FONDAZIONE LEONARDO
Civiltà delle Macchine

CIVILTÀ DELLE MACCHINE

CENTRO STUDI AMERICANI

Winning the Artificial Intelligence era

QUANTUM DIPLOMACY AND THE POWER OF AUTOMATION

I N D I C E

PREMESSA

L'Intelligenza Artificiale, l'analisi dei big data e i computer quantistici porteranno ad una rivoluzione a tutto tondo, sempre più pervasiva. La disponibilità di potenze di calcolo esponenzialmente maggiori consentirà ai decision maker di valutare e agire con una consapevolezza del contesto e una rapidità mai raggiunte prima; un futuro prossimo dove le capacità della macchina potrebbero superare l'elemento umano, il suo controllo, la sua responsabilità.

Frutto della collaborazione tra il Centro Studi Americani e la Fondazione Leonardo Civiltà delle Macchine – con il supporto del Ministero degli Affari Esteri e della Cooperazione Internazionale e con il contributo scientifico del Prof. Enrico Prati - il presente studio mira ad offrire un'analisi il più possibile oggettiva sullo stato dell'arte delle nuove tecnologie e delle loro applicazioni nei nuovi scenari di Difesa e Sicurezza. Tale iniziativa intende inoltre approfondire e analizzare i rischi, le principali sfide e le possibili strategie per gestire le evoluzioni già in atto, nel quadro di norme e valori condivisi.

Al pari dell'innovazione che - per sua natura - è un processo in continuo divenire, complesso, non lineare, anche la definizione dei principi morali ed etici non può che emergere da un dialogo costante tra scienza, tecnologia e istituzioni giuridiche e politiche. Un processo che rimette l'umano al centro, come decisore ultimo, che negozia e stabilisce le regole del gioco, in ogni campo di applicazione, in tempi di pace e in scenari di conflitto.

INTRODUZIONE

di Enrico Prati

1. L'era delle tecnologie profonde

La rapida evoluzione delle tecnologie elettroniche e informatiche, iniziata dagli anni Settanta del Novecento, è entrata in una nuova fase di accelerazione, a partire dall'ultimo decennio. Non solo ci troviamo già nella materializzazione di molte rappresentazioni della fantascienza di cinquanta o sessanta anni fa, ma constatiamo che il cambiamento è solamente agli inizi.

Tra i fattori dell'accelerazione spiccano discipline come la meccanica quantistica e l'intelligenza artificiale che, sebbene fondate rispettivamente circa cento e settanta anni fa, stanno conoscendo un impiego sempre più avanzato. Si pensi ad esempio al cosiddetto quantum advantage del computer quantistico di Google, annunciato nel 2019, o al deep learning applicato al riconoscimento dei tumori e dei danni alla retina o. Come per il computer, anche queste innovazioni devono considerarsi generaliste: aprono nuovi orizzonti applicativi in tutti gli ambiti della conoscenza. Le tecnologie basate su queste discipline, in virtù dell'alto grado di specializzazione, della componente matematica speculativa, dell'ingegnerizzazione evoluta di materiali e tecniche, e – non ultimo - delle potenziali nuove opportunità di sviluppo, che vengono denominate "profonde", in inglese deep tech, ispirandosi alle reti neurali, che hanno recentemente aperto molte delle nuove frontiere.

Un fatto che può sorprendere è che la meccanica quantistica nasce come una teoria matematica necessaria per descrivere sistemi molto piccoli, quali elettroni e atomi, e che le sue applicazioni sono note da molto tempo. Se non si fosse compresa la formulazione della meccanica quantistica e la sua relazione con la realtà fisica, non sarebbe stato possibile – già dagli anni Sessanta - realizzare e sfruttare i semiconduttori e i laser. Analogamente, anche l'intelligenza artificiale - una teoria matematica applicata ai dati e alle informazioni - vanta una gloriosa tradizione che, dalle sue origini, ha portato ad algoritmi evoluti come i "sistemi esperti" e il "Deep Blue": il programma che nel 1997 riuscì a vincere contro Garry Kasparov, allora campione del mondo in carica nel gioco degli scacchi.

L'investimento in tecnologie deep tech è sostenuto in primo luogo dai governi, ma anche dal settore privato dei venture capitals e delle stesse corporation, come, per citarne alcune, Google, Microsoft, IBM, Intel, Blackberry o Alibaba. Un investimento che ha contribuito alla creazione di nuova conoscenza e

all'accelerazione a cui stiamo assistendo e che ha dato nuova linfa all'innovazione tecnologica. Tanto negli Stati Uniti, così come in Canada, in Israele, nel Regno Unito e in Cina - per citare Paesi particolarmente rappresentativi dal punto di vista delle politiche pubbliche di innovazione - lo Stato ha assunto il ruolo di creatore di ecosistemi. Allo stesso tempo, gli investitori e le corporations sono divenuti selezionatori delle idee con maggiore probabilità di successo da un punto di vista del mercato.

Dal lato pubblico, la creazione di ecosistemi si basa su un forte sostegno alla formazione di capitale umano qualificato attraverso una serie di fattori: il potenziamento del sistema universitario, le politiche di incentivi fiscali per le imprese (su un arco temporale almeno decennale), la creazione di parchi tecnologici, il supporto finanziario alla ricerca di base. Dal lato privato, il finanziamento del trasferimento tecnologico al mercato richiede invece: politiche di open innovation, disponibilità di capitali di rischio, l'investimento da parte delle corporation in programmi di ricerca nelle proprie unità di R&D.

Combinati insieme, questi ingredienti, hanno portato a realtà allo sviluppo e alla valorizzazione di nuovo hardware e nuovo software che stanno facendo la fortuna di produttori già consolidati: è il caso di Nvidia, che dal 2006 al 2021 ha centuplicato il proprio valore in borsa, o di nuove startup che non esistevano fino a 5 anni fa e che ora sono quotate al NASDAQ (ad esempio il produttore di computer quantistici IonQ, il cui valore è ora a pochi mesi dall'IPO di 2.8B$; o la società di cybersecurity che impiega l'intelligenza artificiale Crowdstrike fondata nel 2011 e che valeva 1B$ nel 2017, fino al valore attuale di più di 50 B$).

Questo è solo l'inizio. Se da un lato normativo sorgono sfide sul piano etico – si pensi ai droni militari pilotati dall'intelligenza artificiale sviluppati da Paesi come Cina e Turchia - dal lato meramente tecnico queste tecnologie aprono a nuovi scenari: dall'impiego di nuovi materiali (come substrato fisico per sostenere l'architettura astratta del calcolo), fino all'intelligenza artificiale generale in grado di emulare quella umana, o le brain-machine interface come quelle di Neuralink di Elon Musk (che ha raccolto nel 2021 un nuovo round di finanziamenti da 205M$, di Amazon e di Google). In queste ultime, innesti elettronici artificiali nella corteccia del cervello umano consentono uno scambio bidirezionale tra il pensiero che si svolge nell'encefalo (neuroni biologici), e organi di senso aggiuntivi basati su sensori di semiconduttori e metalli, mediati da un sistema di neuroni artificiali addestrati con moderni metodi di intelligenza artificiale. Non è un caso se DARPA ha incluso le BMI nel finanziamento "AI Next" da 2B$ della terza generazione dell'intelligenza artificiale, quella che deve spingersi oltre l'attuale deep learning.

Computer quantistici e intelligenza artificiale stanno fornendo nuova potenza computazionale – parafrasando Tom Conte dell'IEEE Rebooting computing, "nuovo hardware per nuovi tipi di software", che sosterranno la crescita economica e altereranno gli equilibri geopolitici per molti anni a venire.

2. Impatto sulla geopolitica e sulle relazioni internazionali

È indubbio che questo tsunami tecnologico stia alterando gli equilibri geopolitici. Basti pensare alle implicazioni che ha avuto la concentrazione in Oriente - in particolare a Taiwan con TSMC e in Corea del Sud con Samsung (due Aziende che da sole producono il 70% dei semiconduttori al mondo) - della crisi di disponibilità di processori e circuiti integrati: un fenomeno che ha spinto il presidente USA Joe Biden a stanziare 52 miliardi di dollari per potenziare la capacità produttiva domestica di chip e l'Unione Europea a varare il Chips Act da 45 miliardi di euro nel Febbraio 2022. Se guardiamo all'influenza di queste tecnologie sulla geopolitica e sulle relazioni internazionali, rileviamo due livelli di impatto. Il primo riguarda il loro impiego diretto, mediante l'utilizzo delle tecnologie come ausilio alla gestione delle dinamiche relazioni diplomatiche. Il secondo livello consiste invece nell'impiego indiretto, vale a dire - in chiave proattiva - come leva per vincere nella competizione economica in termini maggiore di competitività, ma anche, in termini pragmatici, come strumento di supremazia tecnologica per esercitare maggiore pressione in termini diplomatici.

Muovendosi nell'ambito dell'impiego diretto, è possibile elencare diversi scenari come esempio. L'intelligenza artificiale può consentire di determinare le mosse che un agente artificiale deve compiere per rafforzare la propria posizione nella rappresentazione di uno scenario diplomatico. La sua capacità di gestire grandi quantità di dati può consentire l'analisi quantitativa di uno scenario che evolve e predirne l'evoluzione successiva nei termini degli indicatori considerati. Essa può supportare la decisione umana, spaziando dall'automazione di task di routine, fino al supporto a livello tattico e operativo, anche se presumibilmente senza arrivare all'autonoma decisione strategica che resterebbe appannaggio dell'uomo[1] .

Inoltre, portando alle estreme conseguenze la matematica che soggiace la meccanica quantistica, è possibile formulare problemi relativi a scenari diplomatici mediante concetti esclusivi della meccanica quantistica, come quello di sovrapposizione quantistica, che traslato su uno scenario si può far corrispondere al fatto che, fino a che una decisione non è stata presa, due alternative opposte convivono contemporaneamente, mentre soltanto dopo la decisione se ne sarà realizzata una sola delle due. Oggi, grazie ai processori quantistici, non si tratta più dell'applicazione qualitativa della teoria alla formulazione dei problemi – che già di per sé è una sfida, ma anche potenzialmente della capacità di risolverli, una volta correttamente impostati, mediante un hardware ritagliato su misura e già pronto per restituire una risposta di interesse. Ambito di applicazione rappresentativi sono

[1] Bjola, Corneliu. "Diplomacy in the Age of Artificial intelligence." EDA Working paper, Retreived from http://www. realinstitutoelcano. org/wps/portal/rielcano_en/contenido (2019).

la quantum decision theory o la simulazione della dinamica di una comunità[2]. In particolare, a questo riguardo risulta esemplificativo l'utilizzo di un computer quantistico usato per studiare la stabilità nella formazione di reti tra fazioni terroristiche in Iraq e Siria dal 2006 al 2016[3].

Ci ricorda James Der Derian, pioniere del campo, che il termine quantum diplomacy nasce da una conversazione tra il fisico Sidney Drell e il Segretario di Stato George Shultz del Presidente Reagan, quando il primo osservò che quando in fisica si osserva qualcosa, l'oggetto dell'osservazione cambia, a cui il secondo rispose che è sufficiente mettere una telecamera a osservare qualcosa che immediatamente cambierà l'oggetto dell'osservazione. A prescindere dal fatto che il concetto di quantum diplomacy è ancora in corso di definizione e richiede un percorso di avvicinamento tra tematiche distanti come la fisica quantistica e le relazioni internazionali, un percorso potenzialmente anche lungo, di fatto stiamo assistendo a una transizione da un'era in cui i diplomatici si impegnavano sulla regolamentazione della tecnologia (come i negoziati sul disarmo del nucleare), a una in cui si confronteranno anche in termini positivi grazie alla nuova tecnologia (intorno alla green diplomacy per vincere insieme la sfida climatica) oltre che di regolamentazione su nuove armi che si baseranno anche su di essa. In questo scenario si può concordare con chi sostiene, come Sem Fabrizi, che la diplomazia deve restare guidata dall'uomo pur essendo in futuro probabilmente coadiuvata dalle nuove tecnologie disruptive, tra cui anche quelle quantistiche, fermo restando che il diplomatico resti al centro dell'analisi.

Per quanto concerne l'impiego indiretto, ancora possiamo portare alcuni esempi concreti. Esiste una competizione sull'intelligenza artificiale tra Stati Uniti e Cina, che negli ultimi anni ha accelerato l'inseguimento e in taluni casi ha anche superato gli Stati Uniti in termini, ad esempio, di produzione di brevetti o di finanziamenti in determinate aree. In risposta, l'ex-presidente degli USA Donald Trump, ha firmato nel 2019 l'Executive Order 13859 per mantenere la leadership americana, affermando che *"Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities"*. Anche nell'ambito dei computer quantistici, la Cina sfida la supremazia degli Stati Uniti, sia per una mera ragione di prestigio (infatti ad oggi non vi sono hardware sufficientemente potenti per risolvere problemi reali di grossa taglia, anche se le roadmap prevendono il quantum advantage nei prossimi anni, che anche per una ragione contingente. Essere più veloci

[2] Lucas, Robert F., et al. "Practical Adiabatic Quantum Computing: Implications for the Simulation Community." the Proceedings of the Interservice/Industry Simulation, Training and Education Conference, Orlando, Florida. 2013.

