factor estructural que incide directamente en la fragmentación de la responsabilidad en la guerra contemporánea, al introducir decisiones

críticas cuyo origen no puede ser claramente identificado ni plenamente explicado. Esta opacidad dificulta la supervisión efectiva de las decisiones y complica la reconstrucción posterior de los hechos cuando se produce un error.

Si un sistema clasifica erróneamente un objetivo militar o recomienda una acción incorrecta, puede resultar extremadamente difícil determinar si el problema se originó en los datos utilizados, en el diseño del algoritmo, en el proceso de entrenamiento o en la interpretación realizada por el operador humano. La falta de trazabilidad limita la rendición de cuentas y debilita los mecanismos tradicionales de responsabilidad.

6. El ecosistema tecnológico de defensa

La inteligencia artificial militar se desarrolla en un entorno caracterizado por la colaboración entre Estados, empresas tecnológicas y contratistas especializados.

Las grandes compañías del sector tecnológico desempeñan un papel fundamental debido a su capacidad para desarrollar modelos avanzados, gestionar infraestructuras de datos y proporcionar servicios esenciales para la defensa.

Estos procesos suelen desarrollarse en varias etapas: desde la definición de necesidades estratégicas y la elaboración de requisitos técnicos, hasta la licitación, adjudicación y ejecución contractual. A lo largo de este ciclo, intervienen múltiples actores —instituciones públicas, empresas tecnológicas, contratistas especializados y, en determinados contextos, representantes de intereses o lobbies— cuya participación está regulada, pero que desempeñan un papel relevante en la circulación de información, la definición de estándares y la identificación de soluciones disponibles.

En países como Estados Unidos, la actividad de lobbying forma parte de un marco legal establecido que exige transparencia y registro. No obstante, su existencia refleja una realidad estructural: el acceso a los procesos de contratación y a la información estratégica no es homogéneo. Las empresas con mayor capacidad técnica, recursos financieros y presencia institucional tienden a participar desde etapas tempranas del proceso, lo que les permite influir en la configuración de los requisitos y posicionarse ventajosamente en la fase de adjudicación.

El resultado no es necesariamente una distorsión ilegal del sistema, sino la consolidación de un entorno en el que el acceso, la información y la capacidad de influencia se distribuyen de manera desigual. De este modo, los procesos de contratación no solo seleccionan proveedores, sino que también reproducen y refuerzan una estructura de poder, en la que ciertos actores adquieren una posición privilegiada dentro del ecosistema tecnológico de defensa. En la era de la información, el poder ya no se mide únicamente por la fuerza de las armas, sino por la capacidad de configurar y controlar redes de información y decisión. La IA militar representa una extensión de este fenómeno: controlar los algoritmos y la infraestructura tecnológica no solo amplía las capacidades operativas, sino que también condiciona las opciones disponibles, tanto frente al adversario como dentro de la propia cadena de mando.

Esta situación genera una importante concentración de capacidades tecnológicas. El elevado coste económico y técnico necesario para competir en este ámbito restringe la participación a un número reducido de actores. Como consecuencia, los Estados desarrollan relaciones de dependencia respecto a determinados proveedores tecnológicos cuya infraestructura pasa a formar parte de los elementos estratégicos esenciales para la seguridad nacional.

6.1. Contratación pública y poder tecnológico

Los procesos de adquisición tecnológica en materia de defensa han evolucionado hacia modelos complejos de cooperación público-privada.

Los contratos actuales suelen abarcar no solo la adquisición de sistemas, sino también servicios de integración, mantenimiento, formación y acceso a infraestructuras de datos.

A lo largo de estos procedimientos participan numerosos actores con diferentes grados de influencia. Las empresas que disponen de mayores recursos financieros, capacidad técnica y presencia institucional suelen encontrarse en posiciones más favorables para intervenir en fases tempranas del proceso de contratación.

Este fenómeno contribuye a consolidar estructuras de poder tecnológico que condicionan tanto la capacidad operativa de los Estados como la distribución de responsabilidades dentro del ecosistema de defensa.

Los procesos de adquisición y desarrollo tecnológico en defensa han evolucionado hacia modelos complejos de colaboración público-privada que, aunque formalmente regulados, resultan en la práctica altamente técnicos, prolongados y difícilmente trazables en todas sus fases.

