

DEL CÓDIGO AL COMANDO: LA RESPONSABILIDAD JURÍDICA EN LA GUERRA IMPULSADA POR LA IA

XIMENA MOLINERO MARTÍNEZ

Máster en Geopolítica y Estudios Estratégicos,
Universidad Carlos III de Madrid

La Inteligencia Artificial (IA) está transformando la guerra moderna. La creación de nuevos sistemas armamentísticos y de defensa automatizados –en concreto, la tecnología que integra software de detección automática de objetivos– es ya una realidad que altera el papel que desempeñará el componente humano en futuros conflictos armados. A esto se refería el secretario general de la ONU, António Guterres, cuando afirmaba en 2024 que: «la capacidad de acción del ser humano debe preservarse a toda costa». Si bien el uso de la Inteligencia Artificial en la guerra está regulado de manera indirecta por el derecho internacional, aún existen importantes vacíos legales y éticos que deben debatirse. Una primera premisa es que la tecnología, de por sí, no es ni buena ni mala. Lo que la empuja en un sentido u otro –por lo menos hasta ahora–, es el componente humano necesario para el funcionamiento de las armas convencionales, lo que hace que sea bastante fácil reclamar la responsabilidad legal en los casos en los que lo merita. Sin embargo, el momento actual nos plantea nuevos dilemas: ¿cómo podrá el derecho internacional determinar la responsabilidad jurídica por el uso indebido, accidental o por un error de calibración de un arma autónoma? ¿Sobre quién debería recaer la responsabilidad de estos malos usos: sobre la persona que programó el arma, el comandante militar... o quizá sobre el Estado? Estos son algunos de los interrogantes que cuestionan la capacidad del derecho internacional para regular estas cuestiones. Y con vistas a ello, el presente artículo pretende explorar estas cuestiones sobre la base de los marcos jurídicos ya existentes.

El primer malentendido que conviene aclarar es la creencia de que la Inteligencia Artificial es una tecnología nueva que no tiene un marco jurídico al que responder. Esto no es así, y aunque el marco actual pueda resultar insuficiente en algunos aspectos, no hay necesidad de reinventar la rueda. Reconocer los precedentes que aplican y las leyes ya existentes es el primer paso para acotar los vacíos legales. Como ha señalado Pierrick Devidal, asesor político del Comité Internacional de la Cruz Roja, en su artículo «Trying to square the circle: The ICRC AI policy» (*Humanitarian Law & Policy*, 2024), la Inteligencia Artificial –al igual que cualquier innovación tecnológica– debe someterse a un marco normativo ya existente. Este incluye el derecho internacional de los derechos humanos, el derecho internacional humanitario, la legislación internacional sobre protección de datos, la responsabilidad por productos defectuosos, la propiedad intelectual y la ética de la innovación.

Una de las vías más eficaces para evitar el uso indebido de estas tecnologías es garantizar que todo nuevo sistema de IA cumpla con estas normativas. Para ello, resulta imprescindible incorporar el vocabulario y los conceptos propios de la Inteligencia Artificial al lenguaje de quienes elaboran políticas públicas. Solo así podrán tomarse decisiones informadas y negociarse marcos regulatorios adecuados. Esta labor no solo es una responsabilidad directa de los legisladores, sino que también influirá en cómo el derecho internacional regulará las futuras innovaciones en este ámbito.

Así como es fundamental reconocer que ya existe un marco legal que regula –aunque sea parcialmente– la Inteligencia Artificial, también lo es aceptar que dicho marco resulta

insuficiente. La legislación suele ir por detrás de la innovación tecnológica, y la IA no es una excepción. Uno de los problemas más importantes en relación con el uso de la IA en el sector militar es que, por muy bien programada que esté, la Inteligencia Artificial siempre carecerá de virtudes como el coraje, la responsabilidad y el sentido del deber, que son valores arraigados fundamentalmente en la capacidad de juicio humana. El riesgo de restar importancia a estas virtudes puede debilitar el elemento humano de la toma de decisiones morales. Por otra parte, la dependencia excesiva de estos sistemas automatizados puede conducir a la pérdida de cualificación (*deskilling*) de las fuerzas armadas si no se enfoca correctamente. Si no se gestiona adecuadamente, la IA podría convertirse en un sustituto de habilidades esenciales, en lugar de un complemento. Por ello, es crucial garantizar que el personal militar mantenga su preparación y eficacia, independientemente del uso de Inteligencia Artificial. Es imperativo que las fuerzas armadas no caigan en el «sesgo de automatización», que según Wen Zhou –asesor jurídico del Comité Internacional de la Cruz Roja–, radica en la creencia de que tecnologías –como la IA– tienen capacidades analíticas superiores a las de los humanos. Esto aumenta la probabilidad de que los humanos pasen por alto las anomalías que pueda presentar el sistema y también crea nuevos riesgos para la seguridad debido a la dependencia excesiva de los sistemas de Inteligencia Artificial por parte de las fuerzas armadas.