[3] Ambrosiano, John Joseph, Randy Mark Roberts, and Benjamin Hayden Sims. Using the D-Wave 2X quantum computer to explore the formation of global terrorist networks. No. LA-UR-17-23946. Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2017

dell’avversario a calcolare lo scenario più rapidamente, porta a un significativo vantaggio di posizione, dal momento che si configura come prevedere il futuro.

Non serve la sfera di cristallo per indovinare che il controllo dello scenario geopolitico sarà appannaggio delle potenze che meglio avranno saputo trarre beneficio dall’applicazione delle tecnologie deep tech e di metodi di analisi evoluti, più potenti di quelle dei competitors, se non degli avversari. Per converso, questa tecnologia non può portare a nessun vantaggio per la società se non sarà accompagnata da una consapevole maturazione della sfera etica, della componente sociale, della trasparenza e del rispetto dei diritti e della privacy. Si tratta di una sfida interdisciplinare che richiede l’impegno di tutti gli stakeholder, e di una sintesi che solo la politica, l’arte della misura così come intesa da Platone, può restituire.

Capitolo I

È POSSIBILE QUANTIZZARE LE RELAZIONI INTERNAZIONALI?

di Enrico Prati

SINTESI: È possibile applicare le categorie di pensiero proprie della teoria quantistica alle scienze sociali, incluse le relazioni internazionali. La quantum social science è quella scienza che si pone come obiettivo di investigare i problemi delle scienze sociali, siano esse l'economia, la finanza, la psicologia, la sociologia, con l'ausilio dei metodi formali sviluppati nella teoria quantistica. I concetti di discontinuità (quantizzazione), di complementarità, di indeterminazione, e così via, si adattano a descrivere qualitativamente i fenomeni sociali ed economici inclusi quelli inerenti le relazioni internazionali, come ad esempio lo scambio della moneta, un referendum verso una secessione, l'identità nazionale e lo stato dei rapporti tra Paesi. Tali analogie qualitative costituiscono una base per una modellizzazione anche quantitativa, che consente analisi predittive come avviene nel caso della quantum decision theory.

1. DECODIFICARE I SISTEMI SOCIALI

Da alcuni anni è in corso una riflessione che sta incontrando riscontri in ambito diplomatico intorno all'obiettivo di quantizzare le relazioni internazionali, nel senso di applicarvi i concetti fondamentali della teoria quantistica. Questo connubio tra un ramo delle scienze sociali e una teoria fondamentale della fisica offre da un lato spunti stimolanti per entrambe le discipline e una prolifica interazione, ma al tempo stesso si presta a possibili abusi di linguaggio, interpretazioni errate e sopravvalutazioni. Come avvenuto in passato tra la fisica e la filosofia, per conseguire risultati apprezzabili sul piano gnoseologico, metodologico e anche predittivo, è necessario che i rappresentanti delle due discipline, di formazione differente e complementare, compiano un passo di avvicinamento costruendo in primo luogo tale linguaggio comune, conferendo alla discussione il rigore dei propri argomenti, ma nella consapevolezza dei propri limiti quando progressivamente ci si allontana dal proprio ambito di competenza. Il primo passo consiste nel dare un significato condiviso all'espressione "quantizzare le relazioni internazionali", ripercorrendo il percorso già avviato nel recente passato da alcuni pionieri dal campo, non senza avere prima introdotto i concetti fondamentali – anche in una prospettiva storica, portati da quello che si candida a essere uno strumento evoluto di analisi e di predizione degli scenari geopolitici, appunto la teoria quantistica.

Nei primi anni dopo la sua nascita, consolidata sul finire degli anni '20 del XX secolo, la meccanica quantistica si presentava più come un puzzle di formulazioni matematiche accomunate da un approccio generale e applicate a una serie di esperimenti, che non una loro teorizzazione unificante e onnicomprensiva. Per

questo motivo, tra i contributi dei padri fondatori come Heisemberg, Schroedinger, Bohr, Fermi, Dirac e Pauli, spicca quello di John Von Neumann, un fisico ungherese naturalizzato negli Stati Uniti. Von Neumann, infatti, fu in grado di formulare in un unico quadro gli assiomi della meccanica quantistica insegnati ancora oggi, tali da poter ricomprendere tutto quanto era stato formalizzato fino ad allora in un modo coerente[4]. Rappresentativo in questo contesto è però l'ulteriore fatto che egli fu in grado non solo di formulare matematicamente la teoria della meccanica quantistica, ma che a lui dobbiamo anche l'invenzione della teoria dei giochi in ambito economico[5], quella successivamente ripresa e portata avanti dall'economista John Nash[6]. Non è un caso se la persona – seppure eccezionale – che ha formalizzato la meccanica quantistica è al tempo stesso quella che ha applicato la matematica ai sistemi in cui si devono calcolare le scelte razionali, siano esse di ordine economico, politico o sociale. Infatti, i sistemi in cui è coinvolto, ad esempio, un meccanismo di ricompensa e punizione possono essere formulati in modo quantitativo e molti strumenti di analisi elaborati nell'ambito della fisica per descrivere i sistemi sperimentali trovano anche diretta applicazione nei sistemi sociali.

Il fatto che nello specifico i metodi propri della meccanica quantistica possano essere riconvertiti per spiegare meglio – e quindi necessariamente anche prevedere più accuratamente, i fenomeni descritti dalle discipline che ricadono nelle scienze sociali – quindi un ambito anche molto più vasto di quello delle relazioni internazionali, è stato oggetto di studio accademico a partire già dal 1978. In quell'anno il fisico matematico Asghar Qadir ha teorizzato che il processo di decision-making possa essere meglio descritto da un approccio matematico di tipo quantistico[7] invece che modellizzando il decisore in modo meccanicistico, cioè soggetto a forze basate sull'utilità e la disutilità – come si assume per l'uomo economico razionale dell'economia neoclassica.

Un compendio di tali applicazioni è stato formulato da Haven, Khrennikov e Khrennikov[8] , con un excursus che parte, in primo luogo, dalla stessa definizione di quantum social science come quella che *"...has as goal to investigate problems within the wide remit of the social sciences; be it economics, finance, psychology, sociology or other domains of inquiry; with the help of formal models and concepts used in quantum physics".* Nel libro sono identificate quattro categorie di problemi quantitativi che beneficiano dell'impiego dei metodi matematici della meccanica quantistica, cioè l'asset pricing in ambito finanziario, la scienza delle decisioni

[4] Birkhoff, G., & Von Neumann, J. (1936). The logic of quantum mechanics. Annals of mathematics, 823-843.
[5] Von Neumann, J., & Morgenstern, O. (2007). Theory of games and economic behavior. Princeton university press.
[6] Nash, J. (1951). Non-cooperative games. Annals of mathematics, 286-295.
[7] Qadir, A. (1978). Quantum economics. Pakistan Economic and Social Review, 16(3/4), 117-126.
[8] Haven, E., Khrennikov, A., & Khrennikov, A. I. (2013). Quantum social science. Cambridge University Press.

(decision making), la teoria dei giochi quantistica e una categoria di nuovi concetti delle scienze sociali, tra cui per fare un esempio l'applicazione del principio di indeterminazione di Heisemberg ai sistemi sociali[9].

Athalie e Haven[10] riprendono e portano oltre questa analisi, identificando a partire dal XXI secolo una corrente di pensiero scientifico interdisciplinare che si pone l'obiettivo di sviluppare modelli matematici che impiegano gli strumenti originariamente concepiti per descrivere la realtà quantistica, con il fine di spiegare determinati processi socio-economici e del comportamento umano. Una componente essenziale che viene impiegata in tali applicazioni consiste nella natura probabilistica della meccanica quantistica, che significa che essa non produce risultati certi ma stima la probabilità che un determinato evento si verifichi. Di nuovo, i campi di applicazione vanno dal decision making alla finanza, ma si estendono nell'analisi dei dati socio-economici prendendo in considerazione gli stessi aspetti fisici piuttosto che puramente matematici della fisica quantistica.

Nel solco di questo approccio innovativo alle scienze sociali si collocano i contributi pionieristici rispettivamente di Der Derian[11] e di Hundt[12], che combinano tali nuove metodologie con lo specifico campo delle relazioni internazionali. L'ipotesi è che le relazioni internazionali e l'ambito geopolitico in generale si prestano a una concettualizzazione che può trarre beneficio da una applicazione dei principi che regolano la meccanica quantistica. Nel seguito di questo Capitolo si descrivono le affinità concettuali tra la meccanica quantistica e le relazioni internazionali, gli ambiti di applicazione che sono stati riportati in letteratura, e alcune considerazioni critiche e sui limiti di validità dell'applicazione di questo approccio. Facendo nuovamente riferimento alla ricerca della stima delle probabilità di un determinato evento, sia esso una crisi militare, un crollo dei mercati[13,] o il default di uno stato sovrano, si tratta di un aspetto centrale delle precondizioni a una decisione in ambito internazionale. In questo Capitolo I si esamina in particolare la quantum diplomacy con un taglio di tipo concettuale e qualitativo, inerente l'applicazione delle categorie di pensiero che derivano dai peculiari aspetti della teoria quantistica. Nel Capitolo II invece si esamina l'applicazione quantitativa della teoria quantistica alle scienze sociali e in particolare al caso delle relazioni internazionali.

Entrambi i Capitoli sono sviluppati in accordo a due capisaldi concettuali, il primo dei quali – riproponendo un'osservazione proprio di Der Derian e di Wendt,

---

[9] Baaquie B. (2005). Quantum finance. Cambridge University Press; Cambridge.

[10] Athalye, V., & Haven, E. (2021). Socio-Economic Sciences: Beyond Quantum Math-like Formalisms. Quantum Reports, 3(4), 656-663

[11] Der Derian, J., & Wendt, A. (2020). 'Quantizing international relations': The case for quantum approaches to international theory and security practice. Security Dialogue, 51(5), 399-413.

[12] Wendt, A. (2015). Quantum mind and social science. Cambridge University Press.

[13] Ding, Y., Gonzalez-Conde, J., Lamata, L., Martín-Guerrero, J. D., Lizaso, E., Mugel, S., ... & Sanz, M. (2019). Towards prediction of financial crashes with a D-Wave quantum computer. arXiv preprint arXiv:1904.05808.

che a fronte dell'onda tecnologica che si sta manifestando mediante le nuove tecnologie quantistiche, è meglio precorre che non seguire l'emergere del fenomeno preparandosi al linguaggio e agli strumenti che gli saranno propri; il secondo è quello della valorizzazione di questi strumenti concettuali in una logica di interesse nazionale.

2. RELAZIONI INTERNAZIONALI: QUANDO SCAMBIANDO L'ORDINE DEI FATTORI IL RISULTATO CAMBIA

Al fine di creare un linguaggio comune tra professionisti delle relazioni internazionali e gli studiosi delle scienze e tecnologie quantistiche, è importante chiarire preliminarmente che vi sono due approcci alternativi nel coniugare le scienze sociali e la meccanica quantistica: quello che rientra nel quadro del fisicalismo, che postula che le scienze sociali siano derivabili da principi primi fondati nella fisica – un approccio considerato superato e che non sarà discusso in questa sede, e l'approccio che Orrell[14] chiama quantum-like, che invece intende solo impiegare i medesimi concetti e strumenti matematici che derivano dalla fisica quando questi si mostrano essere incidentalmente efficaci a questo scopo, grazie a una analogia formale favorevole – la cui ragione ultima non è oggetto di ulteriore investigazione.

L'efficacia di tali strumenti matematici trova ragione d'essere più per il fatto che in ultima analisi la teoria manipola informazione, dal momento che si trattano probabilità, informazione e osservabili, piuttosto che enti fisici tangibili.

In questo paragrafo sono illustrati i concetti salienti della meccanica quantistica e casi esemplificativi in cui tali proprietà sono riconoscibili nei sistemi sociali e in particolare nelle relazioni internazionali, per introdurre l'abitudine a una modalità di pensiero non convenzionale grazie al riconoscimento di pattern che si riconducono allo schema quantistico.

[14] Orrell, D. (2020). The value of value: A quantum approach to economics, security and international relations. Security dialogue, 51(5), 482-498.

2.1 TEORIA, SCIENZA E TECNOLOGIA QUANTISTICA

Il primo spunto per la creazione di un substrato di linguaggio comune consiste nel distinguere tra tre ambiti connotati e accomunati dall'aggettivo "quantistico", ma al tempo stesso chiaramente distinte tra loro. Per teoria quantistica si intende quell'insieme di princìpi, come il principio di sovrapposizione, e di regole matematiche – che rappresentano vere e proprie leggi fisiche, come la celebre equazione di Schroedinger, che vanno a costituire l'ossatura formale della meccanica quantistica. La teoria quantistica si basa su alcuni princìpi e su determinate regole di inferenza quantitative che consentono soprattutto di calcolare le probabilità di un intero spettro di possibilità di uscita, e la previsione del futuro – in modo probabilistico – a partire da condizioni iniziali date. È curioso notare come non vi sia in realtà una sola teoria quantistica, ma molte versioni con grado di generalità crescente[15]. Generalmente quella cui si fa riferimento è la teoria originale di Bohr, che è stata poi ampliata da Dirac e a versioni con strutture matematiche ancora più complesse, per cui è sorprendente come la versione più semplice e quindi anche superata risulti ancora eccellente per le applicazioni nelle scienze e nelle tecnologie quantistiche come discusso a seguire.