Los contratos ya no se limitan al suministro de hardware o software, sino que incluyen capacitación, integración de sistemas, acceso a datos y mantenimiento continuo, generando vínculos estratégicos de largo plazo entre los Estados y sus proveedores. En este contexto, los procesos de contratación dejan de ser un elemento meramente administrativo para convertirse en un espacio donde se configura poder estratégico. Esta configuración, a su vez, influye directamente en las dinámicas de dependencia tecnológica y en la creciente dificultad para delimitar responsabilidades en la toma de decisiones militares.

7. Derecho Internacional Humanitario y responsabilidad

El Derecho Internacional Humanitario establece las normas destinadas a limitar los efectos de los conflictos armados y proteger a las personas que no participan directamente en las hostilidades.

Sus principios fundamentales incluyen la distinción entre objetivos militares y población civil, la proporcionalidad en el uso de la fuerza y la obligación de adoptar precauciones para minimizar los daños incidentales.

El Derecho Internacional Humanitario (DIH), también denominado Derecho de los Conflictos Armados (LOAC), constituye el marco normativo que regula la conducción de las hostilidades y la protección de las personas que no participan directamente en los conflictos armados. Su base jurídica principal se encuentra en los Convenios de Ginebra de 1949 y sus Protocolos Adicionales de 1977, así como en el derecho internacional consuetudinario, sistematizado por el Comité Internacional de la Cruz Roja (ICRC). A ello se suma el régimen de responsabilidad penal individual establecido en el Estatuto de Roma de la Corte Penal Internacional (1998), que tipifica los crímenes de guerra y refuerza la obligación de rendición de cuentas por violaciones graves del derecho internacional humanitario.

Este sistema normativo se estructura sobre principios esenciales que no solo organizan la conducta en combate, sino que definen los límites jurídicos del uso de la fuerza: el principio de distinción, que obliga a diferenciar en todo momento entre combatientes y civiles (Protocolo Adicional I, artículo 48); el principio de proporcionalidad, que prohíbe ataques en los que el daño incidental a civiles sea excesivo en relación con la ventaja militar concreta y directa prevista (Protocolo Adicional I, artículo 51(5)(b)); y el principio de precaución en el ataque, que exige adoptar todas las medidas factibles para evitar o minimizar daños a la población civil (Protocolo Adicional I, artículo 57).

El sistema jurídico humanitario atribuye responsabilidad tanto a los Estados como a las personas que participan en la planificación, autorización o ejecución de actos ilícitos.

Asimismo, contempla la responsabilidad de mando cuando los superiores conocen o deberían conocer conductas ilícitas y no adoptan medidas para impedirlas o sancionarlas.

7.1. Inteligencia artificial y atribución de responsabilidad

La utilización de sistemas de inteligencia artificial no elimina las obligaciones jurídicas existentes. Los algoritmos carecen de personalidad jurídica y no pueden ser considerados sujetos responsables en el sentido del Derecho Internacional. Por tanto, la responsabilidad continúa recayendo sobre los Estados, los mandos militares y los individuos que intervienen en el proceso de toma de decisiones. Sin embargo, la creciente complejidad tecnológica dificulta la identificación precisa de los responsables cuando se producen errores o violaciones del Derecho Internacional Humanitario.

La regulación europea sobre inteligencia artificial clasifica determinadas aplicaciones como sistemas de alto riesgo debido a su potencial impacto sobre la seguridad, la integridad física y los derechos fundamentales. En estos casos se exigen mecanismos reforzados de supervisión humana, transparencia, trazabilidad y gestión del riesgo. En el ámbito militar, estas exigencias adquieren una relevancia especial debido a las posibles consecuencias letales de las decisiones automatizadas. Desde esta perspectiva, el principio de precaución obliga a identificar y mitigar los riesgos desde las primeras fases de diseño, desarrollo y despliegue de la tecnología.

7.2. Responsabilidad jurídica e inteligencia artificial en los conflictos armados

El Derecho Internacional Humanitario (DIH), también conocido como Derecho de los Conflictos Armados, constituye el conjunto de normas destinado a regular la conducción de las hostilidades y a proteger a las personas que no participan directamente en ellas. Su fundamento jurídico se encuentra principalmente en los Convenios de Ginebra de 1949, sus Protocolos Adicionales de 1977 y las normas consuetudinarias desarrolladas por la práctica internacional. A este marco se añade el Estatuto de Roma de la Corte Penal Internacional, que establece la responsabilidad penal individual por la comisión de crímenes internacionales, incluidos los crímenes de guerra.

