

Le armi autonome e intelligenti: fra effetti collaterali e mancanze di regole d'ingaggio. Una prospettiva informatico-giuridica e giusfilosofica

di
Casimiro Coniglione*

Sommario: 1. Introduzione alle armi LAWS, al concetto di autonomia nei sistemi e di agente *software* – 2. Alcune tipologie (terra-mare) di armi LAWS e il caso specifico del drone – 3. Le difficoltà sull'imputazione delle responsabilità: tra fiducia e affidamento negli algoritmi – 4. Riflessioni conclusive sull'effettività del diritto e sull'etica militare

1. Introduzione alle armi LAWS, al concetto di autonomia nei sistemi e di agente *software*

Q: Posso dire che faccio più danni io con un portatile [...] di quanti ne faccia tu in un anno sul campo.

Bond: Oh, e che vi servo allora?

Q: Ogni tanto un grilletto va premuto.

Bond: O non premuto. È difficile scegliere se sei in pigiama, Q¹.

Il dialogo introduttivo del contributo vorrebbe rappresentare l'idea della distanza e dell'impersonalità con cui oggi vengono effettuati gli attacchi armati da parte degli operatori: è come se non si tenessero in considerazione gli eventuali effetti collaterali nonché le responsabilità nel caso di attacchi sproporzionati rispetto ai

* Assegnista di ricerca in Informatica giuridica e Filosofia del diritto presso il Dipartimento di Giurisprudenza dell'Università di Modena e Reggio Emilia.

¹ Questo dialogo è tratto dal film *Skyfall* (2012), diretto da Sam Mendes. Il film è il ventitreesimo della serie cinematografica sulle missioni dell'agente segreto dell'MI6 (*Military Intelligence Section* 6) James Bond. Il personaggio di Bond nasce dai romanzi di Ian Fleming (1908-1964) e traggono spunto dalle esperienze dell'autore nei servizi segreti inglesi durante il secondo conflitto mondiale.

target di riferimento. Fra l'altro, i recenti conflitti armati² in Medio Oriente hanno fatto emergere (o meglio, riemergere) in tutta la loro drammaticità il delicato tema delle armi autonome e intelligenti.

Com'è noto, la rivoluzione tecnologica, con una rapidità e pervasività inimmaginabile fino a qualche decennio fa, ha modificato e integrato tutti i campi della conoscenza umana³. Tant'è che, come puntualmente evidenziato dalla letteratura scientifica, la conoscenza informatica e la conseguenziale innovazione tecnologica possono essere considerate come un fatto sociale totale⁴.

Siffatta affermazione è assai pertinente nel campo delle tecnologie belliche. Non è un caso che l'evoluzione degli armamenti militari e l'immenso potenziale offensivo di quest'ultimi siano strettamente connessi allo stato tecnologico di un preciso periodo storico, condizionando gli andamenti e i metodi di conduzione dei conflitti armati fra i belligeranti.

L'esempio più evidente dello sviluppo tecnologico applicato al settore militare è rappresentato sicuramente dall'Intelligenza Artificiale⁵, che ha consentito di

² Anche se il termine giuridico-politico "guerra" non è stato ufficialmente abrogato nel diritto internazionale, sembrerebbe preferibile – in relazione agli scontri armati tra le parti – l'utilizzo del lemma "conflitto armato". A conferma di ciò, come emerge dalle riflessioni di Natalino Ronzitti, il diritto umanitario, vale a dire il *corpus* normativo che disciplina il trattamento dei civili, dei prigionieri di guerra nonché i mezzi e i metodi di combattimento fra le parti, si applica automatica ai belligeranti, pur in assenza di un ufficiale "stato di guerra". Cfr., in questo senso, N. RONZITTI, *Diritto internazionale dei conflitti armati* (1998), Giappichelli, Torino, 2021, pp. 150-153.

³ M. MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Tangram, Trento, 2017, p. 83.

⁴ A. GARAPON, J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, a cura di F. MORINI, il Mulino, Bologna, 2021, p. 73; B.G. BELLO, *(In)giustizie digitali. Un itinerario fra tecnologie e diritti*, Pacini Giuridica, Pisa, 2023, p. 10.

⁵ Sull'Intelligenza Artificiale, e sulle diverse questioni che questa pone al diritto, la letteratura è assai vasta. Per un primissimo inquadramento della tematica si rinvia, *ex multis*, a: F. ROMEO, *Il diritto artificiale*, Giappichelli, Torino, 2002; A.C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Giappichelli, Torino, 2015; G. CONTISSA, *Information Technology for the Law*, Giappichelli, Torino, 2017; P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, Milano, 2017; S. AMATO, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020; L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020; G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022; L. FLORIDI, *Etica dell'intelligenza artificiale, sviluppi, opportunità, sfide*, Raffaele Cortina Editore, Milano, 2022; Th. CASADEI, S. PIETROPAOLI, *Intelligenza artificiale: l'ultima sfida per il diritto?*, in ID. (a cura di), *Diritto e tecnologie informatiche. Seconda edizione aggiornata e ampliata. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 259-274; F.H.

ridisegnare e ripensare gli attacchi armati, ponendo dei significativi cambi di paradigma nel diritto⁶.

Più specificatamente, nel caso degli utilizzi bellici dell'IA si possono ipotizzare diversi impieghi: da un lato, si può fare ricorso alle applicazioni *software*⁷ per raccogliere i dati ed estrarre le informazioni (viene svolta sostanzialmente una funzione di *intelligence*⁸) ovvero l'IA può essere adoperata per la difesa e l'attacco nella *cyberwarfare*⁹; dall'altro lato, è possibile affidare all'IA il ruolo di guida per i sistemi robotici armati. Essi – sfruttando la forza fisica (cinetica) – effettuano movimenti e attacchi verso gli obiettivi selezionati.

LLANO ALONSO, *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Tirant lo Blanch, Valencia, 2024. Inoltre, con un approccio etico-filosofico, M TADDEO, *The Ethics of Artificial Intelligence in Defence*, Oxford University Press, Oxford, 2024.