Con il termine di scienze quantistiche si vanno a indicare tutte quelle discipline che estendono il proprio ambito di competenza grazie all'inclusione di metodi o effetti quantistici, che vanno dalla biologia quantistica[16], alla teoria delle decisioni quantistica[17], alla finanza quantistica[18]. In questo ambito si vuole collocare anche la diplomazia "quantistica"[19].

Le tecnologie quantistiche sono infine costituite dall'ingegnerizzazione dei processi basati su oggetti nanometrici che rivelano proprietà quantistiche, al fine di isolare, trasferire e processare informazione quantistica. Le tecnologie quantistiche, che sono discusse nel Capitolo II, possiedono uno scopo applicativo. La menzionata informazione quantistica si basa sulla generalizzazione dei bit (binary digits) di informazione, in un altrettanto coerente versione quantistica. L'unità fondamentale è il qubit (quantum bit), che non è altro che un bit che – quando interrogato – restituisce un valore casuale che dipende dalle leggi della meccanica quantistica. Anche se questo può risultare contro-intuitivo, questo tipo quantistico di bit abilita i teorici a inventare un nuovo tipo di algoritmi e nuovi tipi di

[15] Prati, E. (2017). Mente artificiale. Cap. 3, EGEA Editore.
[16] Lambert, N., Chen, Y. N., Cheng, Y. C., Li, C. M., Chen, G. Y., & Nori, F. (2013). Quantum biology. Nature Physics, 9(1), 10-18.
[17] Yukalov, V. I. (2020). Evolutionary processes in quantum decision theory. Entropy, 22(6), 681.
[18] Focardi, S., Fabozzi, F. J., & Mazza, D. (2020). Quantum Option Pricing and Quantum Finance. The Journal of Derivatives, 28(1), 79-98.
[19] Agliardi, G., & Prati, E. (2022). Optimal tuning of quantum generative adversarial networks for multivariate distribution loading. Quantum Reports, 4(1), 75-105.

protocolli, che impiegano le proprietà quantistiche inclusa la “casualità controllata” dei qubit.

2.2 LE CATEGORIE DELLA TEORIA QUANTISTICA APPLICATE ALLE RELAZIONI INTERNAZIONALI

Senza entrare nei dettagli matematici e tecnici della teoria della meccanica quantistica, possiamo distinguere numerosi esempi di cambio di paradigma concettuale rispetto alla storia della scienza precedente, che questa teoria ha apportato, e che sono stati poi ben formalizzati anche quantitativamente. Tali categorie concettuali includono il discontinuo (l’essere quantizzato), la complementarietà, l’indeterminazione, l’induzione del collasso del sistema a seguito di un processo di misurazione, la sovrapposizione, l’entanglement e la non-commutazione delle operazioni. Tutte queste categorie trovano naturale applicazione anche nell’ambito dello studio delle relazioni internazionali.

Contrariamente a quanto ritenuto da Leibniz, che sosteneva che *natura non facit saltus*, alla scala nanometrica la natura rivela invece come le proprietà non possano essere piccole a piacere ma che le quantità cambiano a piccoli salti, detti appunto quanti, mentre i valori intermedi sono proibiti. La quantizzazione ha sconvolto gli assi portanti della scienza un secolo fa e ha introdotto novità di carattere concettuale. In realtà la quantizzazione è un concetto familiare a tutti nel quotidiano, ad esempio nello scambio della moneta. Tutti sono abituati all’idea che vi sia un taglio minimo nella moneta, come il centesimo di euro o di dollaro americano e che non sia possibile scambiare quantità inferiori, come mezzo centesimo. Nella teoria quantistica, questo vale ad esempio anche per lo scambio di quantità di energia. Questo semplice esempio mostra come non vi sia nulla in sé di rivoluzionario in un concetto che fa da caposaldo di una rivoluzione scientifica, mentre la novità consiste nell’aver importato della scienza un concetto comune nell’ambito economico e sociale. In certi casi, come in questo esempio, applicare i concetti propri della meccanica quantistica alle scienze sociali è in realtà un ritorno alle origini, dove però il bagaglio con cui si ritorna porta con sé, analogamente al Voyager 6 di fantasia del primo film di fantascienza di Star Trek, nuova conoscenza che deriva dai confini dell’Universo – in questo caso mutuato dalle dinamiche del molto piccolo.

Un altro dei concetti sviluppati nel contesto della meccanica quantistica è il principio di complementarietà. Esso fu enunciato da Niels Bohr nel 1927 per andare incontro al paradosso che talvolta la luce si comporta da onda e talvolta da particella corpuscolare. La soluzione fu di riconoscere che entrambi i comportamenti sono possibili ma al tempo stesso mutualmente esclusivi, in quanto dipendenti anche dalla natura del tipo di misurazione che viene applicato nella

circostanza. Per trasferire questo concetto all'ambito delle relazioni internazionali, possiamo fare riferimento alla recente crisi in Ucraina. Se la Russia avesse proposto dei trattati economici all'Ucraina, sarebbe stato possibile conoscere la sua volontà di cooperazione economica, mentre l'aggressione militare sul suo suolo ha consentito di conoscerne la capacità di risposta militare. Una volta causato lo scenario attuale di crisi militare, non è più possibile conoscere quale sarebbe stata la reazione da parte dell'Ucraina se la Russia avesse proposto dei trattati economici. Conoscere questi due aspetti è alternativo, dal momento che essi non si possono verificare contemporaneamente e si devono quindi considerare complementari. A questo è collegato il concetto di indeterminazione, che nella teoria quantistica afferma che l'accuratezza con cui è nota una grandezza influisce (negativamente) sulla possibilità di conoscere quella di una grandezza complementare, fino al caso limite in cui una perfetta conoscenza di una di esse impedisce del tutto la conoscenza della variabile complementare.

Una categoria rilevante è poi quella di collasso del sistema quando si effettua una misurazione, collegato a quello di sovrapposizione quantistica. La teoria quantistica afferma infatti che fino al momento della misurazione, la variabile che descrive il sistema non assume nessun preciso valore, mentre è l'atto stesso della misura che fa collassare il sistema su un risultato piuttosto che un altro. Con il collasso, uno solo dei potenziali diventa atto. La peculiarità della teoria quantistica è che fino al momento della misurazione, supponendo che il sistema possa trovarsi in due stati alternativi, esso si mantiene in una sovrapposizione di entrambi tali stati possibili. A questo riguardo, la sovrapposizione quantistica (in inglese super-position), fondamentale ad esempio nel calcolo quantistico, è realizzata da particelle che possiedono allo stesso tempo una miscela di diverse proprietà, anche opposte: mentre un pallone da calcio può ruotare in un solo verso per volta, è come se un atomo potesse essere fatto ruotare su se stesso in entrambe le direzioni contemporaneamente. I due concetti di sovrapposizione e di collasso del sistema a seguito della misurazione si adatta bene a descrivere ad esempio quanto avviene quando una popolazione è chiamata a esprimere un voto. Facendo riferimento, ad esempio, al referendum che ha interessato il Regno Unito nel 2016, dal momento in cui il referendum è stato ammesso, il futuro del Regno Unito era duplice: restare nell'Unione Europea oppure uscirne. In termini quantistici, il Regno Unito era in una sovrapposizione potenziale tra i due stati futuri, che non sono diventati atto fino al momento del voto. Il voto ha causato il collasso del potenziale futuro del Regno Unito su uno solo dei due stati possibili: ha vinto il fronte pro-Brexit e da quel momento il futuro del Regno Unito si è disaccoppiato da quello con l'Unione Europea.

Per portare un altro esempio sugli effetti della misurazione come atto condizionante il sistema sotto osservazione, Wendt nota come lo stesso linguaggio

costituisca un apparato di misurazione, che possiede un impatto su ciò che è osservato. Egli afferma che[20] *"in language what brings about a concept's collapse from potential meanings into an actual one is a speech act, which may be seen as a measurement that puts it into a context, with both other words and particular listeners"*. Il collasso dovuto alla misurazione inizia con la decisione di comunicare un significato piuttosto che un altro, che dipende a sua volta dall'ascoltatore, la cui comprensione dipende da come tale linguaggio evoca la sua memoria. Un altro esempio dell'effetto della misurazione che forza il sistema a collassare su un valore preciso a discapito di tutti i possibili valori potenziali alternativi, proviene dalla finanza. In quel contesto, infatti, il prezzo e la volatilità di un titolo azionario può solo essere misurato attraverso le stesse transazioni, che a loro volta alterano tali variabili.

Tra i fenomeni più peculiari della meccanica quantistica vi è l'entanglement. Esso rivela come, a livello fondamentale, le particelle che sono appartenute in origine al medesimo sistema restino collegate tra di loro e le sorti dell'uno continuano a causare conseguenze anche sull'altro. Come esempio di entanglement adattato alle relazioni internazionali, si può considerare un'etnia caratterizzata da un senso di identità nazionale ma che per ragioni storiche è stata suddivisa sul territorio di diversi Stati, come è avvenuto per i Curdi che si trovano distribuiti tra Turchia, Iran, Iraq e Siria e in Europa. Queste comunità, anche se dislocate su diversi Stati e presenti a seguito dell'immigrazione anche in Occidente, continuano a restare collegate e a influenzarsi. Quando negli anni '80 vi fu la persecuzione dei Curdi in Iraq, decine di migliaia di Curdi cercarono rifugio in Iran e Turchia, o ancora gli attivisti curdi in occidente si sono uniti alle proteste dei Curdi iraniani per la condanna a morte e l'esecuzione nel 2020 dell'attivista curdo Heidar Ghorbani in Iran.

Per ultimo, prendiamo in considerazione la non-commutatività delle operazioni nell'ambito delle relazioni internazionali. In genere siamo abituati a considerare operazioni che commutano: cambiando l'ordine nella somma dello scontrino della spesa, il risultato del totale non cambia. Nella teoria quantistica invece si impiegano matrici di numeri al posto dei numeri e per questo motivo le operazioni utilizzate non commutano. Questo concetto apparentemente poco intuitivo, tuttavia, si può rappresentare in modo molto naturale nell'ambito delle relazioni internazionali. Se le operazioni che si considerano sono ad esempio un'ingerenza di una potenza straniera mediante un social medium che prende di mira un Segretario di un partito, e l'altra è una consultazione elettorale nel Paese, il fatto che l'ordine con cui queste avvengano sia rilevante è molto ovvio: un eventuale scandalo politico pochi giorni prima del voto ha effetti molto diversi che se questo viene approcciato solo dopo che le elezioni sono già avvenute. Si pensi, come esempi, al ruolo dell'ordine cronologico nello scandalo che investì Hillary Clinton

[20] Wendt, A. (2015). Quantum mind and social science. pag. 217. Cambridge University Press.

nel 2016 pochi giorni prima delle elezioni in USA, o all'influenza di Cambridge Analytics sulle campagne di diversi politici, sulla Brexit nel 2016 e sulle elezioni in Messico nel 2018.

Questa serie di categorie concettuali, riprese da diversi autori negli ultimi anni, dimostra come la teoria quantistica sia generale a sufficienza da poter essere adattata qualitativamente alle relazioni internazionali e offra prospettive e spunti di riflessione mediante la loro applicazione.

3. CONSIDERAZIONI CRITICHE SULLA QUANTIZZAZIONE QUALITATIVA DELLE RELAZIONI INTERNAZIONALI

A fronte delle analogie e dei punti di contatto elencati, vi sono anche considerazioni di cautela o scettiche per quanto riguarda l'approccio qualitativo alle relazioni internazionali basato sui concetti che derivano dalla meccanica quantistica. La prima critica consiste nel fatto che tale approccio si basa su affinità di natura puramente empirica. In altre parole, non vi è un motivo di carattere intrinseco o teoretico per il quale determinati fenomeni o scenari di tipo geopolitico si prestino a essere descritti con concetti che derivano dall'ambito quantistico. Si tratta più di una constatazione di uno stato di fatto, che consente di mettere in luce con maggior consapevolezza le caratteristiche di uno scenario e descriverlo più accuratamente. Questo aspetto mette in luce il carattere circoscritto e non universale dell'applicazione qualitativa dei concetti quantistici alle relazioni internazionali. Di conseguenza, non vi è alcuna teoria generale i cui casi specifici si declinano sugli scenari di interesse, ma vi sono corrispondenze puntuali tra lo spazio degli scenari possibili che richiedono una descrizione, e le categorie messe in luce dalla meccanica quantistica.