El sistema jurídico humanitario se apoya en principios fundamentales como la distinción entre combatientes y población civil, la proporcionalidad en el uso de la fuerza y la obligación de adoptar precauciones para minimizar los daños incidentales. Estos principios delimitan jurídicamente el empleo legítimo de la fuerza armada y constituyen la base sobre la que se evalúa la legalidad de las operaciones militares.

La inteligencia artificial se ha convertido en una de las tecnologías más influyentes del siglo XXI. Su capacidad para procesar grandes volúmenes de información, identificar patrones complejos, generar predicciones y apoyar procesos de toma de decisiones ha transformado múltiples sectores de la actividad humana. No obstante, el impacto potencial de estas tecnologías no es uniforme. Algunos sistemas poseen una capacidad significativamente mayor para afectar derechos fundamentales, la seguridad pública o bienes jurídicos de especial protección, razón por la cual diversos instrumentos regulatorios han adoptado modelos diferenciados basados en el nivel de riesgo asociado a su utilización.

La aproximación regulatoria más relevante en esta materia se encuentra en el Reglamento de Inteligencia Artificial de la Unión Europea (AI Act), el cual establece un modelo escalonado de gestión del riesgo. Este instrumento parte de la premisa según la cual el nivel de intervención jurídica debe ser proporcional a los riesgos que cada sistema puede generar. En consecuencia, distingue entre sistemas de riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo.

Los sistemas de inteligencia artificial de alto riesgo ocupan una posición particularmente

relevante dentro de esta clasificación. Se trata de tecnologías cuya utilización puede afectar significativamente la vida, la integridad personal, la seguridad, los derechos fundamentales o el funcionamiento de infraestructuras críticas. Por esta razón, se encuentran sometidos a exigencias reforzadas de transparencia, supervisión humana, calidad de datos, trazabilidad y gestión del riesgo.

Desde una perspectiva funcional, los sistemas de alto riesgo suelen compartir varias características. En primer lugar, participan en procesos de toma de decisiones con consecuencias relevantes para las personas. En segundo lugar, operan en entornos donde los errores pueden producir daños de difícil reparación. Finalmente, su funcionamiento depende de modelos algorítmicos cuya complejidad dificulta, en ocasiones, la comprensión integral de los procesos que conducen a determinados resultados.

La estructura de responsabilidad prevista por el DIH opera en dos planos complementarios. Por una parte, los Estados responden internacionalmente por las acciones ilícitas cometidas por sus fuerzas armadas. Por otra, existe responsabilidad penal individual para quienes ordenan, ejecutan o permiten la comisión de violaciones graves del derecho de la guerra. Dentro de este esquema adquiere especial relevancia la responsabilidad de mando, según la cual los superiores pueden responder por los actos de sus subordinados cuando conocían o debían conocer la existencia de conductas ilícitas y no adoptaron medidas adecuadas para impedirlas o sancionarlas.

La incorporación de sistemas de inteligencia artificial a las operaciones militares introduce nuevos desafíos para la aplicación práctica de estas normas. Cuando algoritmos o sistemas semiautónomos participan en la identificación de objetivos, la evaluación de amenazas o la formulación de recomendaciones operativas, surgen dificultades relacionadas con la atribución de responsabilidad en caso de que se produzcan daños no previstos.

Desde el punto de vista jurídico, la inteligencia artificial no puede asumir responsabilidad propia, ya que los sistemas tecnológicos carecen de personalidad jurídica internacional. En consecuencia, la responsabilidad continúa recayendo sobre los Estados, los mandos militares y los responsables de la toma de decisiones. Sin embargo, la creciente dependencia de procesos automatizados dificulta la identificación precisa de los actores responsables dentro de cadenas de decisión cada vez más complejas.

Diversos autores han señalado que el Derecho Internacional Humanitario no prohíbe el uso de tecnologías autónomas o semiautónomas. No obstante, exige que las decisiones con consecuencias letales permanezcan bajo un nivel suficiente de control humano. Este requisito pretende garantizar que exista una valoración humana responsable en aquellas decisiones susceptibles de afectar a la vida y la integridad de las personas.