⁶ Ciò, più in generale, si collegherebbe all'inarrestabile progresso della ricerca scientifica, visto che è stato possibile lo sviluppo di sistemi autonomi, con la precisa conseguenza di apportare importanti cambi di paradigma anche nella scienza giuridica. Sull'importanza della ricerca scientifica nella costruzione dei sistemi autonomi: G. SARTOR, *Introduzione*, in *Rivista di filosofia del diritto*, 1, 2020, pp. 65-72. Sul nesso fra diritto e nuove tecnologie: F.J. ANSATEUIG ROIG, *Nuove tecnologie e spazio pubblico*, in S. SALARDI, M. SAPORITI (a cura di), *Le tecnologie morali emergenti e le sfide etico-giuridiche delle nuove soggettività*, Giappichelli, Torino, 2020, pp. 24-41. In un analogo orizzonte argomentativo, sono pertinenti le riflessioni di Giuseppe Zaccaria, il quale argomenta come le nuove tecnologie pongono al diritto una «difficoltà di inquadrare fenomeni nuovi o in rapidissima trasformazione all'interno di vecchie categorie e sistemazioni tradizionali e quando le regole non si prestano più a ordinare i fatti» (G. ZACCARIA, *Postdiritto. Nuove fonti, nuove categorie*, il Mulino, Bologna, 2022, p. 38).

⁷ Il *software* indica le componenti interne dei sistemi di elaborazione e si contrappone all'*hardware*, quest'ultimo rappresenta le parti materiali (fisiche/tangibili) dei sistemi.

⁸ G. SARTOR, *L'intelligenza artificiale e il diritto*, cit., p. 99.

⁹ La *cyberwarfare* è quell'insieme di attività di preparazione e conduzione delle operazioni belliche nel *cyberspace*. Quest'ultimo è riconosciuto, ormai, come la quinta dimensione della conflittualità. Sulla guerra cibernetica si vedano gli studi, comprensivi sia degli aspetti giusfilosofici sia umanitari, a M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014; M. DURANTE, *Violence, Just Cyber War and Information*, in *Philosophy & Technology*, 28, 2015, pp. 369-385; U. PAGALLO, *Cyber Force and the Role of Sovereign States in Information Warfare*, in *Philosophy & Technology*, 28, 2015, pp. 407-425; S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati digitali*, in *Rivista di filosofia del diritto*, 1, 2019, pp. 379-400; F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche. Temi e problemi*, Giappichelli, Torino, 2021, pp. 500-505; S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Giappichelli, Torino, 2022, pp. 49-66; ID., *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, in *Ars interpretandi*, 1, 2023, pp. 61-76.

Quando l'IA è adoperata come guida per i sistemi menzionati sopra, si è in presenza di armi autonome, intelligenti e letali, conosciute anche con l'acronimo di LAWS (*Lethal Autonomous Weapons System*).

Dal momento che queste armi non sono disciplinate dal diritto¹⁰, non esiste una definizione univoca e condivisa. La più accreditata, introdotta dall'ICRC (*International Committee of the Red Cross*), dispone che i sistemi LAWS siano «Any Weapons systems with autonomy in its critical function. That is a weapon system that can select (i.e. search for detect, identify, track, select) and attack (i.e. use force against, neutralize, damage or destroy) without human intervention»¹¹.

Pertanto, ciò che rileva nelle configurazioni delle armi LAWS non sono le differenti applicazioni dell'IA (come, per fare degli esempi, il *knowledge-based*, il *machine learning*, il *deep learning* e lo *shallow learning neural network*), ma il grado di autonomia dei sistemi¹², dove può essere presente o assente l'intervento umano (*meaningful human control, human in the loop/out of the loop*¹³).

Da un punto di vista squisitamente informatico-giuridico, l'autonomia nei sistemi può essere delineata in tre dimensioni¹⁴: *capability and organizational independence* (la capacità e l'autonomia organizzativa), cioè i sistemi per definirsi autonomi devono possedere le capacità necessarie per svolgere i compiti assegnati nel contesto

¹⁰ Cfr. N. RONZITTI, *Diritto internazionale dei conflitti armati*, cit., p. 211.

¹¹ «Si definisce autonomo un sistema d'arma che può svolgere la sua funzione critica in modo indipendente. Cioè un sistema d'arma che può eseguire operazioni in modo autonomo (cioè cercare, rilevare, identificare, seguire e selezionare) gli obiettivi e attaccarli (cioè usare la forza contro, neutralizzare, danneggiare o distruggere) senza l'intervento umano» (International Committee of the Red Cross, Expert Meeting, *Autonomous Weapons System (AWS). Implications of increasing autonomy in the critical function of weapons*, Versoix, Switzerland, 15-16 marzo 2016, p. 3).

¹² F. MERENDA, *Deliberazione, giudizio e responsabilità nell'epoca degli Autonomous Weapons System (AWS): sulle sfide etiche e giuridiche poste dalla sostituzione di soldati umani con sistemi robotici*, in *Ragion pratica*, 1, 2020, pp. 263-283.

¹³ Cfr. C. HEYNS, *Autonomous weapons system: living a dignified life and dying a dignified death*, in N. BHUTA, S. BECK, R. GEISS, C. KRESS, H.Y. LIU, *Autonomous Weapons System. Law, Ethics, Policy*, Cambridge University Press, Cambridge, 2016, pp. 3-12; M.G. LOSANO, *Guerra e pace in Kelsen – ieri e oggi*, in *Materiali per una storia della cultura giuridica*, 2, 2020, pp. 443-464.

¹⁴ G. SARTOR, A. OMICINI, *The autonomy of technological system and responsabilities for their use*, in N. BHUTA, S. BECK, R. GEISS, C. KRESS, H.Y. LIU, op. cit., pp. 17-45, in part. pp. 23-25; G. CONTISSA, *Automation and liability: an analysis in the context of socio-technical system*, in *i-lex. Rivista di Scienze giuridiche, Scienze Cognitive e Intelligenza Artificiale*, 1, 2017, pp. 17-45, in part. pp. 23-25.

dell'infrastruttura socio-tecnologica; *cognitive skills* (le capacità cognitive), vale a dire che i compiti assegnati al sistema sono importanti, perché così acquisiscono le capacità e le conoscenze necessarie per l'esecuzione delle attività cognitive, che derivano a loro volta dalle precedenti attività del sistema; *cognitive-behavioural architecture* (l'architettura cognitiva-comportamentale), ossia la creazione di un sistema ordinato che opera per la progettazione di comportamenti "intelligenti" in ambiti complessi, includendo le competenze e le conoscenze incorporate nei sistemi.

Strettamente correlata all'autonomia dei sistemi è la definizione di agente *software*, un'entità che percepisce con sensori l'ambiente circostante e che agisce su esso tramite attuatori¹⁵.

