Mariella Berra

Regolare l'intelligenza artificiale rinforzare la società

Mariarosaria Taddeo, *Codice di guerra. Etica dell'intelligenza artificiale nella difesa*, Cortina Edizioni, Milano, 2025, pp. 312.

Parole chiave
Etica, intelligenza artificiale, difesa, *robot killer*, *cyberware*, armi autonome, *governance*

Mariella Berra, docente del Dipartimento CPS dell'Università di Torino, si è occupata di innovazione tecnologica e digitale, nuovi modelli produttivi e di scambio socio economici e di donne e nuove tecnologie nella società 4.0. Sui temi delle trasformazioni del lavoro, della innovazione digitale ha al suo attivo fra libri e articoli in riviste italiane e straniere 150 pubblicazioni (mariella.berra@unito.it)

Nello scenario di tensione geopolitica crescente e di proposte di riarmo degli Stati europei, questo libro solleva problematiche e richieste sempre più urgenti. La domanda che pone l'autrice, docente di Digital Ethics e Defence Technology all'Università di Oxford, è se sia possibile affidarsi all'uso dell'intelligenza artificiale nella difesa senza sacrificare i princìpi umanitari, etici e di responsabilità su cui si basano le democrazie liberali. Le implicazioni dell'uso della intelligenza artificiale nell'ambito difensivo coprono

ISSN: 2784-8272 (print) | DOI: 10.53145/indiscipline.v7i1
www.morlacchilibri.com/universitypress/indiscipline

un ampio raggio di azione che non riguarda solo le guerre, ma i processi decisionali, le modalità di acquisire dati, informazioni, le tattiche, le strategie difensive e l'intera organizzazione della difesa. Precisa, infatti, l'autrice come il titolo della versione italiana potrebbe fare supporre che il libro non tratti dell'etica della intelligenza artificiale nella guerra e nella organizzazione degli affari militari, del rafforzamento e delle capacita di difesa degli Stati. L'espressione Codice di guerra della pubblicazione italiana, a due anni di distanza da quella inglese, richiama anche la recrudescenza della guerra russo-ucraina e l'offensiva israeliana nella striscia di Gaza, dove si è ricorsi per la prima volta all'uso di armi autonome.

L'attenzione è rivolta alle implicazioni concettuali ed etiche dei processi di digitalizzazione crescenti, in particolare a un uso non regolato e controllato dell'intelligenza artificiale dove oggi spesso si crea una collisione fra diritto internazionale e democrazia. Infatti, l'adozione dell'intelligenza artificiale nella difesa senza un fondamento etico chiaro e condiviso aumenterebbe le probabilità che logiche disumanizzanti, staccate dal controllo umano, ma fortemente dipendenti da interessi di parte, guidino le guerre del futuro. L'etica costituisce, dunque, un principio necessario per governare la nuova trasformazione digitale e stabilire i limiti da non superare per una migliore convivenza internazionale e per il bene degli individui, della società e dell'ambiente. L'autrice precisa come non si tratti solamente di fissare divieti nell'utilizzo dell'intelligenza artificiale, ma di considerarne i rischi e le opportunità. L'introduzione dell'intelligenza artificiale, infatti, può supportare il ragionamento umano incrementando la consapevolezza della situazione, la conoscenza del contesto e facilitando il processo decisionale. Potrebbe anche migliorare il modo in cui si esercita la violenza se adeguatamente regolata e programmata. Vanno, quindi, considerate non solo le modalità di azione di queste tecnologie, ma occorre anche intervenire e guidarne i processi di progettazione e di uso.

Il libro, risultato di una ricerca ultradecennale, articolato in nove capitoli scritti con lessico tecnico solo quando strettamente

necessario, è agile e non presenta ostacoli alla piena comprensione non solo per gli specialisti, ma anche per i lettori attenti e curiosi. Si rivolge a un pubblico ampio e trasversale, dai sostenitori ottimisti o ottimisti interessati che individuano nella regolamentazione etica un ostacolo allo sviluppo dell'intelligenza artificiale, ai critici che si oppongono al suo uso nella difesa; dagli scienziati ai decisori pubblici e ai cittadini. La guerra digitale, come è noto, è profondamente diversa da quella tradizionale: con l'uso delle nuove tecnologie, operazioni conflittuali e forza non sono più necessariamente legate. Si viene così a infrangere quel principio di proporzionalità tra conflitto e forza, cardine della teoria della guerra giusta. È questo, come è noto, un consolidato concetto etico-giuridico, base del diritto internazionale e del diritto internazionale umanitario che ha stabilito i criteri rigorosi (autorità legittima, giusta causa, giusti mezzi) secondo i quali un conflitto armato è moralmente e legalmente giustificabile. Di conseguenza, l'uso dell'intelligenza artificiale nella difesa potrebbe, grazie a un'abile distribuzione di infrazioni tattiche, determinare una erosione e una progressiva obsolescenza del diritto internazionale. Si sottolinea, quindi, l'urgenza di stabilire con chiarezza i limiti normativi, che segnino i confini entro i quali l'intelligenza artificiale può operare e ampliare e riaggiornare i princìpi del diritto umanitario internazionale, in modo da estenderne l'applicazione anche alle tecnologie emergenti. La conclusione dell'autrice è il rischio che l'altra faccia del progresso tecnologico diventi uno strumento di involuzione giuridica e/o di decadenza morale.