Il secondo problema che emerge da questo approccio risiede nel fatto che l'applicazione delle sole categorie senza che vi sia una quantificazione che consente la formulazione di modelli, espone all'impossibilità di effettuare previsioni. Ci si limita a dare un cambio di prospettiva per far emergere ulteriore comprensione di un determinato scenario, consentendo di identificare ad esempio eventuali vincoli, oppure relazioni tra grandezze mutuamente esclusive che sono di volta in volta accessibili. Le previsioni invece possiederebbero una duplice natura: di carattere informativo, dal momento che consentono di stabilire qualcosa del futuro, e di carattere ontologico. A quest'ultimo riguardo, grazie a una successiva investigazione empirica, esse consentono infatti di smentire o confermare il modello. Questo è un aspetto fondamentale della scienza moderna,

ovvero controllare sia la verificabilità che anche la falsificabilità del modello, secondo l'accezione di Karl Popper[21].

Come è descritto nel Capitolo II, è possibile elaborare ulteriormente questi modelli qualitativi, e arrivare quindi a una fenomenologia quantitativa, basata su leggi matematiche che descrivono i fenomeni sociali. Ad esempio, come nel caso della quantum decision theory: essa impiega, invece di una logica della probabilità basata su elementi booleani legati da delle alternative di tipo OR, un inclusivo AND.

La consapevolezza di questo potenziale non deve tuttavia indurre a trascurare l'importanza che può rivelare l'applicazione delle categorie quantistiche menzionate sopra, quando si tratta di valutazione uno scenario geopolitico. In primo luogo, se impiegate come strumento di analisi, esse possono essere di supporto nella comprensione di un uno scenario o di un processo, inclusa l'analisi degli eventuali limiti alla conoscenza conseguibile. Si pensi a questo riguardo l'identificazione di proprietà complementari su uno scenario, che implica che conoscerne una rende impossibile conoscere contemporaneamente l'altra. In secondo luogo, possono offrire spunti verso l'elaborazione di una corrispondente teoria quantitativa, che sarà basata su una corretta codifica delle variabili e dei processi coinvolti. Per concludere, citando de Freitas e Sinclair[22] : *"We ask the reader to bear in mind, however, that any formal system will involve massive limitations and brutal simplifications. Probabilistic models of cognition are top-down – any such formalism will misrecognize much of the dynamic nature of events. But our aim is not to argue that quantum probability explains human judgment definitively – as that would go against the grain of the quantum – but rather to trouble reliance on classical probability and to invite speculation and experiment around different ways of reasoning with uncertainty".*

[21] Karl R. Popper, La scienza, congetture e confutazioni, in Congetture e Confutazioni, trad. it., Bologna, Il Mulino, pp. 68-69.

[22] de Freitas, E., & Sinclair, N. (2018). The quantum mind: Alternative ways of reasoning with uncertainty. Canadian Journal of Science, Mathematics and Technology Education, 18(3), 271-283.

CONCLUSIONI:

- La teoria quantistica impiega concetti, alcuni dei quali di uso corrente che, formalizzati nella teoria stessa, forniscono una base di analisi anche nelle scienze sociali
- È possibile utilizzare la teoria quantistica per descrivere scenari studiati nelle relazioni internazionali
- Un modello basato sull'uso qualitativo della teoria quantistica applicato a uno scenario di interesse nelle relazioni internazionali può facilitare lo sviluppo di modelli quantitativi evoluti che calcolano previsioni, ad come esempio la teoria quantistica delle decisioni

Capitolo II

TECNOLOGIE QUANTISTICHE E RELAZIONI INTERNAZIONALI

di Enrico Prati

SINTESI: I sensori quantistici (con la metrologia), le comunicazioni quantistiche, e i computer quantistici (con i simulatori) sono in grado rispettivamente di generare dati quantistici, spostare dati quantistici - garantendo integrità e sicurezza, e processarli con algoritmi appositi. Gli USA, e poi altre potenze, hanno finanziato la ricerca in questi campi con piani di investimento di alcuni miliardi di dollari. Gli USA sono leader per i computer quantistici mentre la Cina – che ha beneficiato della ricerca dell'Occidente – nelle comunicazioni quantistiche. Le aspettative nei confronti di queste tecnologie devono essere commisurate ai limiti che lo sviluppo in corso cerca di superare, ma vi sono argomenti per non temere un quantum winter dopo questa fase di hype. Quanto all'utilizzo, i computer quantistici possono essere direttamente impiegati nello studio delle scienze sociali e in particolare delle relazioni internazionali, di cui si riporta come esempio la dinamica delle reti terroristiche in Medio Oriente.

1. VERSO L'INTRODUZIONE DELLE TECNOLOGIE QUANTISTICHE

Nel corso dell'ultimo secolo si sono succedute una serie di rivoluzioni tecnologiche, talmente ravvicinate che non c'è stato il tempo che si esaurisse lo sviluppo di una, che un'altra era già in piena accelerazione. Oltre alla spinta data dall'elettromagnetismo di Maxwell, alla base di queste rivoluzioni vi sono state la meccanica quantistica e la relatività ristretta, che hanno ampliato la visione che avevamo del mondo, condizionata dall'esperienza quotidiana incapace per sua natura percepire i fenomeni nel molto piccolo e nel molto veloce, fino alla velocità della luce. Nell'ordine, dopo i radar e la tecnologia a microonde la scienza ha prodotto la tecnologia nucleare, la tecnologia dei semiconduttori e dei circuiti integrati, dei laser e delle telecomunicazioni, che hanno portato a sviluppare i computer e la rete internet, da cui la fase matura dell'intelligenza artificiale, fino alle nanotecnologie. Le tecnologie quantistiche sono il prodotto di queste onde successive di innovazione, grazie al controllo a livello nanometrico - praticamente a scala atomica - dei materiali e delle fabbricazioni, e a strumenti di progettazione evoluti e dotati di elevata potenza di calcolo, che consentono di simulare i dispositivi, i sensori e i processi senza bisogno di realizzarli realmente fino a che il progetto non sia indirizzato. Grazie a tutti questi ingredienti, e a modelli teorici potenti, da circa venti anni è possibile pensare realisticamente di fabbricare dispositivi, strumenti e apparati che ricadono sotto il nome di tecnologie quantistiche. Queste sono accomunate dal fatto di codificare o di processare l'informazione direttamente in oggetti generalmente nano-strutturati (fatta eccezione per i superconduttori che lo consentono anche con una micro-strutturazione) al punto da esibire in modo diretto le proprietà caratterizzanti la

meccanica quantistica elencate nel Capitolo 1. Non è sufficiente, infatti, che la meccanica quantistica entri semplicemente in gioco, come avviene indirettamente già da settant'anni per i normali semiconduttori: l'aspetto qualificante e nuovo consiste nel codificare o processare l'informazione mediante gli stati quantistici stessi, in modo diretto, siano essi basati su singoli elettroni, singoli atomi, da superconduttori, o da quanti di luce - detti fotoni.

Le tecnologie quantistiche ricadono in tre grandi famiglie: quella delle comunicazioni quantistiche, quella del calcolo quantistico (incluse le simulazioni), e infine quello dei sensori quantistici, in cui si può far ricadere anche la metrologia.

I sensori quantistici sfruttando la meccanica quantistica possono possedere maggiore sensibilità, anche al di sotto della soglia del rumore, e sono in grado di generare anche dati già in formato quantistico, e quindi compresso grazie alla natura quantistica del supporto fisico. Vi sono sensori di gravità, sensori di molecole chimiche, per fare degli esempi, e si parla di quantum radar e di quantum imaging[23] .

I computer quantistici, a partire dalla fondazionale conferenza di IBM e MIT "The Physics of Computation" tenutasi alla Endicott House dell'MIT a Dedham in Massachusetts dal 6 all'8 Maggio del 1981, furono concepiti in origine per dissipare meno energia sfruttando processi reversibili, ma con la scoperta degli algoritmi quantistici che aumentavano smisuratamente la potenza di calcolo – algoritmi che si possono eseguire solo su computer quantistici - l'interesse è stato rivolto quasi esclusivamente alla potenza di calcolo che ne deriva[24] . Per fare un esempio, vi sono problemi che un computer quantistico potrà[25] risolvere in minuti o ore, che un computer normale non risolverebbe nel tempo di vita dell'Universo (da cui si parla di quantum speed-up).

Le comunicazioni quantistiche invece hanno sia lo scopo di garantire la sicurezza e l'integrità della comunicazione impiegando gli stati quantistici della luce (quantum key distribution)[26], ma anche quello di trasportare i dati quantistici generati dai sensori, o quelli che escono da un computer quantistico per arrivare a un computer quantistico remoto (quantum internet)[27].

Le tecnologie quantistiche coprono l'intera filiera del data processing: i sensori quantistici aumentano i nostri sensi e contribuiranno a un quantum internet of things, le comunicazioni quantistiche potranno trasportare questi dati in modo

---

[23] Lanzagorta, M. (2013, May). Amplification of radar and lidar signatures using quantum sensors. In Active and Passive Signatures IV (Vol. 8734, pp. 83-93). SPIE.

[24] Prati, E. (2017). Mente artificiale, Capitolo 3. EGEA

[25] A oggi non è ancora disponibile un computer quantistico universale di potenza sufficiente per risolvere problemi arbitrari con un sistematico vantaggio computazionale. Per questo motivo attualmente ci si limita a convincenti dimostrazioni di principio su piccola scala.

[26] Cavaliere, F., Prati, E., Poti, L., Muhammad, I., & Catuogno, T. (2020). Secure quantum communication technologies and systems: From labs to markets. Quantum Reports, 2(1), 80-106.

[27] Cuomo, D., Caleffi, M., Krsulich, K., Tramonto, F., Agliardi, G., Prati, E., & Cacciapuoti, A. S. (2021). Optimized compiler for Distributed Quantum Computing. arXiv preprint arXiv:2112.14139.

integro e sicuro, e i computer quantistici processeranno tali dati. L'impulso a questa onda di tecnologia è stato impresso con le due Roadmaps di ARDA[28] sui computer quantistici e sulle comunicazioni quantistiche nel 2004. Oggi molte delle idee di vent'anni fa sono state realizzate, ma è necessario essere cauti nel valutare l'impatto e la robustezza di queste tecnologie. Ciascun sensore, dispositivo, circuito, apparato, è portato al proprio limite tecnico e opera in condizioni estreme in termini di sensibilità e di esposizione a interferenze. Dal momento che gli stati quantistici sono difficili da isolare e sono molto fragili, e quindi si deteriorano velocemente secondo il processo della de-coerenza[29], i problemi di tipo ingegneristico sono molto più rilevanti di quelli concettuali. Pertanto, è prematuro attendersi a oggi un successo commerciale, ma allo stesso tempo tutti i Governi hanno varato piani di investimento a supporto del trasferimento tecnologico di queste tecnologie per creare valore nel tessuto industriale, auspicandone l'incorporazione nelle tecnologie consuete o mediante la creazione di sistemi radicalmente innovativi. A questi, contribuiscono anche fondi di venture capital evoluti, che consentono alle startup "deep tech" di sviluppare prodotti basati sulle tecnologie quantistiche, esponendosi a logiche di grande rischio a fronte potenziali grandi benefici.

[28] Bennett, C. H., & Brassard, G. (2004). A Quantum Information Science and Technology Roadmap. Part, 2, 12. ARDA - LA-UR-04-4085

[29] Porotti, R., Tamascelli, D., Restelli, M., & Prati, E. (2019). Coherent transport of quantum states by deep reinforcement learning. Nature Communications Physics, 2(1), 1-9.

2. GEOPOLITICA E TECNOLOGIE QUANTISTICHE

Il Paese pioniere e che ha maggiormente ha investito nelle tecnologie quantistiche sono gli Stati Uniti. Forte di un sistema di finanziamento pubblico della ricerca lungimirante e meritocratico, ha avviato come già anticipato uno scouting di queste tecnologie e ha definito una roadmap tecnologica nel 2004 poi aggiornata nel 2007, che ha stimolato la ricerca principalmente nei centri pubblici.

Successivamente il finanziamento è ruotato sullo sviluppo nelle imprese e nell'arco di circa dieci anni ha prodotto diversi progetti industriali di sviluppo di un computer quantistico da parte di public companies, come quelli di Intel, di IBM, di Google e di Microsoft. L'ordine di grandezza dei finanziamenti messi in campo da questi giganti dell'industria dell'information technology nordamericana si aggira tra i 200 e i 500 milioni di dollari per ciascuno di essi, ciascuno dei quali con molte decine – anche centinaia di persone coinvolte nell'ingegnerizzazione di tutti i livelli, dallo strato hardware fino a quello delle applicazioni software. Anche il Canada ha messo in campo importanti finanziamenti e ha portato alla creazione del computer quantistico DWave, che si basa su un'architettura alternativa chiamata quantum annealing che fu proposta per la prima volta da due scienziati italiani – Bruno Apolloni e Diego De Falco nel 1988. Recentemente, in occasione dell'apertura dell'annuale High Performance Computing and Quantum Computing Workshop organizzato dall'Autore in collaborazione con il CINECA[30], i due scienziati hanno ricordato come all'epoca dei loro studi pionieristici, il numero di esperti al mondo che si occupava di questa idea contasse poche unità, mentre oggi la computazione quantistica include aziende quotate al NASDAQ come la statunitense IonQ e si insegna nei corsi di Laurea Magistrale.