In questo contesto, pare opportuno illustrare anche la descrizione di "agente debole", elaborata da Micheal Wooldrige e Nicholas Jennings. Un agente debole è dotato di autonomia, abilità sociale (l'idoneità per comunicare con altri agenti o essere umani) e di proattività (acquisizione delle competenze necessarie per operare e prendere le iniziative più utili per il conseguimento dei risultati prestabiliti)¹⁶.

Le descrizioni dell'autonomia dei sistemi e degli agenti *software* consentono di sviluppare delle argomentazioni sugli effetti giuridici che producono. A una prima e sommaria analisi, si potrebbe ipotizzare che gli agenti – essendo immateriali – non siano rilevanti per il diritto. In realtà, l'immaterialità delle azioni e delle percezioni degli agenti *software* hanno importanti ripercussioni nella riflessione informatico-giuridica e giusfilosofica, visto che pongono nuove considerazioni sulle relazioni semi-giuridiche¹⁷ fra automi e sull'imprevedibilità delle loro azioni¹⁸.

¹⁵ Cfr. S.J. RUSSEL, P. NORVIG, *Artificial Intelligence. A Modern Approach* (1995), Pearson, Hoboken (NJ), 2020.

¹⁶ M. WOOLDRIGE, N.R. JENNINGS, *Intelligent agent: theory and practice*, in *The Knowledge Engineering Review*, Vol. 12, 2, 1995, pp. 115-152, in part. 116. Cfr. anche G. FIORIGLIO, *Guerre telematiche, sicurezza informatica e Società dell'informazione. Spunti di riflessione fra informatica, filosofia e diritto*, in A. CESOLINI, E. GRAZIANI (a cura di), *Le dimensioni della politica. Il paradigma della guerra*, Vol. II, Aracne, Roma, 2017, pp. 147-172.

¹⁷ C. FARALLI, *La filosofia del diritto contemporanea* (2012), Laterza, Roma-Bari, 2019, p. 81. Oltre a ciò, allo stato attuale, è difficile ipotizzare il riconoscimento della personalità giuridica agli

Trasportando tali questioni nei casi in cui l'IA ricopra le vesti di guida per le armi LAWS, sarebbe importante domandarsi a chi attribuire le responsabilità nei casi degli effetti collaterali nonché sproporzionati: all'operatore, alla macchina o al produttore¹⁹? Sono quesiti a cui il diritto, al momento, non riesce a trovare una risposta e ciò per diverse motivazioni: l'oscurità del codice informatico (algoritmi nel *software*) non consente di capire la logica con la quale vengono elaborati e selezionati i *target*; la mancanza di una regolamentazione a livello internazionale contribuisce a rendere poco chiare le "regole d'ingaggio"; l'eccessivo "affidamento" agli algoritmi da parte degli operatori; l'ineffettività del diritto nei casi di sproporzionalità negli attacchi.

Prima di fornire degli spunti di riflessione alle questioni poste *supra*, è importante vagliare le principali tipologie di armi LAWS che hanno consentito una tecnologizzazione della violenza²⁰, con significativi costi sia in termini economici-organizzativi sia di vite umane²¹.

2. Alcune tipologie (terra-mare) di armi LAWS e il caso specifico del drone

I conflitti armati contemporanei, contrassegnati da un'evidente asimmetria tecnologica che può instaurarsi tra le parti e da un disallineamento morale,

agenti *software* (e, più in generale, alla IA), poiché non sono in grado di comprendere pienamente le conseguenze delle loro azioni, limitandosi alla mera esecuzione dei compiti assegnati. Per questi aspetti: P. MORO, *Libertà del robot? Sull'etica delle macchine intelligenti*, in R. BRIGHI, S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 525-544; S. SALARDI, M. SAPORITI, *Perché l'IA non deve diventare Persona. Una critica all'ineluttabile 'Divenire Antropomorfo' delle Macchine*, in ID. (a cura di), op. cit., pp. 52-74.

¹⁸ Come opportunamente argomentato da Giovanni Sartor, è possibile distinguere fra l'imprevedibilità teorica e pratica: la prima imprevedibilità, la teorica, argomenta sulle difficoltà – se non l'impossibilità – di un'accurata previsione dei comportamenti degli agenti *software*; la seconda imprevedibilità, la pratica, evidenzia come sia in palese contraddizione con la delega dei compiti cognitivi agli agenti *software* la costante previsione dei loro comportamenti. Sul punto: G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Il diritto dell'informazione e dell'informatica*, 1, 2003, pp. 27-59, in part. p. 62.

¹⁹ È un quesito che investe non solo la sfera tecnico-giuridica, ma anche quella di natura esistenziale. Cfr., in tal senso, M. INNOCENZI, B. LEUCADITO, G. PETROCCO, *Il diritto tra digitale ed esistenziale*, Giappichelli, Torino, 2022.

²⁰ Cfr. T. SERRA, *Lo Stato e la sua immagine*, Giappichelli, Torino, 2005, p. 129.

²¹ Per questi aspetti, si rinvia alle argomentazioni di D. ZOLO, *Chi dice umanità. Guerra, diritto e ordine globale*, Einaudi, Torino, 2000, pp. 42-45.

dimostrano come il diritto – e in modo particolare il diritto umanitario – non sia più in grado di fornire delle risposte adeguate alle innovazioni tecnologiche e alle esigenze della comunità internazionale, posto che il diritto è il frutto di scelte e bilanciamenti mentre la tecnica non necessita di un'interazione dialogica²².

Prendendo ispirazione dalle intuizioni di Carl Schmitt (1888-1985), è ragionevole portare avanti l'idea che tutta la storia del diritto internazionale sia impregnata dell'idea di guerra e della sua evoluzione in termini di armamenti militari²³.

Del resto, come accennato *supra*, le armi LAWS sono dotate di un considerevole grado di autonomia, per cui sono in grado sia di consigliare sia di decidere le azioni da intraprendere, avviando un processo di «simil macchine-simil umani»²⁴. In sostanza, si sta innescando un procedimento di fusione fra soldati e robot²⁵ e ciò indicherebbe che l'attuale forma della guerra – diversamente da come è rappresentata nell'immaginario collettivo – tende a sfumare su un unico quadro di controllo²⁶, in quanto i soggetti principali sono gli operatori di queste armi che, al contempo, si limitano solo a prendere atto delle decisioni prese dai sistemi autonomi.