Por ello, el principal reto actual no radica en la inexistencia de normas jurídicas aplicables, sino en la dificultad de mantener mecanismos claros de atribución de responsabilidad en entornos operativos caracterizados por la intervención simultánea de factores humanos, organizativos y tecnológicos.

7.3. Sistemas de inteligencia artificial de alto riesgo

La inteligencia artificial se ha consolidado como una tecnología con capacidad para transformar profundamente múltiples ámbitos de la actividad humana. Sin embargo, no todos los sistemas presentan el mismo nivel de impacto potencial. Algunos pueden afectar de forma significativa a derechos fundamentales, a la seguridad pública o a bienes jurídicos especialmente protegidos, lo que ha llevado a desarrollar marcos regulatorios diferenciados en función del riesgo.

La referencia normativa más relevante en esta materia es el Reglamento de Inteligencia Artificial de la Unión Europea, que establece

una clasificación escalonada basada en el nivel de riesgo. Este modelo distingue entre sistemas de riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo, imponiendo obligaciones más estrictas a medida que aumenta la capacidad potencial de producir daños.

Los sistemas considerados de alto riesgo son aquellos que pueden afectar de manera significativa a la seguridad, la integridad física, la vida de las personas o el ejercicio de derechos fundamentales. Por este motivo, están sujetos a exigencias reforzadas relacionadas con la transparencia, la supervisión humana, la calidad de los datos utilizados, la trazabilidad de las decisiones y la gestión continua de riesgos.

Estos sistemas suelen intervenir en procesos de toma de decisiones con consecuencias relevantes, operan en entornos donde los errores pueden generar daños importantes y se basan en modelos algorítmicos cuya complejidad dificulta, en ocasiones, la comprensión completa de su funcionamiento interno.

La problemática adquiere una dimensión especialmente sensible cuando estas tecnologías se aplican al ámbito militar. La utilización de inteligencia artificial en tareas de vigilancia, reconocimiento, identificación de objetivos, análisis de inteligencia o apoyo a decisiones operativas genera riesgos que exceden las preocupaciones habituales presentes en otros sectores. El problema jurídico no se limita al potencial destructivo de las armas, sino que se extiende al propio proceso mediante el cual se adoptan decisiones relacionadas con el uso de la fuerza.

Una característica particularmente relevante es que los riesgos asociados a estos sistemas pueden originarse mucho antes de su utilización efectiva. El diseño de los algoritmos, la selección de datos de entrenamiento, los procesos de validación y las condiciones de despliegue influyen directamente en los resultados obtenidos durante su funcionamiento. Por ello, errores, sesgos o limitaciones incorporados en fases tempranas pueden proyectarse posteriormente sobre decisiones adoptadas en escenarios reales de conflicto.

Esta circunstancia obliga a replantear la gestión jurídica del riesgo. Si los peligros pueden identificarse desde las etapas iniciales de desarrollo tecnológico, también deben surgir desde ese momento obligaciones de prevención, control y supervisión.

El principio de precaución ocupa una posición central dentro del Derecho Internacional Humanitario. Su fundamento se encuentra en la obligación de adoptar todas las medidas factibles para evitar o minimizar los daños a la población civil y a los bienes protegidos durante las operaciones militares.

A diferencia de los mecanismos de responsabilidad que actúan una vez producido el daño, las obligaciones de precaución tienen una finalidad preventiva. Su objetivo consiste en identificar riesgos potenciales antes de que se materialicen y adoptar medidas destinadas a reducir su probabilidad o impacto.

Desde esta perspectiva, la gestión del riesgo asociado a la inteligencia artificial puede considerarse una manifestación contemporánea del principio de precaución. La identificación temprana de riesgos durante las fases de diseño, entrenamiento, validación y despliegue genera la obligación de implementar mecanismos de mitigación adecuados.

Entre estas medidas destacan la supervisión humana permanente, la realización de auditorías técnicas, la evaluación de la calidad de los datos utilizados y la monitorización continua del funcionamiento de los sistemas. Estas actuaciones no constituyen únicamente buenas prácticas tecnológicas, sino exigencias derivadas de los deberes jurídicos de prevención presentes en el Derecho Internacional Humanitario.

En consecuencia, cuanto mayor sea la capacidad potencial de una tecnología para producir consecuencias graves, mayor deberá

ser el nivel de diligencia exigido a quienes intervienen en su diseño, desarrollo y utilización.