In risposta, anche la Cina ha promosso lo sviluppo di progetti di quantum computing (Baidu e Alibaba) basati sul potenziamento di iniziative di ricerca pubbliche, come quello della Chinese Academy of Science (CAS). Gli scienziati cinesi che si occupano di quantum computing sono un esempio da manuale della pianificazione su scala pluridecennale della Cina e di un programma di rientro dei talenti attuato con adeguate risorse. La Cina ha riportato in patria i dottorandi e i post-doc in visita negli Stati Uniti reclutati temporaneamente nei centri di ricerca di quantum computing e li ha dotati ancora giovanissimi di cattedre universitarie e fondi consistenti per acquistare apparecchiature di avanguardia. La medesima operazione di rientro dei talenti è valsa alla Cina anche il primato nelle comunicazioni quantistiche. Dopo aver conseguito il dottorato all'Università di Vienna con il Prof. Zeilinger, universalmente riconosciuto essere uno dei fondatori

[30] D. Ottaviani, R. Mengoni and E. Prati, IV Workshop High Performance Computing and Quantum Computing Workshop, 15-16 Dicembre 2021, online

dell'informazione quantistica, Jian-Wei Pan si è spostato all'Università di Heidelberg in Germania dove ha ricevuto sostegno finanziario dell'Unione Europea, tra cui uno Starting Investigator Research Grant dell'EuropeanResearch Council dal 2008 al 2013 pari a quasi 1.5 Meur[31]. È stato quindi reclutato dalla University of Science and Techology of China (USTC) dove nel 2016 ha guidato il progetto per il lancio del primo satellite Micius del Quantum Experiments at Space Scale che nel 2017 ha dimostrato l'accoppiamento terra-spazio mediante comunicazione quantistica[32], su scala di 1200 km. Forte di questi successi, la Cina gli ha affidato anche la costruzione di un computer quantistico basato sui fotoni chiamato Zuchongzhi 2.1 che è stato dichiarato essere di un milione di volte più veloce del chip Sycamore di Google. Jian-Wei Pan continua a guidare un gruppo all'Università di Heidelberg composto per l'80% di personale cinese, ma la rete di comunicazione terra-spazio che ha conseguito il primato è costruito in Cina, che sta finanziando le ricerche sulle tecnologie quantistiche con 15 miliardi di dollari. La sola Provincia di Anhui ha varato un fondo da 1.6 miliardi di dollari per il Quantum Science Industry Development Fund.

Vi è un grande numero di eccellenti scienziati italiani nell'ambito delle tecnologie quantistiche all'estero, sia nel settore accademico che privato, ma il tasso di rientro è trascurabile. In una logica di interesse nazionale, per avvalersi delle competenze degli italiani nel mondo sarebbe necessario istituire cattedre universitarie a tempo indeterminato, vestite di un finanziamento pluriennale e collegate a spazi dedicati commisurati sul versante pubblico, e potenziare le misure di finanziamento di nuove startup sul lato privato. In questo senso poli scientifici come lo Human Technopole a Milano e il nuovo centro di High Performance Computing in costituzione a Bologna possiedono le caratteristiche che sarebbero necessarie per supportare simili iniziative.

I vari Paesi hanno affrontato con diverso atteggiamento le opportunità offerte dalle tecnologie quantistiche. Un metro dei risultati di queste politiche è leggibile mediante il numero di brevetti depositati nei vari ambiti. Emerge un distinto trend di crescita nei brevetti degli USA nell'ambito dei quantum computers, mentre altrettanto distinto è il trend nell'ambito delle comunicazioni quantistiche in Cina (Figura 1). L'Unione Europea ha approvato un programma Flagship da 1 miliardo di Euro in 10 anni tra 25 Paesi dell'Unione, con una media quindi di circa 4 milioni di Euro a Paese all'anno, che non può sostituire gli effetti dei programmi nazionali come quelli messi in campo da alcuni Paesi: per fare un esempio la sola regione del Waterloo in Canada ha messo in campo 568 milioni di dollari per l'Institute for Quantum Computing, 205 milioni di dollari nel QuantumValley Investments, e 591 milioni di dollari nel Perimeter Institute, per un totale di più di 1.3 miliardi di dollari. I

[31] https://cordis.europa.eu/project/id/202499/it

[32] Yin, J., Cao, Y., Li, Y. H., Liao, S. K., Zhang, L., Ren, J. G., ... & Pan, J. W. (2017). Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343), 1140-1144.

risultati sono stati lo sviluppo di diverse aziende di quantum computing come DWave e Xanadu per l'hardware, o come Zapata e 1Qbit per il software, o ancora di comunicazione quantistica come EvolutionQ, che valgono già di più del finanziamento messo in campo. L'investimento, quindi, ha generato valore e contribuito a una supremazia geopolitica come quantum-haves rispetto ai quantum-haves-not.

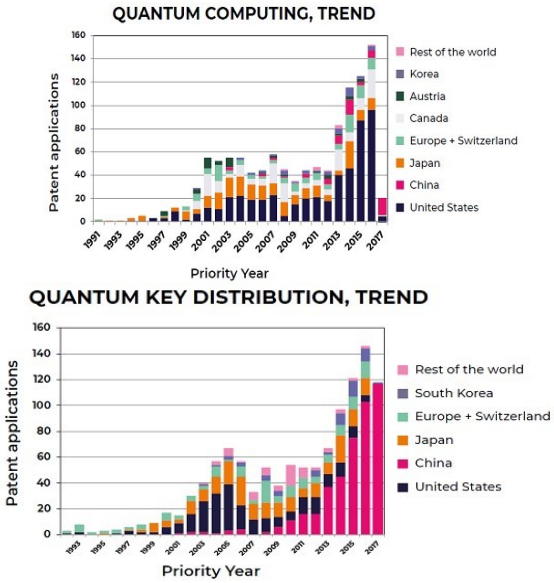


Figura 1: Numero di brevetti rispettivamente in ambito quantum computing e quantum key distribution, per Paese fino al 2017. Si osserva un lento abbandono della quantum key distribution (QKD) da parte degli Stati Uniti, che si sono concentrati sui computer quantistici, mentre la Cina ha invece investito principalmente proprio in tali comunicazioni quantistiche. Recentemente la Cina ha reimpiegato le tecnologie per la QKD anche per i computer quantistici. Il Giappone ha prodotto più brevetti dell'intera Europa. Fonte: Roadmap della Commissione Europea sulle Tecnologie Quantistiche (2018).

Anche la Russia con il finanziamento da 790 milioni di dollari al Russian Quantum Center ha deciso di rendere pubblico il proprio impegno nella competizione quantistica[33]. Conseguire l'indipendenza in termini di tecnologie quantistiche una volta che saranno arrivate alla maturità determinerà in primo luogo un vantaggio rispetto agli altri Paesi in termini di utilizzo, ma anche un quantum divide, tra i Paesi che fanno parte della cerchia di quelli con potenza computazionale superiore, maggiore awareness e sorveglianza, e comunicazioni più sicure e quelli che dipendono da loro o ne sono del tutto esclusi. Detenere tali tecnologie consente anche una conoscenza approfondita in termini delle sue vulnerabilità. È infatti necessario essere consapevoli che se da un lato le

[33] https://www.nature.com/articles/d41586-019-03855-z

comunicazioni quantistiche promettono un metodo inviolabile e garantito come sistema operante in condizioni idealizzate, è altrettanto vero che le realizzazioni pratiche fanno i conti con tutta la componente dell'elettronica di gestione dei segnali e quella della fotonica, che ha permesso negli ultimi venti anni di elaborare almeno 30 diversi attacchi noti, sia ai trasmettitori che ai ricevitori. In altre parole, la comunità scientifica ha reso pubblici un nuovo tipo di attacco alla QKD ogni 8 mesi per due decenni, senza contare quelli non pubblicati. Diversi osservatori raccomandano cautela e vi sono Agenzie che deprecano - allo stato attuale - l'impiego di metodi QKD per la codifica di messaggi di vitale importanza.

In conclusione, è presumibile attendersi che le tecnologie quantistiche svolgeranno un ruolo analogo a quello dell'intelligenza artificiale, delle telecomunicazioni e dei semiconduttori in termini di leva a livello geopolitico, sia per le ricadute economiche che esso conferisce, sia per la supremazia tecnologica che esse comporteranno in termini di controllo e processamento dell'informazione, ma vi sono in ciascuna di esse ancora dei passi importanti da compiere che includono quelli tecnologici per arrivare a prodotti robusti capaci di affrontare il mercato, ma anche quello della certificazione per rendere tali prototipi anche dei prodotti commercializzabili. A questo riguardo, vi sono iniziative di standardizzazione come quello promosso da NIST e IEEE in USA, e di certificazione come quello promosso da ETSI, di impatto potenziale elevato, in grado di decretare anche i vantaggi e gli svantaggi competitivi nello sviluppo delle future tecnologie quantistiche. Ad esempio, vi sono attualmente due iniziative per standardizzare la certificazione di sicurezza dei sistemi di QKD ISO/EN 15408 "Common Criteria" quali appunto la ETSI ISG-QKD e la ISO SC27 WG3 che è in corso di pubblicazione di tali standard. Le comunità di elaborazione di standard e certificazione sono aperte e in quanto tali penetrabili, potendo così risentire di eventuali interessi portati dagli attori che vi contribuiscono.

3. COMPUTER QUANTISTICI: HYPE O PIATTAFORMA TECNOLOGICA PER LE SCIENZE SOCIALI?

I computer quantistici rappresentano un potenziale breakthrough nell'ambito della computazione dal momento che, grazie all'impiego dei bit quantistici (i qubit), è possibile concepire e applicare algoritmi quantistici che sono in grado di ridurre anche esponenzialmente il numero di passi da compiere per arrivare alla soluzione di determinati problemi[34]. Le applicazioni esplorate vanno dall'ambito finanziario, alle energie rinnovabili[35], alla logistica, al design di nuovi materiali per l'avionica, alla chimica di batterie più efficienti, alla distribuzione nelle reti siano esse nel settore energia, traffico stradale o telecomunicazioni, e non ultima l'intelligenza artificiale nella sua versione quantistica[36].

Tuttavia, se da un lato non vi sono dubbi sul fatto che realizzare calcoli quantistici sia una realtà – si pensi ai computer quantistici in cloud messi a disposizione da IBM, DWave, Rigetti, IonQ solo per citarne alcuni - vi è invece dibattito sulla prospettiva temporale entro la quale i computer quantistici saranno in grado di ospitare problemi di taglia sufficiente da poter dare un effettivo vantaggio rispetto a quanto non si sappia già fare con i computer tradizionali.

Un importante aspetto di valutazione è che vi sono molti diversi tipi di computer quantistico. I computer quantistici seguono quattro possibili alternative di architettura computazionale (circuitale, adiabatico, one-way e topologico) che si differenziano per come i dati sono codificati e poi elaborati. Allo stesso tempo, essi possono essere realizzati nel concreto con differenti tecnologie, come i superconduttori, gli atomi nel vuoto, i semiconduttori, e i fotoni, ciascuna delle quali può essere adatta o meno alle varie architetture menzionate sopra, per cui solo determinate combinazioni di architettura e tecnologia sono effettivamente possibili. Dal 2017, il numero di qubit gestiti in un chip quantistico cresce in modo costante di anno in anno in tutte le tecnologie menzionate fino all'attuale centinaio (migliaia nel caso dell'architettura adiabatica). Anche se un confronto tra le tecnologie non è semplice, ogni anno possono esserci capovolgimenti di fronte nello stimare quali siano le tecnologie hardware con il maggiore numero di risorse computazionali, segnando un trend chiaro che assomiglia al trend di miniaturizzazione dei transistori (la legge di Moore) dei primi anni Sessanta. Le industrie, nonostante questi hardware quantistici siano di fatto dei prototipi commercializzati, hanno

[34] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.
[35] Giani, A., & Eldredge, Z. (2021). Quantum computing opportunities in renewable energy. SN Computer Science, 2(5), 1-15.
[36] Rocutto, L., Destri, C., & Prati, E. (2021). Quantum semantic learning by reverse annealing of an adiabatic quantum computer. Advanced Quantum Technologies, 4(2), 2000133.

avviato sperimentazioni su casi d'uso per non trovarsi impreparate qualora i quantum computer dovessero maturare nel loro sviluppo e offrire potenzialità di calcolo superiori rispetto a quanto già non si faccia con metodi di calcolo convenzionali. Non interessarsi di questa innovazione da parte di una grande azienda potrebbe determinare l'esclusione dal mercato in un futuro non lontano, analogamente a quanto è avvenuto dopo l'arrivo di Netflix alla nota catena di noleggio di film Blockbuster, che presidiava tutte le città dell'Occidente e sparita nel nulla. Dal momento però che il numero di risorse in termini di qubits in un processore quantistico è dell'ordine di 10-150 qubits, attualmente si possono solo provare dimostrazioni di principio su piccola scala su casi d'uso di taglia ridottissima. Si pensi ad esempio che per determinati algoritmi, per garantire di processare il calcolo, e allo stesso tempo effettuare la necessaria correzione quantistica degli errori, potrebbero servire a partire da milioni di qubits. Non si deve dimenticare infatti che il consumo di qubit è appesantito dal fatto che per proteggere l'informazione di un qubit dai disturbi ambientali e mantenerlo in vita per tutta la durata di qualsiasi calcolo, servono in media dai 100 ai 1000 ulteriori qubits.