Le armi LAWS hanno avuto la straordinaria capacità di monopolizzare tutte le dimensioni spaziali dei conflitti (terra, mare e aria), introducendo scenari dove

²² Cfr. F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano, 2019, pp. 6-7.

²³ C. SCHMITT, *Il concetto discriminatorio di guerra* (1938), a cura di S. PIETROPAOLI, Prefazione di D. ZOLO, Laterza, Roma-Bari, 2008, p. 3. Sulla filosofia di Schmitt, *ex multis*, cfr. S. PIETROPAOLI, *Schmitt*, Carocci, Roma, 2012; TH. CASADEI, *Carl Schmitt: il diritto come decisione sovrana*, in ID., GF. ZANETTI, *Manuale multimediale di Filosofia del diritto*, Giappichelli, Torino, 2022, pp. 357-367; T. GAZZOLO, S. PIETROPAOLI (a cura di), *Il corvo bianco. Carl Schmitt davanti al nazismo*, Quodlibet, Macerata, 2022.

²⁴ A.C. AMATO MANGIAMELI, *I diritti umani tra teorie e prassi*, Giappichelli, Torino, 2022, p. 44.

²⁵ S. AMATO, *Neuroscienze e utilizzazione militare delle tecniche di potenziamento*, in *Etica & Politica*, 2, 2014, pp. 182-198. Inoltre, sul tema del potenziamento umano si veda: L. PALAZZANI, *Il potenziamento umano. Tecnoscienza, etica e diritto*, Giappichelli, Torino, 2015; G. FIORIGLIO, *Informatica medica e diritto. Un'introduzione*, Mucchi Editore, Modena, 2020, pp. 84-88; S. SALARDI, *Neurotecnologie tra potere e libertà*, Wolters Kluwer, Milano, 2024.

²⁶ Ernst Jünger (1895-1998), traendo spunto dalla sua esperienza nel primo conflitto mondiale, osservò che la *Total Mobilmachung* è l'atto con cui «è possibile, impugnando un unico comando su di un quadro di controllo, far confluire la rete d'energie – tanto ramificata e diffusa – della vita moderna nella grande corrente dell'energia bellica» (E. JÜNGER, *La Mobilitazione Totale*, in ID., *Scritti politici e di guerra 1919-1933*, 3 voll., vol. II (1930), Libreria Editrice Goriziana, Gorizia, 2005, p. 161).

L'attaccante massimizza il profitto – in questo caso il conseguimento degli obiettivi prescelti – senza contare, ovvero minimizzando, perdite fra le sue schiere.

Nei sistemi LAWS terrestri si segnalano i RAS²⁷ (*Robotic Autonomous Systems*), progettati per svolgere diverse attività: disinnescare degli ordigni esplosivi, ricognizioni via terra e lancio degli attacchi. Tali sistemi, oltre a possedere un importante grado di autonomia, impiegano gli algoritmi per compiere previsioni e variare – qualora sia ritenuto necessario e/o doveroso – il proprio comportamento.

In ambito marino, i sistemi LAWS – conosciuti altresì col termine MAS (*Maritime Autonomous Systems*) – sono adottati per mansioni come le missioni di pattugliamento, protezione delle rotte marittime, sorveglianza, interdizioni dello spazio marittimo nonché, pure in questo caso, l'attacco ai *target* selezionati²⁸.

In forza di ciò, dopo aver brevemente esposto le armi LAWS terra-mare – e premettendo, comunque, che si tratta di uno strumento *dual use*²⁹, dato che può essere adottato sia in ambiti civili sia in ambiti militari –, è necessario soffermare l'attenzione sull'esempio più paradigmatico di queste: il drone.

Il drone – dal verbo inglese *to drone* (ronzare) – è unUCAV (*Unmanned Combat Aerial Vehicle*) che dà la possibilità di comunicare tra ambienti distanti: lo spazio sicuro dove effettivamente l'operatore imposta le coordinate e i comandi, nonché l'area nella quale il drone opera. Tale arma agisce tramite un processo di identificazione, inteso anche come *pattern of life*, un metodo di sorveglianza – o meglio di datavegliaza³⁰ – che documenta e racchiude le abitudini dei *target*. I dati

²⁷ Sulle variegata tipologie di RAS: S. TROATH, *Trusting technology to wage war: the politics of trust and ethics in the development of robotics, autonomous system and artificial intelligence*, in *Critical Military Studies*, 1, 2024, pp. 1-19.

²⁸ Cfr. T. TÄRNHOM, H. LIWANG, *Military organization and emerging technologies – How do unmanned system find a role in future navies?*, in *Journal of Military Studies*, Vol. 11, 1, 2022, pp. 37-48.

²⁹ M.G. LOSANO, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. FORNI, T. VETTOR (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Giappichelli, Torino, 2019, pp. 20-38, in part. p. 29.

³⁰ Sulla datavegliaza si rinvia alle riflessioni di: G. FIORIGLIO, *Controllo e sorveglianza nella Società dell'informazione*, in *Studi sulla questione criminale*, 2-3, 2015, pp. 7-24; G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaele Cortina Editore, Milano, 2015; S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (2019), LUISS University Press, Roma, 2023; P.B. HELZEL, *Datavegliaza*, in A.C.

raccolti dai droni possono rispecchiare qualsivoglia aspetto del modo di vivere degli obiettivi mirati, venendo utilizzati per prevedere le azioni e i comportamenti “anomali”. Difatti, una delle modalità d’attacco dei droni è il *signature strikes*. Questa opzione d’attacco viene attivata allorquando l’identità dei soggetti da colpire non è nota, ma il loro “modello di vita” potrebbe indicare il coinvolgimento in attività a forte rischio³¹.

La seconda modalità d’attacco di quest’arma, probabilmente la più nota, è il *targeted killing* (uccisione mirata). In questo caso – a differenza del *signature strikes* –, l’identità dei soggetti da colpire è nota e li bersaglia con una precisione chirurgica³². Ciò nondimeno, sia da una prospettiva giusfilosofica sia informatico-giuridica, i droni incarnano delle problematicità che non possono essere eluse.

Da una parte, come messo a fuoco da Filippo Ruschi, queste armi disegnano l’attuale deriva della forma contemporanea della guerra, i nemici sono spogliati da ogni valenza umana e ridotti a meri bersagli da demolire³³, gli attacchi oltrepassano i confini e i limiti³⁴ degli Stati e pongono nuove sfide allo *ius in bello*³⁵. Ci si ritrova innanzi a quella che è stata definita una «sublimazione della guerra aerea»³⁶.

