

Difesa Armi autonome, cyberattacchi, furti di dati: l'analisi di Mariarosaria Taddeo per l'editore Cortina

Intelligenza artificiale e guerra

La necessità di un codice etico

di **Daniele Manca**

La guerra, le guerre sono tornate a essere drammaticamente al centro delle nostre vite. Potrebbe apparire un esercizio superfluo occuparsi di etica dell'intelligenza artificiale nella difesa quando questa tecnologia viene usata in modo massiccio in conflitti che di per se stessi spesso sono conseguenza della violazione di regole consolidate. La domanda se l'è fatta anche Mariarosaria Taddeo a conclusione del suo lavoro diventato un libro: *Codice di guerra*, in uscita per Raffaello Cortina editore il prossimo 26 agosto. La versione inglese, come racconta l'autrice, allieva di Luciano Floridi e docente di Digital Ethics and Defence Technologies all'Università di Oxford, l'ha chiusa a due anni dall'inizio dell'invasione russa in Ucraina e a pochi mesi dal nuovo conflitto a Gaza. Ma il suo libro è la testimonianza che è proprio nel fuoco di eventi scatenati da chi non vuol rispettare né la tradizione lunga dell'etica militare tantomeno la Teoria della guerra giusta, che ci si deve sforzare di ancorare la propria azione e riflessione alle regole.

L'orrore di fronte alle conseguenze dei conflitti non può e non deve paralizzarci nel tentare di mantenere quell'impegno a evitare la guerra e a «preservare un residuo di moralità e liceità quando questa diventa ineluttabile», scrive Taddeo. Richiamandosi e citando uno dei maggiori filosofi mondiali anche in questo campo, Michael Walzer, che nel 2006 scriveva «è dalle limitazioni della guerra che germogliano i semi della pace». A maggior ragione quando ci sono tecnologie che se utilizzate forzano quasi automaticamente principi come quelli contenuti nel diritto umanitario internazionale.

È già accaduto in passato. L'uso di armi nucleari «ha annullato la distinzione tra combattenti e non combattenti». Nella Seconda guerra mondiale è cioè venuto

meno il principio di discriminazione che pure fino a quel momento era alla base della Teoria della Guerra Giusta. L'utilizzo della Intelligenza artificiale (IA) impone inoltre autentici salti concettuali. Non solo perché le atrocità delle quali siamo capaci e alle quali abbiamo assistito e stiamo assistendo dovrebbero imporlo, ma anche perché «considerando che l'IA è progettata per massimizzare (e persino superare) le capacità umane, l'urgenza di un'analisi etica che ne guidi l'uso nella difesa dovrebbe apparire evidente a tutti».

Prima della rivoluzione digitale si è tentato di regolare la guerra attraverso il mettere, o provare a mettere sotto controllo la forza. Ma con le nuove tecnologie le operazioni conflittuali non sono state necessariamente legate all'uso della forza. Si è resa necessaria la distinzione tra attacchi «cinetici» tesi a procurare danni a persone e cose e «non cinetici». Allargando quindi il campo di battaglia a organizzazioni che prima non erano state responsabili della loro difesa da attacchi. Già nel passato attraverso approcci basati sull'analogia si era provato a utilizzare il quadro di governo per i conflitti armati anche nel caso di *cyberwarfare* (Il Manuale di Tallinn del 2017 della Nato).

Ma non è in discussione il fatto che «cyberattacchi che hanno gli stessi effetti o effetti simili a un attacco cinetico vanno trattati come tali». Quanto il come considerare quegli atti che creano interruzioni di servizio, accessi non legittimi ai dati e via dicendo. Basti pensare agli attacchi digitali che hanno interessato le infrastrutture ucraine prima dell'invasione russa. Gli ultimi anni hanno visto numerosi esempi di questo tipo. Dall'attacco russo a Estonia e Georgia, a quelli all'Iran tramite Stuxnet o quelli più recenti a Paesi europei e alle loro infrastrutture sempre all'indomani dell'attacco «cinetico» a Kiev e all'Ucraina.

C'è poi il grande capitolo dei sistemi d'arma autonomi (AWS nell'acronimo anglosassone). Riuscire ad arrivare a una definizione condivisa di questi sistemi,

oltre agli AWS anche i LAWS (sistemi d'arma autonomi e letali), è opera ardua. In alcune tabelle Taddeo riporta ben 12 definizioni di AWS e LAWS formulate da diversi Stati e organizzazioni internazionali. Con molti Stati che si sono detti preoccupati proprio per l'utilizzo di questi sistemi. Ma dove si ferma il concetto di autonomia? Senza condivisioni di questo tipo arrivare a parlare di sistemi d'arma autonomi e quindi affrontare problemi etici e giuridici è quasi impossibile.

È per questo che Taddeo si spinge a fornire raccomandazioni, basate su definizioni condivise di «controllo umano» per esempio. Il tentativo meri-

torio è quello di fornire «un contributo concreto a quanti, tra fornitori di tecnologia e le organizzazioni della difesa si impegnano» nell'operare in direzione dell'assunzione di responsabilità per evitare che queste tecnologie siano un mero strumento di guerra. Guerra che è il male assoluto, e se l'aggressione di uno Stato a un altro Stato o popolo è ingiustificabile, il difendersi è un diritto innegabile. Ma si deve evitare che ad atrocità si aggiunga atrocità, dimenticando quel principio di umanità che è uno dei valori fondanti delle nostre democrazie liberali.

© RIPRODUZIONE RISERVATA

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

074898

Incontri



● Il saggio
*Codice
di guerra. Etica
dell'intelligenza
artificiale
nella difesa*,
di Mariarosaria
Taddeo,
uscirà martedì
26 agosto
da Raffaello
Cortina editore
(pp. 320, € 25).
Taddeo
è docente
di Digital Ethics
and Defence
Technologies
all'Università
di Oxford

● L'autrice
presenta il libro
il 30 agosto
al Festival
della Mente
di Sarzana
(Teatro
degli Impavidi,
ore 9.45);
l'11 settembre
al Festival della
Comunicazione
di Camogli
(Terrazza della
Comunicazio-
ne, ore 22);
il 18 settembre
a Pordenone-
legge (Arena
Europa, ore 11)



Ai Weiwei (1957), *L'ultimo soldato Usa lascia l'Afghanistan* (2022), in mostra alla Faurischou Foundation, New York, fino allo scorso febbraio (Ansa)