8. Conclusiones

La incorporación de la inteligencia artificial al ámbito militar está transformando profundamente la naturaleza de los conflictos armados contemporáneos. La automatización, la rapidez en el procesamiento de información y la capacidad de apoyo a la toma de decisiones ofrecen importantes ventajas operativas, pero al mismo tiempo generan una creciente fragmentación de la responsabilidad.

La inteligencia artificial está transformando profundamente la forma en que se desarrollan los conflictos armados contemporáneos. Aunque estas tecnologías ofrecen importantes ventajas operativas, también generan nuevos desafíos relacionados con la transparencia, el control humano y la atribución de responsabilidades.

La creciente participación de sistemas automatizados en la toma de decisiones militares favorece procesos de fragmentación y dilución de la responsabilidad que dificultan la rendición de cuentas.

A pesar de ello, el Derecho Internacional Humanitario continúa proporcionando un marco normativo válido para exigir responsabilidades a los actores humanos e institucionales implicados. La cuestión central no es si existe responsabilidad, sino cómo identificarla adecuadamente en entornos caracterizados por una compleja interacción entre personas, organizaciones y sistemas tecnológicos.

Por ello, el desarrollo futuro de la inteligencia artificial en el ámbito militar deberá ir acompañado de mecanismos eficaces de supervisión, transparencia y control que garanticen la preservación de los principios fundamentales del Derecho Internacional y la protección de los derechos humanos.

La Unión Europea ha desarrollado un marco regulatorio que busca compatibilizar la innovación tecnológica con la protección de valores fundamentales como la dignidad humana, los derechos fundamentales, el Estado de Derecho y la responsabilidad democrática. Este conjunto normativo condiciona no solo el desarrollo y comercialización de tecnologías de inteligencia artificial, sino también la forma en que pueden ser utilizadas por los poderes públicos.

La expansión de sistemas automatizados plantea una tensión constante entre la búsqueda de eficiencia y la necesidad de preservar el control humano sobre decisiones que afectan a derechos fundamentales. Las decisiones susceptibles de producir consecuencias graves para las personas deben seguir siendo objeto de valoración humana, garantizando la existencia de responsabilidad, supervisión y mecanismos de revisión.

La inteligencia artificial no elimina la responsabilidad jurídica, pero sí modifica la manera en que esta se distribuye y se identifica. La complejidad creciente de las cadenas de decisión tecnológicamente asistidas dificulta la atribución de responsabilidades y exige el desarrollo de mecanismos institucionales capaces de preservar la rendición de cuentas.

Finalmente, aunque actualmente no exista un régimen internacional específico y universal para regular la inteligencia artificial militar, los principios generales del Derecho Internacional Humanitario, las obligaciones derivadas de los derechos humanos y los deberes de prevención y precaución proporcionan una base jurídica suficiente para exigir medidas destinadas a identificar, controlar y reducir los riesgos asociados al empleo de estas tecnologías.

Referencias

ALONSO SALGADO, Cristina (2021). Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad. *IUS ET SCIENTIA*. Vol. 7 Nº 1. pp. 25 - 36

https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.03

BALCELLS, Marc. (2020). Luces y sombras del uso de la inteligencia artificial en el sistema de Justicia penal. En A. Cerrillo I Martínez y M. Peguera Poch (Eds.). Retos jurídicos de la inteligencia artificial. Cizur Menor (Navarra): Aranzadi.

BRAYNE, Sarah. (2017). Big Data Surveillance: The Case of Policing. American Sociological Review, 82(5), 977-1008. https://doi.org/10.1177/0003122417725865

BUOLAMWINI, Joy., & GEBRU, Timnit. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Science Advances, 4(1), eaas8576. Proceedings of Machine Learning Research. 81:77-91 Available from https://proceedings.mlr.press/v81/buolamwini18a.html

CHESNEY, Robert., & CITRON, Danielle. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs, 98(1), 147-155. Available at: https://scholarship.law.bu.edu/shorter_works/76

CHÉN, Oliver. (2022). Uniting Machine Intelligence, Brain and Behavioural Sciences to Assist Criminal Justice. arXiv preprint arXiv:2207.01511. https://doi.org/10.48550/arXiv.2207.01511

El Derecho. com (2024). Responsabilidad penal y la inteligencia artificial en España. Editorial Jurídica El Derecho.