AMATO MANGIAMELI, G. SARACENI (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino, 2023, pp. 146-150.

³¹ N. FRANZ, *Targeted killing and pattern-of-life: weaponised media*, in *Media, Culture & Society*, Vol. 39, 1, 2017, pp. 111-121; K.J. HELLER, ‘One Hell of a Killing Machine’. *Signature Strikes and International Law*, in *Journal of International Criminal Justice*, 11, 2013, pp. 89-119.

³² In questo specifico senso, è esemplare l’omicidio mirato – effettuato nel gennaio del 2020 presso l’aeroporto internazionale di Baghdad – del generale Quasem Soleimani, comandante in capo delle forze Niru-ye-Gods in Iran.

³³ Cfr. F. RUSCHI, *Il volo del drone. Verso una guerra post-umana? Una riflessione di filosofia del diritto internazionale*, in *Jura Gentium*, 1, 2016, pp. 12-37, in part. pp. 34-37. Cfr. anche: G. CHAMAYOU, *Teoria del drone. Principi filosofici del diritto di uccidere*, DeriveApprodi, Roma, 2014, p. 15; A.C. AMATO MANGIAMELI, *I diritti umani tra teorie e prassi*, cit., p. 46.

³⁴ Per i confini e i limiti, in una prospettiva squisitamente giusfilosofica, si vedano le puntuali argomentazioni di GF. ZANETTI, *Confini e limiti del diritto*, Editoriale Scientifica, Napoli, 2020.

³⁵ Le controversie maggiori che i droni pongono sono, nella maggior parte dei casi, sulla transnazionalità degli attacchi. Per l’analisi di stampo internazionalistico: G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, Napoli, 2018, pp. 189-210; D. MAURI, “Aggiornamento disponibile”: *nuove tecnologie, uso della forza armata e diritto internazionale*, in TH. CASADEI, S. PIETROPAOLI (a cura di), op. cit., pp. 243-254.

³⁶ F. RUSCHI, *Il volo del drone. Verso una guerra post-umana? Una riflessione di filosofia del diritto internazionale*, cit., p. 34.

In concreto, con la *drone warfare*, per dirlo à la Sergio Cotta (1920-2007), viene interrotta ogni forma di comunicazione, dando libero sfogo a «un'attività-contro, sregolata, non dialogica e non co-esistenziale»³⁷, con la specifica conseguenza di trasformare le attività dei droni in sorveglianza e annientamenti³⁸.

Dall'altra parte, non è superfluo ricordare che i sistemi e le decisioni algoritmiche non sono in grado di distinguere fra gli obiettivi leciti e illeciti. Sussistono concretamente dei rischi che fanno aumentare gli effetti collaterali e la sproporzionalità degli attacchi armati effettuati con le armi LAWS, specialmente nei confronti degli obiettivi civili.

Al di là della nota questione dell'opacità algoritmica³⁹ in cui il procedimento tra l'inserimento dell'*input* e il ricavo dell'*output* è pressoché sconosciuto (c.d. *black box*⁴⁰), la complessità della società contemporanea non è tanto la fiducia posta nei confronti degli algoritmi, bensì il totale affidamento degli operatori al lavoro degli algoritmi, trascurando la circostanza che essi – sia volontariamente sia involontariamente – possono contenere dei *bias* pregiudizievole.

Siffatta circostanza, sicuramente l'emblema della Società algoritmica, reca con sé nuove e inaudite questioni a cui il giurista deve inevitabilmente rapportarsi.

3. Le difficoltà sull'imputazione delle responsabilità: tra fiducia e affidamento negli algoritmi

L'IA, a questo punto della storia del mondo, è da considerarsi una componente essenziale della società contemporanea: si discute più della Società algoritmica⁴¹

³⁷ S. COTTA, *Perché la violenza? Una interpretazione filosofica* (1978), con una introduzione di P.P. PORTINARO, Scholé, Brescia, 2018, p. 105. Si rinvia anche all'interpretazione del pensiero di Cotta su violenza, con le considerazioni di: D. CANANZI, *Sulla domanda cottiana: perché la violenza?*, in *Teoria e storia del diritto privato*, Speciale (a cura di F. MANCUSO e V. GIORDANO), 2022, pp. 1-17.

³⁸ G. CHAMAYOU, *Teoria del drone. Principi filosofici del diritto di uccidere*, cit., pp. 35-41.

³⁹ Conosciuta altresì come "indecifrabilità". Sul punto si veda: P. SAVARESE, *Diritto ed episteme. Note sullo statuto dello strumento giuridico*, Edizioni Nuova Cultura, Roma, 2014, p. 33.

⁴⁰ Tale termine, com'è noto, fu introdotto dall'opera di F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Harvard, 2015.

⁴¹ Sulla Società algoritmica, con le diverse questioni e problematichità che essa pone, si rinvia, *ex multis*: J. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, 78, 2017, pp. 1217-1241; F. PASQUALE, *Towards a Fourth Law of Robotics: Preserving Attribution*,

che della pregressa Società dell'informazione e della conoscenza. All'interno della Società algoritmica l'organizzazione si basa sui processi decisionali delegati ai *software* i quali, nell'esecuzione più o meno complessa degli algoritmi, elaborano le informazioni per fini decisionali o di apprendimento. Tra l'altro, la costante fornitura di dati permette ai sistemi di imparare e di continuare progressivamente a farlo, basandosi anche sulla pregressa esperienza.

In questo contesto, com'è noto, gli intermediari privilegiati per l'esercizio del potere sono gli algoritmi. Probabilmente, la definizione più accurata di "algoritmo" fu formulata da Renato Borruso (1928-2014), che definì gli algoritmi come «un insieme ordinato in sequenza di tutte le regole precise inequivoche, analitiche, generali, astratte, formulate *ex ante*, cioè prima che si presentino concrete questioni da risolvere e senza riferimento specifico ad esse, la cui scrupolosa e letterale applicazione da parte di chiunque lo pone infallibilmente in grado di conseguire il risultato giusto»⁴².