È legittimo quindi aspettarsi che, nonostante gli importanti finanziamenti a livello globale e il coinvolgimento di early users importanti (come Airbus, JP Morgan, General Electrics, Volkwagen, DHL, solo per citarne alcuni o Banca Intesa ed ENI per restare in Italia) il protrarsi eccessivo di una situazione di sviluppo di prototipi commerciali senza ancora arrivare a un vantaggio evidente potrebbe portare l'industria a disilludersi verso la fattibilità del computer quantistico universale, dando luogo a un quantum winter.

Tuttavia, anche tenendo conto del principio di cautela che si deve mantenere quando si ha a che fare con tecnologie emergenti, vi è un argomento per non prefigurare per lo scenario attuale un futuro simile al cosiddetto AI winter, che precedette per due decenni l'epoca attuale di piena maturità dell'intelligenza artificiale. Il pioniere degli algoritmi quantistici Umesh Vazirani ad esempio è convinto che a differenza dell'intelligenza artificiale, che soffriva negli anni settanta di strettoie concettuali non ancora comprese e solo di recente superate, per quanto riguarda i computer quantistici ad esempio non vi è tale collo di bottiglia dal momento che si verificano due condizioni differenti: la prima è che vi sono molte tecnologie in competizione, basate su tecnologie completamente diverse tra di loro e che fanno da backup l'una dell'altra; la seconda è che non vi sono problemi concettuali nella teoria, che è pienamente compresa e che potrà solo aumentare in termini di ulteriori miglioramenti e contributi, ma questioni di carattere ingegneristico che si stanno affrontando da relativamente poco tempo e con comunità ancora piccole in continua crescita.

Detto questo, è utile esaminare più in dettaglio se sia possibile, tra le varie applicazioni, applicare la potenza dei computer quantistici anche alle scienze sociali e di riflesso quindi alle relazioni internazionali come caso d'uso di elezione.

Il presupposto è in primo luogo che vi siano modelli quantitativi, in cui le categorie quantistiche applicate per descrivere uno scenario di interesse nell'ambito delle relazioni internazionali siano impiegate mediante equazioni matematiche derivanti dalla teoria quantistica.

Lo scenario plausibile è quello di considerare i computer quantistici un promettente strumento esplorativo da affiancare agli elaboratori classici, in attesa che arrivino a piena maturazione e possano contenere problemi quantitativi grandi abbastanza da non potersi risolvere in altro modo o così velocemente.

I metodi adatti ai computer quantistici per fare community detection si basano in genere sui già studiati metodi tra cui i traditional detection methods, i dynamic-, i local- e gli overlapping detection methods. Ad esempio, sono stati condotti studi su quantum social networks (QSNs), che si sono dimostrate di essere più efficienti degli strumenti basati su reti classiche su specifici problemi[37]. Con la teoria quantistica many-body (a molti corpi) sono stati sviluppati modelli matematici basati sulla teoria della complessità validati mediante la simulazione di reti sociali, compiendo una social network analysis (SNA) che porta a conoscere la dinamica della rete sociale in esame[38]. Ancora, gli studi di evoluzione dell'entropia di una rete sociale propongono di studiare sistemi di consenso quantistici per stabilire una relazione tra la componente quantistica rispetto a quella classica che descrive la rete, fino a considerare un quantum gossiping[39]. Akbar e Saritha hanno raccolto e descritto una ventina di metodi di analisi delle reti sociali che impiegano algoritmi per i computer quantistici[40].

Vi è inoltre un'area ibrida tra l'intelligenza artificiale e il quantum computer, che consiste nella quantum artificial intelligence e nel suo ramo del quantum machine learning. Dal momento che l'intelligenza artificiale è in grado di ricostruire da dati incompleti, identificare patterns, predire serie temporali, analogamente gli algoritmi di quantum machine learning[41], possono in via di principio essere applicati anche per studi inerenti le relazioni internazionali laddove si potesse applicare il machine learning convenzionale[42].

Nella sezione che segue, si prende in esame un caso specifico di esempio di come utilizzare un computer quantistico per l'analisi di uno scenario a valenza geopolitica.

---

[37] Cabello, A., Danielsen, L. E., López-Tarrida, A. J., & Portillo, J. R. (2012). Quantum social networks. Journal of Physics A: Mathematical and Theoretical, 45(28), 285101.

[38] Bisconti, C., Corallo, A., De Maggio, M., Grippa, F., & Totaro, S. (2010). Quantum modeling of social dynamics. International Journal of Knowledge Society Research (IJKSR), 1(1), 1-11.

[39] Fu, F., Christakis, N. A., & Fowler, J. H. (2017). Dueling biological and social contagions. Scientific reports, 7(1), 1-9.

[40] Akbar, S., & Saritha, S. K. (2020). Towards quantum computing based community detection. Computer Science Review, 38, 100313.

[41] Lazzarin, M., Galli, D. E., & Prati, E. (2022). Multi-class quantum classifiers with tensor network circuits for quantum phase recognition. Physics Letters A, 128056

[42] Agliardi, G., & Prati, E. (2022). Optimal tuning of quantum generative adversarial networks for multivariate distribution loading. Quantum Reports, 4(1), 75-105.

4. UN CASO DI STUDIO: L'EVOLUZIONE DI RETI TERRORISTICHE GLOBALI

Nell'anno 2017, presso i laboratori di Los Alamos in USA i tre ricercatori Ambrosiano, Roberts e Sims pubblicarono il rapporto tecnico LA-UR-17-23946 commissionato dal Department of Energy in cui si investigava per la prima volta l'applicazione di un computer quantistico a uno studio di scienze sociali basato su un modello che descrive un equilibrio di interesse geopolitico[43]. Questo studio impiega il computer quantistico Dwave da 2000 qubits e implementa di fatto un problema che va sotto il nome tecnico di bipartizione di un grafo. Il modello alla base dell'impiego del computer quantistico si fonda sulle seguenti assunzioni: si supponga di poter descrivere un social network mediante collegamenti tra gli elementi di tale rete (detti i nodi) che corrispondano a relazioni di amicizia e di inimicizia (collegamenti positivi e negativi, rispettivamente). La questione fondamentale del bilancio strutturale di tale rete è se essa sia bilanciata o meno. Tale social network è bilanciato se la rete delle connessioni di amicizia o inimicizia consente di essere bipartita, cioè ripartita tra solo 2 fazioni, all'interno delle quali sussistano solo relazioni di amicizia, e tra le quali sussistano solo relazioni ostili. Meno le connessioni rispetteranno questa semplice regola, più tale network risulterà sbilanciato, rendendo le due fazioni maggiormente ambigue. La sociologia suggerisce che tali reti non bilanciate risultino instabili e associate a maggiore violenza[44].

Esiste un metodo analitico per valutare il grado di bilanciamento nelle reti sociali, che avviene ripartendo nel miglior modo possibile tra le fazioni i vari soggetti, a ciascuno dei quali è associato un nodo della rete, in modo tale che all'interno di ogni fazione sia minimo il numero, possibilmente zero, di relazioni ostili. Questo problema, dal punto di vista matematico e computazionale, è del massimo grado di complessità (detta NP-hard). E' qui che entra in gioco la possibilità di impiegare un computer quantistico. Infatti, questo tipo di ricerca – ovvero di assegnare i gruppi alle fazioni introducendovi allo stesso tempo il minor numero possibile di nodi legati da una relazione ostile – è matematicamente equivalente a ricercare la minima energia del circuito quantistico che descrive

[43] Ambrosiano, J. J., Roberts, R. M., & Sims, B. H. (2017). Using the D-Wave 2X quantum computer to explore the formation of global terrorist networks. Technical report LA-UR-17-23946, Los Alamos National Laboratory.

[44] Nakamura K., Tita G., Krackhardt D., "Violence in the 'Balance': A Structural Analysis of How Rivals, Allies, and Third-Parties Shape Inter-Gang Violence", Heinz College Research, Research Showcase @CMU, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1411&context=heinzworks, (2011).

l'insieme delle relazioni di amicizia e ostilità. Questo tipo di ricerca della minima energia di un circuito quantistico è svolto efficacemente da un computer quantistico adiabatico, come il D-Wave 2X basato su qubit a superconduttore.

Il problema sottoposto al computer quantistico è quindi stata la valutazione della deviazione dall'equilibrio perfetto di due scenari caratterizzati dalla forte presenza di organizzazioni militanti su due teatri in particolare, quali l'Iraq e la Siria. In concreto, sono stati esaminati i dati raccolti dalla Stanford's Mapping Militants Project negli anni che sono andati dal 2000 al 2016 per entrambi li scenari, dando luogo a reti dell'ordine della ventina di nodi, pari al numero di organizzazioni militanti che sono dell'ordine di 20-30, e associando a ciascuna coppia l'informazione se queste fossero di tipo amichevole oppure ostile.

Rispetto ai risultati osservati da questo studio, il grado di bilanciamento ha iniziato ad esempio a calare sul teatro siriano a partire da quando lo Stato Islamico è entrato in un contesto già popolato da altri gruppi. Si è anche potuto osservare quantitativamente che mentre che in un determinato periodo la rete sociale cresceva, lo sbilanciamento associato in media a ogni singolo nodo non variava significativamente, un fatto che pò essere spiegato mediante un comportamento adattivo delle varie fazioni.

C'è da precisare che per questo problema, su questa scala di attori coinvolti, non si verifica un vantaggio rispetto alla risposta che si ottiene da mezzi computazionali ordinari alla stessa domanda, e va pertanto considerato alla stregua di una dimostrazione di principio. Tuttavia, trattandosi di un problema computazionalmente hard, il tempo di calcolo aumenterà esponenzialmente al crescere del numero di nodi (di fazioni), mentre per il computer quantistico continuerà a bastare una singola valutazione, dando luogo a un tempo di calcolo estremamente vantaggioso. All'epoca di questo studio furono impiegati sostanzialmente tutti i 1150 qubit del computer quantistico DWave disponibile al momento. A distanza di cinque anni, il numero di qubit è più che quadruplicato e il numero delle connessioni di ciascun qubit con gli altri è raddoppiata, a testimonianza di come il campo si stia evolvendo rapidamente.

CONCLUSIONI:

- Le tecnologie quantistiche includono sensori, comunicazioni e computazione
- Le tecnologie quantistiche si differenziano per il grado di maturazione e sono tutte in corso di sviluppo, inclusi prototipi commercializzati
- In particolare, i computer quantistici costituiranno una leva nell'equilibrio di potere tra i vari Stati
- Il rischio di hype tecnologico per i computer quantistici è mitigato dalla varietà delle possibili tecnologie realizzative e dall'assenza di colli di bottiglia concettuali
- I computer quantistici, essendo general purpose, si applicano anche alle relazioni internazionali, a patto di avere un modello quantitativo basato sulla teoria quantistica
- Il computer quantistico Dwave è stato usato per lo studio della stabilità tra le fazioni di gruppi terroristici in Siria e Iraq

Capitolo III

Impiego dell'intelligenza artificiale nei sistemi d'arma: normativa internazionale

di Andrea Gilli e Lucrezia Scaglioli

SINTESI: L'accelerazione tecnologica degli ultimi decenni nei processori, big data e machine learning hanno portato al progresso rivoluzionario dell'intelligenza artificiale. Questi sviluppi hanno attirato una rinnovata attenzione e diffusa preoccupazione riguardante i possibili rischi derivanti dal suo utilizzo soprattutto in campo militare. Per questo, studiosi ed esperti ne hanno chiesto più volte una maggior regolamentazione, controllo e persino interdizione. Tuttavia, è opportuno chiedersi se queste paure siano giustificate e se l'intelligenza artificiale possa offrire più rischi che opportunità. In questo Capitolo cerchiamo di rispondere a tale quesito, partendo dalle origini e sviluppi dell'intelligenza artificiale, la portata e le implicazioni di questa nuova tecnologia applicata al dominio militare e ai sistemi d'arma autonoma. Successivamente, sulla base di questa analisi valutiamo le critiche, di esperti e studiosi, sui rischi legati al suo uso. Infine, analizzeremo la struttura etico-legale che ne definiscono le regole di verifica e utilizzo a livello internazionale.