El País. (2024). El caso de deepfakes en España reabre el debate sobre la regulación de la IA. Recuperado de https://www.elpais.com

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM/2021/206 final.

EL KADY, Ramy. (2025). "Challenges of Criminal Liability for Artificial Intelligence Systems." In Exploration of AI in Contemporary Legal Systems, edited by Halim Bajraktari, 1-42. Hershey, PA: IGI Global,. https://doi.org/10.4018/979-8-3693-7205-0.ch001

GUTHRIE FERGUSON, Andrew. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: NYU Press. https://doi.org/10.18574/nyu/9781479854608.001.0001

GARVIE, Clare., BEDOYA, Alvaro. & FRANKLE, Jonathan. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/

XAVIER JANUÁRIO, Tulio. Felippe. (2023). Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales: Un análisis de sus aspectos materiales y procesales . *Estudios Penales Y Criminológicos,* 44(Ext.), 1-39. https://doi.org/10.15304/epc.44.8902

GRIGORE, Andrea. Elena. (2022). Derechos humanos e inteligencia artificial. *IUS ET SCIENTIA*, 8(1), 164–175. https://doi.org/10.12795/IETSCIENTIA.2022.i01.10

HERNÁNDEZ GIMÉNEZ, María. (2019). Inteligencia artificial y Derecho penal.. *Actualidad Jurídica Iberoamericana,* 10(bis), 792-843. https://revista-aji.com/wp-content/uploads/2019/06/792-843.pdf

HILDEBRANDT, Mirelle. (2022). Law for Computer Scientists and Other Folk. Oxford University Press. , https://doi.org/10.1093/oso/9780198860877.001.0001

CRAWFORD, Kate. (2022). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Perspectives on Science and Christian Faith. https://doi.org/10.56315/PSCF3-22Crawford

MANDALAPU, Varun., ELLURI, Lavanya., VYAS, Piyush., & ROY, Nirmalya. (2023). Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future. https://doi.org/10.48550/arXiv.2303.16310 https://doi.org/10.1109/ACCESS.2023.3286344

MORÁN ESPINOSA, Alejandra. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista del Instituto de Ciencias Jurídicas de Puebla*, México. vol. 15, No. 48. https://doi.org/10.35487/rius.v15i48.2021.706

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2021). Los riesgos de la inteligencia artificial para la privacidad exigen una acción urgente. Recuperado de https://goo.su/TegmwK

PAGALLO, Ugo (2013). The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Imprint: Springer. https://doi.org/10.1007/978-94-007-6564-1

PASQUALE, Frank. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

RICAURTE, Paola. (2024). Las grandes compañías tecnológicas son aliadas de gobiernos autoritarios. El País. Recuperado de https://elpais.com/america/lideresas-de-latinoamerica/2024-10-16/paola-ricaurte-las-grandes-companias-tecnologicas-son-aliadas-de-gobiernos-autoritarios.html

SCANTAMBURLO, Teresa, Andrew CHARLESWORTH, & Nello CRISTIANINI, (2019). Machine Decisions and Human Consequences, in Karen Yeung, and Martin Lodge (eds), Algorithmic Regulation. Oxford Academic. arXiv https://doi.org/10.48550/arXiv.1811.06747

THAMER NAJM, Abdullah Abbas., HAMEED, Raed., AKRAM KADHIM, Ali., & HASHIM QASIM, Namer. (2024). Artificial intelligence and criminal liability: exploring the legal implications of aIenabled crimes. *ENCUENTROS. Revista de Ciencias Humanas, Teoría Social Y Pensamiento Crítico.,* 22 140-159. https://doi.org/10.5281/zenodo.13386675

UNIÓN EUROPEA. 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 (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119, 4 mayo 2016.

UNIÓN EUROPEA. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). Diario Oficial de la Unión Europea, 2024.

WACHTER, Sandra., MITTELSTADT, Brent., & RUSSELL, Chris. (2018) "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", Harvard Journal of Law and Technology. 31 (2) 841-887. https://doi.org/10.2139/ssrn.3063289

WACHTER, Sandra., MITTELSTADT, Brent., & RUSSELL, Chris. (2021). Why fairness cannot be automated: Bridging the gap between AI and human rights law. Computer Law & Security Review, 43(4), 34-55. https://doi.org/10.1016/j.clsr.2021.105567