Malgrado ciò, allo stato attuale dell'avanzamento tecnologico, è difficile sostenere che l'automazione algoritmica possa risolvere le controversie inerenti alle decisioni inconsapevolmente o consapevolmente illecite, errate, arbitrarie o palesemente discriminatorie⁴³. Gli algoritmi, infatti, non sono né eticamente né tecnicamente neutri⁴⁴: sono solo una parziale rappresentazione della realtà e non la totalità di essa⁴⁵. Inoltre, a causa della loro segretezza, gli algoritmi «nascondono la vecchia

Responsability and Explainability in an Algorithmic Society, in *Ohio State Law Journal*, 78, 2017, pp. 1243-1255; W. BARFIELD (eds.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, Cambridge, 2020; M. SCHUILENBURG, R. PEETERS (eds.), *The Algorithmic Society. Technology, Power and Knowledge*, Routledge, Abingon-on-Thames, 2021; H.W., MICKLITZ, O. POLLICINO, A. SIMONCINI, G. SARTOR, G. De GREGORIO (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, 2021.

⁴² R. BORRUSO, *Computer e diritto*, 2 tt., Giuffrè, Milano, 1988, t. I, *Analisi giuridica dei computer*, p. 189.

⁴³ Per una puntuale osservazione dei punti descritti: S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la Pubblica Amministrazione, le imprese*, Wolters Kluwer, Milano, 2021, pp. 97-108.

⁴⁴ Cfr. A.C. AMATO MANGIAMELLI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, pp. 122-123. Nei medesimi termini: C. O'NEIL, *Come i big data aumentano la disegualianza e minacciano la democrazia*, Bompiani, Milano, 2017.

⁴⁵ Questo è il fenomeno del "dataismo". Si veda: L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, cit., pp. 28-29; Y.H. HARARI, *Homo deus. Breve storia del*

ambizione di dominio, tipica dell'assolutizzazione del potere oligarchico»⁴⁶. La programmazione degli algoritmi – implementati e incorporati all'interno dei sistemi intelligenti – fa acquistare un significativo potere economico, che può ingrandirsi proprio grazie alla segretezza di quest'ultimi, protetti a loro volta dalle normative della proprietà intellettuale e industriale⁴⁷.

Anche nella remota ipotesi che venisse riconosciuto il diritto alla *disclosure* algoritmica (e quindi l'accesso al codice informatico e la visione), l'estrema complessità dei sistemi automatizzati non renderebbe affatto immediata la comprensione della loro articolazione. Oltretutto, una conoscenza accurata dei comportamenti dei sistemi non è agevole, ed è molto complesso (anche oneroso) ricostruire con assoluta precisione la logica di un sistema informatico in un preciso arco temporale⁴⁸.

Se si applica questa prospettiva nel campo delle armi LAWS, è agevole constatare che sorgerebbero delle importanti problematiche nell'imputazione delle responsabilità nei casi di gravi effetti collaterali o di attacchi sproporzionati (c.d. *accountability gaps*). Siffatta difficoltà avviene perché non è facilmente dimostrabile

futuro, Bompiani, Milano, 2017. Parimenti interessanti e rilevanti sono le riflessioni, sul punto, di Raffaella Brighi, che indica come «Non solo il software guida i comportamenti umani al punto che ciò che è possibile o impossibile tecnologicamente si sovrappone alle categorie del permesso e dell'obbligo [...] Tali tecnologie aggregando (e quindi creando) dati informatici trasformano la realtà e riducono la distinzione tra essa e la sua rappresentazione digitale, creando una dimensione della realtà» (R. BRIGHI, *La vulnerabilità nel cyberspazio*, in *Ars interpretandi*, 1, 2017, p. 82).

⁴⁶ L. AVITABILE, *Il diritto davanti l'algoritmo*, in *Rivista italiana per le scienze giuridiche*, 8, 2017, p. 325. In aggiunta a ciò, come rappresentato da Bruno Romano, «Nella peculiarità della contemporanea società dei dati, la tendenza dominante appare inizialmente quella strutturata in modo che i gruppi elitari offrano informazioni-servizi» (B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, edizione curata da G. PETROCCO, Giappichelli, Torino, 2020, p. 204).

⁴⁷ In effetti è assai arduo scardinare l'opacità algoritmica, posto che «comporterebbe una sostanziale revisione delle varie normative nazionali e internazionali che regolamentano la proprietà industriale e intellettuale; avrebbe un impatto devastante su gran parte del settore informatico» (G. FIORIGLIO, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici*, in *Ars interpretandi*, 1, 2021, p. 55).

⁴⁸ Per rimediare all'opacità algoritmica, la letteratura scientifica propone il principio della "conoscibilità dei dati", ovvero sia la conoscenza dei dati derivati, collettivi o statistici che hanno contribuito alla formazione del processo decisionale automatizzato. Così facendo si otterrebbe, almeno in parte, un diritto alla spiegabilità. Cfr., in tal senso, M. PALMIRANI, S. SAPIENZA, *Big Data, Explanations and Knowability*, in *Ragion pratica*, 57, 2021, pp. 349-364; U. PAGALLO, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 1, 2020, pp. 93-106.

l'elemento soggettivo (per esempio, il dolo o la colpa) dell'operatore. Le difficoltà maggiori nel provare l'elemento soggettivo avvengono nel caso di improvvisi malfunzionamenti del sistema, poiché in questo caso è assai arduo attribuire delle responsabilità al produttore (quantomeno la colpa).

Ragionando in questi termini, gli algoritmi stabilirebbero *ex ante* dati e parametri di giudizio senza nessuna cognizione delle materie da applicare e delle molteplici variabili che potrebbero essere in gioco, dato che presupporrebbero che in ogni caso sia "giusta" la selezione dei dati e dei parametri scelti in precedenza.

Quanto rappresentato consentirebbe di soffermare l'indagine sulla tematica più delicata della Società algoritmica, ossia la deresponsabilizzazione degli operatori e delle loro azioni, i quali "affidano" sé stessi ai dispositivi e alle tecniche⁴⁹, causando un "esonero cognitivo"⁵⁰ nonché una rinuncia alla comprensione e alle motivazioni per cui vengono adottate alcune decisioni e non altre da parte dei sistemi⁵¹.

Alla luce delle considerazioni svolte *supra*, pare che si stia delineando uno scenario in cui l'IA si proporrebbe come agente regolatore⁵² decidendo – sempre nel campo delle armi LAWS – come e quando attaccare il nemico. Così facendo, ci sarebbe il concreto rischio di pregiudicare il diritto umanitario, e ciò perché in questo campo manca una regolamentazione chiara e precisa sull'utilizzo di queste armi.

⁴⁹ Imprescindibili le riflessioni sul tema di G. ANDERS, *L'uomo è antiquato* (1956), 2. Voll., Bollati Boringhieri, Torino, 2007. Sull'interpretazione di Anders si veda S. VANTIN, *Le metamorfosi della responsabilità. Tecnica, diritto, bioetica*, Giappichelli, Torino, 2024, pp. 45-63.