1. INTELLIGENZA ARTIFICIALE: SVILUPPO E SCETTICISMO

Gli sviluppi e l'accelerazione dell'intelligenza artificiale, a partire dagli anni 2000, sono stati accompagnati da un'eguale ondata di critiche e pessimismo riguardo il suo utilizzo. In particolar modo, le maggiori preoccupazioni riguardano l'uso dell'IA applicato al dominio militare. Con l'avvento di nuovi sistemi d'arma autonomi, alcuni esperti e studiosi, infatti, sostengono che siamo di fronte a una nuova rivoluzione militare in grado di cambiarne la tecnologia, redistribuire potere militare, causare conflitti nuovi, più frequenti e più letali, e determinare stravolgimenti negli equilibri mondiali. Prima di poter verificare tali predizioni, tuttavia, è opportuno comprendere le origini, modalità di sviluppo, funzioni e prospettive future di crescita dell'intelligenza artificiale. Il pessimismo diffuso nei confronti dell'IA si basa, infatti, su tre generiche affermazioni: il continuo e crescente progresso, la predominanza del settore commerciale e quindi la maggior diffusione e infine, la grande pervasività dell'IA. Analizzando gli sviluppi, l'articolazione tecnica tecnologica e i possibili impieghi militari dell'IA sarà possibile comprendere i limiti sia tecnologici, che di questo scetticismo, la cui attenzione è focalizzata unicamente sulle conseguenze. Parte delle critiche mosse all'IA, infine, riguardano il campo dell'etica e della normativa internazionale. L'ultima parte di questo capitolo analizzerà, quindi, i principi etici che i futuri sviluppi dell'IA dovranno rispettare, oltre alla struttura legale già in vigore.

2. RIVOLUZIONE TECNOLOGICA

In questa sezione ci occuperemo dello sviluppo tecnologico che ha portato alla smisurata accelerazione dell'intelligenza artificiale, dando una definizione di che cosa è l'IA, quali funzioni può avere e infine, di che tipo di struttura tecnologica necessita per continuare questa sua espansione. Descriveremo, poi, i due tipi di approccio all'IA, dal Good Old Fashion AI (GOFAI) al Deep Learning (DL), il cui passaggio è dovuto all'esponenziale progresso nel campo dei processori, *big data e machine learning*.

Gli sviluppi e i continui progressi della tecnologia hanno portato a tre diverse rivoluzioni industriali nella storia dell'umanità, a cambiamenti sociali e politici.[45] Dall'incremento nella computazione e conseguenzialmente nei livelli di precisione, all'avvento e sviluppo di nuove tecnologie elettroniche e informatiche, dall'intelligenza artificiale (IA) al *machine learning* (ML) – ovvero la chiave computazionale dell'intelligenza artificiale – e *big data* (BD), siamo di fronte a ciò che alcuni, come Karl Schwab, definiscono la quarta rivoluzione industriale o altri, Second Machine Age.[46] Quest'era è contraddistinta da un aumento esponenziale dello sviluppo e della diffusione della tecnologia, in maniera più pervasiva e veloce rispetto alle precedenti ondate evolutive, in grado di portare a grandi trasformazioni, toccando ogni aspetto delle nostre vite, con implicazioni socio-economiche e politico-internazionali.[47] La pandemia stessa, paradossalmente, ha comportato un ulteriore accelerazione verso questa trasformazione e digitalizzazione delle nostre vite, forzando il lavoro da remoto e l'utilizzo di tecnologie digitali. Difatti, la potenza computazionale ha subito un incremento esponenziale dal 1965 ad oggi, grazie allo sviluppo di processori, algoritmi e dati.

L'intelligenza artificiale, che costituisce il cuore di questa nuova ondata rivoluzionaria tecnologica, viene definita da alcuni come *general purpose technology* (GPT), ma più in generale può essere interpretata come una tipologia di tecnologia volta a simulare l'intelligenza degli esseri umani e il cui impatto, è già possibile predire, si verificherà in plurimi campi, dall'economico al militare. L'intelligenza artificiale può essere applicata a diversi domini per diverse funzioni:

---

[45] Headrick D. R. (2010), *Power over people: technology, environments and Western imperialism, 1400 to the Present*, Princeton University Press, Princeton, NJ; Onorato M., Scheve K. and Stasavage D. (2014), "Technology and the era of mass army", *The Journal of Economic History*, Vol. 74, No. 2, pp. 49-81; Boulanin V. and Verbruggen M. (2017), *Mapping the development of autonomy in weapon systems*, SIPRI, Stockholm.

[46] Schwab K. (2016), *The fourth industrial revolution*, Crown Business, New York; Brynjolfsson E. and McAfee A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies,* New York, NY: W. W. Norton & Company.

[47] Horowitz M. C. (2018), *Artificial Intelligence, international competition and the balance of power*, Texas National Security Review, Vol. 1, No. 3, pp. 37-57.

può essere utilizzata per dirigere oggetti fisici, come robot, senza il controllo umano, oppure per processare e interpretare informazioni o infine, attraverso la sovrapposizione di più funzioni specifiche può essere usata per nuove forme di comando e controllo (C2).[48] Non vi è accordo comune tra gli studiosi su quale sia o debba essere il campo di applicazione predeterminato, tuttavia, è opinione comune che l'impatto, proprio per la sua natura pervasiva, sarà tale da portare cambiamenti, trasformazioni e rinnovata competizione sullo scenario della politica internazionale, spesso paragonato agli effetti dell'elettricità o del motore a vapore prima ancora. Così come per i processori, esistono due tipologie di intelligenza artificiale: una viene definita generale, ovvero in grado di compiere molteplici funzioni parallelamente, rappresentando la tipologia di IA che in uno scenario futuro sarebbe in grado di sostituirsi agli esseri umani; l'altro modello, invece, ha un approccio più limitato e specializzato a precisi campi di azione, definito pertanto *narrow*.[49]

Vi sono due tipi di meta-approcci all'IA: uno top-down e uno bottom-up. Il primo, definito anche come Good Old Fashion AI (GOFAI), si basa su un approccio deduttivo, per il quale tutte le informazioni devono essere codificate e inserite *ex ante*. Questo è stato l'approccio predominante fino agli anni 2010 e proprio a causa della sua struttura, che implica una codificazione in linea teorica di ogni possibile scenario, ne evidenzia i chiari limiti e carenze di apprendimento. Con l'accelerazione esponenziale di semiconduttori, chips, processori e algoritmi, le tecniche di machine learning hanno conosciuto nuovi sviluppi. Per quantificare queste trasformazioni basti pensare all'incremento nella produzione di dati, da cinque exabyte nel 2003 a 59 zettabytes – o 59 trilioni di gigabytes nel 2020; alla rapida decrescita nei costi dei sensori 3D Lidar (*Light detection and ranging*) da $30,000 nel 2009 a $80 nel 2019.[50] Sequenze di calcolo che nel 1982 avrebbero richiesto 89 anni, oggi vengono risolte in pochi secondi.[51] Questo miglioramento è stato possibile grazie anche all'aumento e specializzazione dei processori. Esistono due tipi di microprocessori, quelli specializzati, ovvero utilizzati per specifiche funzioni e sequenze, e quelli generici, in grado, invece, di essere adoperati per molteplici e parallele applicazioni.[52] I processori specializzati hanno iniziato ad essere richiesti e sviluppati in numeri crescenti, in particolar modo a partire dal 2010, visto il loro ruolo fondamentale in operazioni sequenziali nel

[48] Horowitz M. C. (2018), *Artificial Intelligence, international competition and the balance of power*, Texas National Security Review, Vol. 1, No. 3, pp. 37-57.
[49] See Russel S. and Norvig P. (2010), *Artificial intelligence: a modern approach*, Upper Saddle River, NJ, Prentice Hall, 3rd edition.
[50] Lee K. F. (2018), *AI Superpowers: China, Silicon Valley and the new world order*, Boston, MA, Houghton Mifflin.
[51] Brynjolfsson E. and McAfee A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies,* New York, NY: W. W. Norton & Company.
[52] Henessey J. L., Patterson D. A. (2019), *Computer architecture: a quantitative approach*, Morgan Kaufmann, Sixth Edition, Cambridge, MA.

funzionamento degli algoritmi di *machine learning*. Gli sviluppi negli algoritmi, a loro volta, sono la conseguenza di nuove tecniche di ML e dell'espansione nell'utilizzo e nelle funzioni dei software, tra cui la sua applicazione a sistemi di intelligenza artificiale.[53] Questo progresso, inoltre, è stato reso possibile dall'aumento nella produzione e disponibilità di dati. Con la digitalizzazione di diversi tipi di informazione, la diffusione di dispositivi portabili, quali telefoni, laptop, tablet ecc., la quantità di dati disponibile è diventata esorbitante.[54] Questi tre potenziamenti, nei microprocessori, tecniche di ML e dati disponibile, hanno determinato la rinnovata attenzione, i nuovi investimenti nel campo dell'intelligenza artificiale e il passaggio da GOFAI all'approccio induttivo, o bottom-up, basato sul deep learnig, in cui cioè si lascia che l'IA impari e si migliori grazie ai pattern, trend e capacità di predizione, ricavabili dalle enormi quantità di dati inseriti e dalle sue interazioni con il mondo.[55] Concetto che, come tale, esiste dal 1965, introdotto nella conferenza a Dartmouth College in Hanover, New Hempshire, ma che conosce un'accelerazione nel suo sviluppo e utilizzo in particolare dal 2010 in poi basandosi sullo sfruttamento del deep learning, per le ragioni precedentemente enunciate.[56]

3. IMPLICAZIONI MILITARI

Dopo aver accennato alle origini e sviluppi dell'IA è opportuno passare alla sua implementazione nel campo militare. Le conseguenze di queste trasformazioni per il dominio militare, della difesa e sicurezza sono ancora a uno stadio iniziale nello sviluppo e le implicazioni del loro utilizzo non completamente chiare. Di certo, tuttavia, queste nuove tecnologie pongono nuove opportunità, vantaggi, ma anche domande, sfide, rischi e preoccupazioni.[57] Il settore della difesa e sicurezza ha iniziato, ormai da vari anni, il processo di integrazione dell'IA alla sua struttura di forza, tuttavia, il dibattito spesso si concentra unicamente sulle conseguenze, destando preoccupazioni e critiche. Si parla, infatti, di corsa agli armamenti, dei rischi dovuti alla maggior diffusione e pervasività dei sistemi d'arma autonomi e persino di stravolgimento degli equilibri di potenza. In questo paragrafo

[53] Allen G. (2020), *Understanding AI technology*, US Department of Defense, Joint Artificial Intelligence Center, Washington, DC.
[54] Manyika J. Et al. (2011), *Big data: the next frontier for innovation, competition and productivity*, McKinsey Global Institute, New York.
[55] Gilli A. e Gilli M. (2021), "Tecnologia e nuovi conflitti globali", *Aspenia*, Vol. 94, pp. 117-127.
[56] Haenlein H. and Kaplan A. (2019), "A brief history of artificial intelligence: on the past, present and future of artificial intelligence", *California Management Review*, Vol.61, No.4.
[57] Horowitz M. C. (2018), *Artificial Intelligence, international competition and the balance of power*, Texas National Security Review, Vol. 1, No. 3, pp. 37-57.

toccheremo questi punti e analizzeremo se queste paure e preoccupazioni siano o meno giustificate.[58]

L'espressione usata da giornalisti, politici e ricercatori di "corsa agli armamenti di intelligenza artificiale", oltre ad incrementare un dibattito di competizione strategica, non coincide con la realtà fattuale. Le grandi potenze sono, effettivamente, in competizione per la ricerca e lo sviluppo di tecnologie militari e commerciali collegate all'intelligenza artificiale, ma ciò non corrisponde alla tradizionale definizione di "corsa agli armamenti".[59] Nonostante il fenomeno non corrisponda esattamente alla definizione di corsa agli armamenti, l'accelerazione negli sviluppi e potenziali utilizzi dell'intelligenza artificiale al campo militare vengono enfatizzati da leader politici, CEOs e accademici, come una vera e propria rivoluzione militare. Ne sono un esempio l'obiettivo del governo cinese del 2017 di raggiungere l'egemonia mondiale nel campo dell'intelligenza artificiale, l'introduzione di strategie militari per l'IA da parte delle più importanti potenze europee e dalla NATO, il programma del Pentagono Project Maven o le dichiarazioni di Putin, per il quale controllare l'intelligenza artificiale comporta il dominio mondiale.[60]

L'intelligenza artificiale, ricordiamo, ha lo scopo di imitare il comportamento e ragionamento umano attraverso una catena di informazione che va dalla percezione, alla cognizione e infine all'azione. Questo funzionamento significa che i sistemi autonomi dell'IA stabiliscono la propria azione sulla base di ragionamenti e calcoli probabilistici determinati dagli input dei sensori, che devono percepire il mondo circonstante e destrutturarlo, ma pur sempre senza connessioni logiche.[61] Ciò che per un computer richiede enormi quantità di dati da processare e una sorta di training, viene effettuato in pochi secondi dal cervello umano, dimostrando il paradosso di questa cosiddetta quarta rivoluzione industriale: più le tecnologie sono articolate, sviluppate e complicate, e più c'è e ci sarà bisogno degli esseri umani a controllarle, dirigerle e interpretarle.[62]

Le implicazioni militari dell'IA sono molteplici e presentano vari vantaggi per il dominio della difesa e sicurezza. In primo luogo, l'IA permette un'estrapolazione, raccolta, trasmissione e analisi di dati maggiori, grazie ai miglioramenti dei radar e sensori, incrementando le azioni di *intelligence, surveillance and reconnaissance.* In secondo luogo, consente di ottimizzare problemi combinatori e quindi di migliorare la logistica con l'utilizzo di *unmanned autonomous vehicles* di terra, aria o mare. In terzo luogo, aumenta la precisione nel targeting del nemico, attraverso