I primi tre capitoli ci guidano nella conoscenza dell'etica della intelligenza artificiale e delle sue regole; dei documenti che delineano i criteri guida per uno sviluppo responsabile dell'intelligenza artificiale nel suo ciclo di vita: progettazione, sviluppo e uso sono abbastanza recenti. Risalgono al 2023 e sono il DOD, promosso dal Ministero della Difesa degli Stati Uniti, oggi Ministero della Guerra; il MOD promosso dal Ministero della difesa della Gran Bretagna; il terzo promosso dalla Nato. Il MOD stabilisce che l'uso deve essere centrato sul rispetto degli esseri umani; quello della

Nato sul principio di governabilità; il DOD sul principio di legalità. E proprio al rapporto DOD, considerato il testo più completo, che confronta i princìpi etici base di applicazione dell'intelligenza artificiale in generale e quelli specifici alla difesa, l'autrice fa riferimento. Ne descrive cinque: usi giustificati e ridefinibili; sistemi e processi giusti e trasparenti; responsabilità morale umana; controllo umano significativo; sistemi di intelligenza artificiale affidabili.

Affidabilità e spiegabilità, quest'ultima ancora in forte discussione, sono i requisiti che possono offrire ai decisori la possibilità di giustificare e rendere trasparenti le decisioni adottate. Riguardano la trasparenza del sistema, le competenze degli analisti, i problemi di raccolta, la lettura e l'interpretazione dei dati, gli elementi in grado di consentire l'impiego e la vigilanza umana su tutto il percorso di creazione e applicazione dell'intelligenza artificiale.

Il libro prosegue considerando tre ambiti di applicazione dell'intelligenza artificiale: il supporto alle funzioni strategiche; l'impiego in conflitti non cinetici (in particolare il cyberspazio); l'integrazione in sistemi d'arma autonomi. L'obiettivo del libro, chiarisce l'autrice, non è offrire una tassonomia delle tecnologie che usano l'intelligenza artificiale, ma indicare criteri per identificare i problemi etici collegati ai differenti impieghi dell'intelligenza artificiale nella difesa. Il primo si riferisce a operazioni di difesa e attacco, che rimangono al di sotto della soglia cinetica. Riguarda prevalentemente l'intelligenza aumentata e la logistica predittiva. Il secondo concerne l'impiego di strumenti digitali e informatici per ottenere effetti strategici (spionaggio, sabotaggio, disinformazione, interruzione di infrastrutture) senza usare armi fisiche, combattendo specialmente nel cyberspazio. Internet e le reti, come è recentemente successo in Ucraina, vengono utilizzate come un nuovo teatro di guerra, invisibile, ma potente.

Il terzo e più allarmante capitolo riguarda i sistemi d'arma autonomi, gli AWS (Autonomous War System) e le LAWS (Lethal Autonomous War System). Sono questi ultimi sistemi d'arma autonomi e letali in grado non solo di raggiungere un obiettivo, ma di modificare il proprio stato interno

a seconda dell'obiettivo da colpire. Sono rappresentati dai robot killer, protagonisti di una guerra disumana, impegnati con successo a Gaza, la prima guerra robotica della storia, come orgogliosamente la definisce Yaron Sarig, responsabile delle ricerche tecnologiche del Ministero della Difesa israeliano. In questi casi, considerazioni strategiche politiche ed etiche nel regolamentare i limiti e i livelli di tecnologia raggiungibili stentano a definire un quadro normativo comune e adeguato. È molto complicato pervenire a un accordo fra diversi Paesi e stabilire un controllo, in quanto queste tecnologie spesso dipendono dalle modalità di impiego, dal sistema adottato e dalle caratteristiche del livello operativo. In alcune tabelle, Taddeo riporta ben 12 definizioni di AWS e LAWS formulate da diversi Stati e organizzazioni internazionali. Senza un protocollo comune, tenere conto e regolare i problemi etici e giuridici che derivano dall'uso di sistemi di armi autonomi è quasi impossibile. Nelle conclusioni, realisticamente l'autrice si domanda se un futuro digitale più sostenibile e necessario potrebbe essere ancora possibile. *Si vis pacem para bellum* sembra essere la massima che sottolinea come l'uso della forza da parte degli Stati più potenti stia diventando una nuova normalità nel contesto geopolitico attuale, che vede crescere il peso nelle relazioni internazionali della *gunboat diplomacy*. Taddeo, richiamando quanto scriveva nel 2006 il filosofo Michael Walzer, "dalle limitazioni della guerra che germogliano i semi della pace", sottolinea l'impegno a ripristinare il controllo umano e a regolamentare l'uso. Diventa improrogabile costruire un sistema di governo multilivello dell'intelligenza artificiale, che integri visioni giuridiche, filosofiche e democratiche e far crescere il livello di conoscenza e consapevolezza nell'opinione pubblica.

La domanda che si pone chi scrive riguarda il futuro dell'applicazione dell'intelligenza artificiale nella difesa e anche nell'ambito sociale, qualora lo sviluppo dell'innovazione venga lasciato prevalentemente nelle mani dei produttori di tecnologia, portatori di un progetto tecno-politico che forse sottovaluta il ruolo degli esseri umani come agenti moralmente responsabili degli usi e degli esiti dei sistemi di innovazione.