⁵⁰ Il concetto di "esonero cognitivo" è ripreso da A. GEHLEN, *Sull'essenza dell'esperienza*, in ID., *Prospettive antropologiche*, a cura di V. RASINI, il Mulino, Bologna, 2005, pp. 45-67. Per una magistrale interpretazione dell'"esonero cognitivo" di Gehlen, applicato nella Società algoritmica, si rinvia a TH. CASADEI, *Algoritmi ed esonero: a partire da Arnold Gehlen*, in *Revista Jurídica de Asturias*, 45, 2022, pp. 245-266.

⁵¹ Come preconizzato da Martin Buber (1878-1965) negli anni Quaranta del XX secolo, «le macchine, inventate per servire all'uomo che lavora, lo hanno asservito. Esse non sono più, come l'utensile, un prolungamento del braccio umano: l'uomo è diventato un loro prolungamento, un'articolazione meccanica periferica che apporta e porta fuori» (M. BUBER, *Il problema dell'uomo* (1943), Marietti Editore, Bologna, 2019, p. 59).

⁵² Cfr. le argomentazioni di S. SALARDI, *Intelligenza artificiale e semantica del cambiamento. Una lettura critica*, Giappichelli, Torino, 2023. Estremizzando l'idea di agente regolatore, Eric Sadin rileva come all'IA sia affidato il compito di enunciare la verità. Sul punto: E. SADIN, *Critica della ragione artificiale*, LUISS University Press, Roma, 2019, p. 10.

Per siffatte motivazioni è fondamentale che la riflessione giusfilosofica e informatico-giuridica orienti e trovi delle soluzioni affinché sia fortemente limitato il devastante impatto delle armi autonome, intelligenti e letali.

4. Riflessioni conclusive sull'effettività del diritto e l'etica militare

Dalle considerazioni svolte emerge che l'autonomia dei sistemi intelligenti, attraverso gli agenti *software* che eseguono le istruzioni degli algoritmi, presenta delle criticità ai giuristi, dal momento che le armi LAWS agiscono, il più delle volte, in totale autonomia. Affiorano anche difficoltà maggiori nell'imputazione delle responsabilità nel caso degli effetti collaterali e/o sproporzionati di queste armi. Ciò potrebbe compromettere il diritto umanitario dei conflitti armati, la cui *ratio* sarebbe quella della «tutela della persona-vittima, in funzione del *principio di umanità*, sia nei conflitti internazionali sia nei conflitti interni»⁵³.

All'interno della comunità internazionale, come detto in precedenza, non sussiste nessuna legislazione (o un trattato) che regolamenti l'uso di tali armi, né viene previsto un regime delle responsabilità. In tal senso, è presente solo una risoluzione delle Nazioni Unite, che suggerisce agli Stati membri di adoperarsi per l'adozione di una legislazione vincolante sull'inibizione di tali armi entro il 2026⁵⁴.

Nell'ipotesi di una futura (e auspicata) regolamentazione delle armi LAWS, con un'interpretazione giusfilosofica, è possibile ispirarsi all'idea della regola regolativa.

Gianfrancesco Zanetti, nei suoi studi sulle diverse elaborazioni del diritto in Thomas Hobbes (1588-1679) e Giambattista Vico (1668-1744), ha messo in rilievo che in Hobbes è preminente la regola regolativa. Quest'ultima istituisce obblighi, divieti e sanzioni per il *demos* e lo scopo sarebbe quello del mantenimento

⁵³ I. TRUJILLO, *Diritti umani e diritto umanitario: convergenze, complementarità e deroghe*, in TH. CASADEI (a cura di), *Diritti umani e soggetti vulnerabili*, Giappichelli, Torino, 2012, p. 65.

⁵⁴ [Risoluzione 78/241 del 2023](#).

dell'ordine. Fra l'altro, la regola regolativa parte dall'assunto che l'ente da regolare sia già esistente nella realtà⁵⁵.

Servendosi di questa metodologia, sarebbe possibile concepire una legislazione scrupolosa sull'utilizzo delle armi LAWS contenendo, a sua volta, la collateralità e la sproporzionalità di questi attacchi (quantomeno quelli derivanti da attacchi a cui sono riconducibili gli Stati). Ciò gioverebbe, da un lato, a una disciplina rispettosa dei diritti umani e, dall'altro lato, sarebbe coerente con il compito del giurista, il quale non deve limitarsi solo alla raccolta e al coordinamento del diritto esistente, ma deve effettuare compiti di ideazione e progettazione degli strumenti giuridici, allo scopo di adattarli alla complessità delle nuove tecnologie⁵⁶.

Pertinente, in quest'ultimo senso e attraverso gli strumenti d'indagine informatico-giuridici, potrebbe essere l'idea dell'inserimento di una "manopola etica" nelle armi LAWS.

L'idea della manopola, pensata originariamente per i veicoli a guida autonoma⁵⁷, permetterebbe all'operatore di personalizzare il raggio d'azione, effettuando delle scelte fra diverse impostazioni etiche: l'operatore, così, girerebbe la manopola nell'altruismo (preferenza per la vita dei terzi), nell'imparzialità (indifferenza tra la vita del conducente e quella dei terzi) e nell'egoismo (assoluta priorità per la vita del conducente). La previsione di una manopola per i sistemi d'armi LAWS ridurrebbe così l'autonomia dei sistemi, nonché favorirebbe possibili configurazioni della responsabilità (a condizione, però, che la legislazione sia in grado di quantificare il grado di "egoismo" scelto dall'utente per l'irrogazione della sanzione). Oltre a ciò, la progettazione di questa farebbe ipotizzare anche una responsabilità del

⁵⁵ Per la regola regolativa, e per la comparazione con la regola costitutiva, si vedano i lavori di GF. ZANETTI, *Introduzione al pensiero normativo*, Diabasis, Reggio Emilia, 2004, pp. 70-72; ID., *Vico eversivo*, il Mulino, Bologna, 2011, p. 83; *Eguaglianza come prassi. Teoria dell'argomentazione normativa*, il Mulino, Bologna, 2015, pp. 23-24; ID., *Diritto e civilizzazione: Giambattista Vico*, in Th. CASADEI, ID., op. cit., p. 184.