Además, el citado sesgo de la automatización puede erosionar la capacidad de los mandos para asumir la responsabilidad moral de sus decisiones, conduciendo en última instancia, a lo que la filósofa de la tecnología Shannon Vallor define como

La Inteligencia Artificial –al igual que cualquier innovación tecnológica– debe someterse a un marco normativo ya existente

una «pérdida de capacidad moral» (*moral deskilling*) de las fuerzas armadas, que es independiente de sus aptitudes físicas. Si la capacidad de acción del ser humano en relación con las armas autónomas queda reducida a tan solo veinte segundos para decidir si el objetivo es correcto o no, el margen de error aumentará. La deshumanización del objetivo conducirá finalmente a la desvalorización de la vida humana, lo que planteará la cuestión de quién es responsa-

ble de las muertes accidentales que cause el sistema de armas. Aunque existe una cadena de mando para decidir la responsabilidad militar sobre las acciones, los límites se difuminan respecto a quién es responsable de los errores, si el comandante que da las órdenes, el soldado que aprieta el gatillo o el programador del algoritmo.

Otro reto que aumenta parejo al uso de la IA en los sistemas militares es la regulación de la información utilizada para entrenar este tipo de armas. Tal y como ha señalado en numerosos estudios el profesor Gideon Christian, los sistemas de reconocimiento facial basados en IA presentan sesgos significativos. Estos sesgos pueden derivar en resultados discriminatorios no deseados que vulneran el derecho internacional, comprometen los principios de rendición de cuentas y afectan directamente a la ética en la toma de decisiones militares. La tecnología no es neutral: se moldea según los datos y criterios que introducen sus programadores. Esto abre la puerta a que los sistemas de IA militar puedan ser deliberadamente entrenados bajo ciertos prejuicios raciales o de género contra una determinada población o minoría. Tal y como menciona el académico Jamie Allinson en su artículo «Necropolitics of Drones» (*International Political Sociology*, junio de 2015), existen informes acerca de drones que han

dirigido ataques contra determinadas personas en función de su aparente afiliación a un grupo étnico como resultado de una programación sesgada. En caso de que se demuestre que uno de estos sistemas se ha entrenado con determinados sesgos de forma intencionada, ¿quién será responsable de las muertes humanas que pueda causar? Y si damos por hecho que el soldado que da luz verde al ataque de un arma autónoma, puede desconocer que existen sesgos en su programación, ¿se puede juzgar entonces a los programadores que han codificado estos sistemas? Si la responsabilidad recae íntegramente en los estados, es necesario establecer mecanismos claros que vinculen responsabilidad de estas acciones con las figuras gubernamentales y militares. De lo contrario, existe el riesgo de que la culpa recaiga exclusivamente sobre individuos concretos, como el programador que estaba a cargo del proyecto.

Aunque existe una cadena de mando para decidir la responsabilidad militar sobre las acciones, los límites se difuminan respecto a quién es responsable de los errores

En conclusión, el marco jurídico que rodea a la IA sigue siendo incompleto e insuficiente para dar una respuesta definitiva a este tipo de situaciones, especialmente en el ámbito militar. Existen sin embargo, múltiples medidas que la comunidad internacional puede –y seguramente debería– adoptar para garantizar que estas tecnologías se utilicen en beneficio de la humanidad. El primer paso es reconocer el marco jurídico existente que ayuda a regular estas innovaciones y garantizar que cualquier nuevo sistema cumpla todos los requisitos legales antes de lanzarlo o probarlo en un escenario real. El segundo paso consiste en analizar las deficiencias de la legislación vigente y determinar en qué medida se debe responsabilizar a los programadores de estas armas. Para ello, probablemente será necesaria la colaboración entre profesionales de diversas disciplinas y responsables políticos con el fin de alcanzar acuerdos aceptables. Y sin duda, el interés de los estados también es un factor que influirá en los resultados del debate. Por último, el reto más importante es garantizar por todos los medios que se preserve la capacidad de acción del ser humano, cuya supervisión es imprescindible para garantizar un uso ético de la IA en el ámbito militar. Solo así podrá establecerse una cadena de responsabilidad legal por las consecuencias que estas tecnologías puedan tener en una guerra real. La Inteligencia Artificial no puede ser juzgada en un tribunal, por lo que la responsabilidad debe recaer en los seres humanos que hay detrás de ella. De lo contrario, sabremos que hemos perdido el control sobre la tecnología.