⁵⁶ Cfr. S. COTTA, *La sfida tecnologica*, il Mulino, Bologna, 1968, pp. 175-178.

⁵⁷ Per i veicoli a guida autonoma, *ex multis*, si veda: S. SCAGLIARINI (a cura di), *Smart roads e driveless cars: tra diritto, etica, tecnologie, etica pubblica*, Giappichelli, Torino, 2019.

produttore⁵⁸ (si pensi, ad esempio, al settaggio preimpostato della manopola in “altruista” da parte dell’operatore e il sistema – diversamente da quanto programmato – opti arbitrariamente in “egoista”).

Alla luce di ciò, più che opportuna, oltre che necessaria, apparirebbe una specifica regolamentazione sull’utilizzo delle armi LAWS, riconsiderando così i parametri della legittimità e della legalità nella forma della guerra contemporanea⁵⁹, ed evitando che il conflitto si trasformi in una mera campagna di abbattimento degli obiettivi leciti o illeciti.

Le considerazioni svolte in precedenza non possono tralasciare in alcun modo i soggetti istituzionalmente preposti alla conduzione dei conflitti armati: i militari. Sul punto, potrebbe anche essere utile richiamare i concetti legati all’etica militare, minacciata sempre di più dalla pervasività della tecnica.

L’etica militare, a differenza di quanto si possa pensare, non è in alcun modo riducibile alla mera *summa* delle disposizioni che regolamentano il comportamento dei militari in tempo di pace e in tempo di guerra⁶⁰, né alla legge che disciplina l’ordinamento militare⁶¹, ma è l’espressione di una moltitudine di componenti emotivi, razionali, etici che appartengono a un peculiare *ethos*. Effettivamente, come bene argomentato da Maurizio Manzin, grazie alla significativa valenza etica delle operazioni PSO (*Peace Support Operation*), gli appartenenti alle forze armate godono di un’immagine assai evocativa e cavalleresca, visto che essi si prodigano per le popolazioni appartenenti alle zone più sensibili, delicate e difficili del

⁵⁸ Sulle discussioni attorno all’inserimento della manopola etica nei sistemi autonomi si rinvia, per l’ampissima bibliografia e le dimostrazioni scientifico-matematiche dell’opportunità dell’inserimento di questa, a G. CONTISSA, F. LAGIOIA, G. SARTOR, *La manopola etica: i veicoli eticamente personalizzabili e il diritto*, in *Sistemi intelligenti*, 3, 2017, pp. 601-614.

⁵⁹ «È invece necessario tornare a riflettere sulla questione della forma della guerra contemporanea, sui parametri di legittimità e di legalità del conflitto e, in definitiva, sul concetto stesso di nemico. Solo una scienza giuridica consapevole del suo ruolo è all’altezza di questo obiettivo: una scienza capace di ispirarsi alle vicende della codificazione ottocentesca del diritto bellico e in grado di affrontare la sfida di un nuovo *nomos* della guerra» (F. RUSCHI, *Il diritto, la guerra e la «tecnica scatenata»*, in R. CAMPIONE, ID. [a cura di], *Guerra, diritto e sicurezza nelle relazioni internazionali*, Giappichelli, Torino, 2019, p. 66).

⁶⁰ Il C.p.m.p. (Codice penale militare di pace) e il C.p.m.g. (Codice penale militare in tempo di guerra) sono stati entrambi approvati con il RD. 20 febbraio 1941 n. 303.

⁶¹ Il Codice dell’ordinamento militare è stato emanato con il D.lgs. 15 marzo 2010 n. 66, aggiornato con D.lgs. 24 febbraio 2012 n. 20.

mondo. È importante mantenere integra siffatta immagine perché, ad avviso dell'autore, la pervasività della tecnica (in sostanza l'uso delle armi LAWS) lede l'elegante immagine dei *miles*, dal momento che la simbolica nonché eroica figura dei soldati viene ridotta a quella di meri operatori dei sistemi (automi) quando, nella realtà, i membri dell'ordinamento militare possiedono uno specifico *ethos* e *nomos*⁶².

Sulla base di queste brevissime considerazioni – che possono essere dedicate anche alla totalità degli utenti – dunque, è necessario (*rectius*, obbligatorio) che i *miles* non si facciano soggiogare dalla tecnica: dovrebbero, invece, dominarla senza farsi condizionare dalla complessità dei sistemi LAWS.

In conclusione, fermo restando la grandissima importanza dello sviluppo tecnologico nell'attuale società, è importante rammentare che il diritto e la tecnica non possono essere disgiunte, ma solo insieme possono realizzare il progresso della civiltà.

Come ebbe a dire Norberto Bobbio (1909-2004), «Coloro che oggi si preoccupano di trovare una soluzione, quale che sia, al problema, oscillano tra questi due estremi: rifiutare la seduzione del progresso immancabile, senza lasciarsi tentare dal fascino dell'abisso. Non sono né ottimisti né pessimisti. Credono che la salvezza sia, ancora una volta, il risultato di una ricerca razionale e di uno sforzo consapevole, e operano di conseguenza»⁶³.

Le parole di Bobbio restano attuali, non possono che essere la pietra miliare del giurista per un "umanesimo digitale"⁶⁴ rispettoso, in ogni sua forma, della dignità e della vita umana, in stretta aderenza con quella stella polare rappresentata, oggi, dai diritti umani che, ovviamente, spettano indifferentemente a tutti e tutte. In modo particolare, nel momento in cui scoppiano i conflitti armati la loro

⁶² Per la peculiarissima analisi sulla specificità della figura dei militari, dell'ordinamento militare e dei suoi principi fondamentali si vedano le puntuali argomentazioni di: M. MANZIN, *Ethos e nomos nell'ordinamento militare*, in *Diritto costituzionale. Rivista quadrimestrale*, 2, 2022, pp. 118-145.

⁶³ N. BOBBIO, *Lezioni sulla guerra e sulla pace*, a cura di T. GRECO e con una postfazione di P. POLITO, Laterza, Roma-Bari, 2024, p. 221.

⁶⁴ Cfr., in quest'ultimo senso, A. PUNZI, *L'umanesimo digitale verso un nuovo principio di responsabilità?*, in *Democrazia e diritti sociali*, 1, 2023, pp. 23-32.

osservanza – specialmente sull'utilizzo delle armi – deve essere assolutamente cogente; altrimenti, opinando diversamente, verrebbe sacrificato il principio di umanità sull'altare di un supposto "progresso tecnologico di precisione".

dirittifondamentali.it