---

[58] Frey B. C. (2019), *The technology trap: capital, labor, and power in the age of automation*, Princeton, Princeton University Press.
[59] Scharre P. (2021), *Debunking the AI arms race theory*, Texas National Security Review, Vol. 4, Issue 3.
[60] Gilli A. e Gilli M. (2021), "Tecnologia e nuovi conflitti globali", *Aspenia*, Vol. 94, pp. 117-127.
[61] Cummings M. L. (2017), *Artificial Intelligence and the Future Warfare*, Chatham House.
[62] Ibid.; Gilli A. (2020), *"NATO-Mation": Strategies for leading in the age of Artificial Intelligence,* NDC Research Paper N. 15, Rome, NATO Defense College.

precision-guided weapons, la cui implicazione può essere vista come una riduzione dei danni collaterali nei confronti di civili. Inoltre, accelera il tempo di guerra, aumentando conseguentemente quelle che sono le azioni di analisi predittive e decision making, che l'IA può realizzare più rapidamente di un cervello umano.[63] Vi sono ulteriori aspetti da tenere in considerazione:

- L'utilizzo dell'IA alla sfera militare riduce ulteriormente il rapporto tra *labour e capital*, tendenza iniziata a partire dalla rivoluzione industriale secolare.
- Mentre nella prima rivoluzione industriale i macchinari sostituivano l'energia prodotta dai muscoli degli uomini, animali o naturale, in questa rivoluzione industriale le macchine cercano di sostituire le capacità cognitive degli individui. In questa fase però, algoritmi e robotica sono ancora prevalentemente utilizzati per missioni 4D *(dangerous, dull, dirty, dumb)* e i limiti di deep learning non possono permettere ancora usi che sostituiscano appieno gli esseri.
- Sfruttando l'IA si può avere una superiore velocità e precisione grazie agli algoritmi che permettono di velocizzare i tempi di attacco e discriminare con maggior precisione i target nemici. Raggiungendo velocità superiori alle capacità umane.
- L'utilizzo dell'IA al campo militare introduce però anche un problema di comando e controllo, relativo a *human machine interaction* (HMI) o *human machine teaming* (HMT). L'IA genera una questione di fiducia e affidabilità tra il *commander* (militare) e i robot o i sistemi automatizzati. C'è anche una questione relativa a come addestrare e istruire gli esseri umani a lavorare meglio con questi sistemi, come ad esempio disegnare le interfacce, capire la psicologia umana nell'interagire con sistemi autonomi e automatizzati, o rivedere la formazione.
- Infine, bisogna considerare la base industriale. Se in passato la base industriale era fondamentale per vincere le guerre, nell'era post-industriale, caratterizzata da software e *big data*, sarà necessario adeguare la base industriale a quest'era, per garantire la sicurezza futura.

Nonostante gli incredibili sviluppi nel campo dei sistemi autonomi, d'aria, terra o mare, il passaggio all'implementazione effettiva in operazioni militari è ancora lontano, in parte come conseguenza dei necessari adattamenti organizzativi e strutturali, agli enormi costi, in parte dovuto alla priorità attribuita allo sviluppo di veicoli e sistemi d'arma tradizionali ed infine, secondo alcuni, perché in questa fase il settore trainante negli sviluppi e utilizzi degli UVs, quali i droni o auto senza conducenti, è proprio quello commerciale e privato.[64]

Gli sviluppi e l'integrazione degli *autonomous weapon systems* ha sollevato amplio dibattito e preoccupazioni crescenti riguardo l'inizio dell'era robotica e la

[63] Ibid.
[64] Cummings M. L. (2017), *Artificial Intelligence and the Future Warfare*, Chatham House.

diminuzione del controllo umano in campo militare. Le preoccupazioni più comuni, di studiosi ed esperti, vanno dal rischio di maggiore instabilità e conflitti, allo stravolgimento dell'ordine e dell'equilibrio internazionale. Le critiche generalmente sollevate poggiano su tre assunti principale: una maggior diffusione di sistemi autonomi negli anni a venire, una più amplia pervasività di questi sistemi e un continuo progresso dell'IA. In questo paragrafo, muovendo dalle critiche, analizziamo i rischi che l'IA potrebbe o meno comportare.

La prima preoccupazione riguardo gli sviluppi dell'IA, guidati principalmente dal settore commerciale, è la sua più rapida e pervasiva diffusione per due motivi: la diminuzione del prezzo unitario di produzione e la più facile diffusione di questi da parte di privati incentivati dal profitto ed economie di scala. Una maggiore propagazione limiterebbe da un lato i vantaggi strategici militari e dall'altro aumenterebbe ed espanderebbe la pervasività di queste tecnologie. Il rischio interconnesso a questa possibilità implicherebbe che più attori possano avere facile accesso sia a sistemi d'IA commerciali che a sistemi d'arma letali, con conseguente aumento dei conflitti e dell'instabilità politica internazionale.[65] Questo tipo di critica, tuttavia, si basa sul presupposto che l'IA sia una tecnologia più economica e facile da realizzare, replicare e diffondere, rispetto ai sistemi d'arma tradizionali. Infatti, se da un lato va riconosciuto che la tecnologia commerciale è relativamente più economica, dall'altro è necessario specificare che una volta spostatasi all'ambito militare quella tecnologia necessita di requisiti sempre più specifici e costosi per un minor numero di unità, che ne impedisce lo sfruttamento di economie di scala.[66]

Un secondo tipo di critica riguarda, invece, la pervasività e accelerazione nell'utilizzo dell'IA. Questa diffusione maggiore potrebbe comportare cambiamenti al carattere della guerra: rendendola potenzialmente più rapida, più instabile e letale. Ulteriore motivo per cui i sistemi d'arma automatizzati letali, o LAWs, creano apprensione e avversità sia nell'opinione pubblica che fra i militari stessi.[67] Più facili da produrre, da imitare e meno costosi, secondo alcuni studiosi, i droni, ad esempio, potrebbero cambiare le dinamiche della politica internazionale redistribuendo potere militare, con conseguente aumento dell'instabilità e frequenza di nuovi, più veloci e più letali conflitti. Effettivamente, l'aumento nell'utilizzo di robot incorporanti intelligenza artificiale, o armi autonome – *unmanned autonomous vehicles* (UAVs) – se da un lato vengono acclamati come il primo stadio verso una nuova era tecnologica-robotica, dall'altro incrementano la preoccupazione e il dibattito degli ultimi 15 anni sulla possibilità di mettere al bando quelli che vengono definiti come *"killer robots"* che comporterebbero crisi, violenza e violazione dei diritti umani, ad esempio a causa di un malfunzionamento

[65] Horowitz M. C. (2018), *Artificial Intelligence, international competition and the balance of power*, Texas National Security Review, Vol. 1, No. 3, pp. 37-57.
[66] Gilli A. e Gilli M., Artificial Intelligence and International Security, *working paper*.
[67] Ibid.

o imprecisione dell'algoritmo.[68] Tuttavia, anche questa critica può essere vista come esagerata, infatti non si sono verificati né casi di guerre condotte unicamente da *killer robots*, e il numero di perdite inflitte da droni nei recenti conflitti, ad esempio in Siria o Nagorno-Karabakh, sono notevolmente inferiori rispetto alle vittime causate da scontri tradizionali.

Queste paure e apprensioni, più in generale, esasperano la realtà fattuale dello sviluppo degli UAVs e dell'intelligenza artificiale in sé. In effetti, entrambi i due meta-approcci utilizzati nell'intelligenza artificiale per le armi autonome presentano dei limiti. L'approccio deduttivo, o top-down da un lato, fondandosi su una programmazione *ex ante*, che deve includere ogni tipo di evenienza o imprevisto, è chiaramente irraggiungibile con l'attuale tecnologia, in particolar modo se il *killer robot* deve agire in un ambiente in continua evoluzione.

L'approccio induttivo, invece, o bottom-up, si basa sulla raccolta di enormi quantità di dati per estrapolarne tendenze e modelli che il software dovrà imparare attraverso sistemi di *machine learning*. Le problematiche in questo caso sono molteplici: avere accesso a queste enormi quantità di dati, gli elevati costi di training da sostenere ed infine l'esposizione a maggiori vulnerabilità, quali gli attacchi cyber, comportando un'alta esposizione a rischi operativi e la conseguente cautela prima di un loro utilizzo appieno sul campo di battaglia.[69] Questo secondo approccio ha, inoltre, limiti di hardware: l'attuale *computer architecture* non è in grado di gestire le enormi quantità di dati prodotti e non ha sufficiente potere computazionale per processarli, vista la recente esplosione del *deep learning*, come nuova base di sviluppo dell'IA.[70]

Alla luce dei limiti tecnologici e strutturali legati all'impiego dell'IA, risulta evidente l'eccessivo pessimismo e apprensione nei confronti di una tecnologia ancora in fase di sviluppo e lontana dallo stravolgimento del campo militare.

4. QUESTIONI ETICO-NORMATIVE

L'accelerazione nella digitalizzazione, nell'era robotica e nei sistemi autonomi, in cui la tecnologia e i robot sembrano sostituirsi agli uomini, ed essere in grado di agire o fare predizioni da soli, fanno sì che il dominio dell'etica e il ruolo delle normative internazionali acquisiscano rinnovato valore e importanza. Solitamente vi sono due tipi di approcci nei confronti dell'innovazione tecnologica: prima innovare e poi gestire le conseguenze, oppure cercare di prevenire i rischi

[68] Gilli A. e Gilli M. (2021), "Tecnologia e nuovi conflitti globali", *Aspenia*, Vol. 94, pp. 117-127.
[69] Gilli A. e Gilli M. (2021), "Tecnologia e nuovi conflitti globali", *Aspenia*, Vol. 94, pp. 117-127.
[70] Gilli A. e Gilli M., Artificial Intelligence and International Security, *working paper*.

dell'innovazione *ex ante*. In numerosi casi si è utilizzato il primo tipo di approccio, tuttavia, per quanto riguarda l'IA il secondo sembra trovare maggior consenso visti i dibattiti sui principi etici.[71] In quest'ultimo paragrafo, ci focalizziamo su queste sfide etiche e normative in vigore o tentativi di regolamentazione.

La crescente attenzione nei confronti dell'etica richiederebbe a tali nuove tecnologie, sia di uso commerciale che militare, di comportarsi seguendo le norme, i valori e i giudizi che gli esseri umani adotterebbero, seguendo quello che potremmo definire come il nostro codice morale. Tuttavia, il loro comportamento e le loro azioni dipendono dai codici inseriti in fase di programmazione, dagli algoritmi e dai dati in loro possesso. Nonostante i crescenti contributi etici e normativi da parte di alcuni gruppi, il dominio dell'etica per l'IA manca di parametri precisi che determinino la relazione tra sviluppo tecnologico e le più ampie discussioni sociali.[72] Conseguentemente, accademici, studiosi, ONG, chiedono che la realizzazione di UAV venga effettuata seguendo alcuni principi e linee guida, che possiamo racchiudere in sei presupposti.[73]

Primo fra questi è che l'IA abbia al centro, della sua attenzione e programmazione, gli esseri umani e i diritti dell'uomo, in modo tale che il suo utilizzo sia volto a migliorare, e non ledere, le condizioni di vita di questi. In secondo luogo, affinché si possa sviluppare un senso di fiducia nei confronti dell'utilizzo dell'IA, è necessario che le loro azioni siano spiegabili, comprensibili e trasparenti, *ex ante* ed *ex post*, che si tratti di armi autonome letali o di auto senza conducente. Una terza posizione è, invece, la problematicità nell'attribuzione della responsabilità e *accountability*. Questa criticità si presenta soprattutto in caso di errori, malfunzionamenti o attacchi cibernetici, che complicano maggiormente lo scenario, aumentando la difficoltà nell'individuare i responsabili. L'attribuzione di responsabilità in caso di equivoci, si collega agli aggiuntivi principi di affidabilità e sicurezza, da garantire prima dell'utilizzo di nuove tecnologie, a maggior ragione nei casi di sistemi autonomi. Questi principi, da seguire nella fase di programmazione, costruzione, test, valutazione e validazione, prima di implementarli, permetterebbero di ridurre il margine di rischio diretto alla vita degli esseri umani, ma anche di rallentare la diffusione o messa in commercio di tali tecnologie. La quinta posizione di questo dibattito prevede e richiede l'integrazione di principi di uguaglianza e inclusione.

Come in ogni competizione, infatti, a seconda delle capacità di singoli paesi, esistono aziende o individui con minor digitalizzazione, accessibilità a dati o nuove tecnologie. Il rischio che si intercorre è di cambiare l'ordine gerarchico o di

---

[71] Luca de Biase (2021), "Where ethics meet algorithms", *Aspenia*, Vol. 94, pp. 128-135.

[72] Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault, *The AI Index 2021 Annual Report*, AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March 2021.

[73] Gilli A. (2020), *"NATO-Mation": Strategies for leading in the age of Artificial Intelligence,* NDC Research Paper N. 15, Rome, NATO Defense College, pp. 29-34.

incrementare le differenziazioni e la marginalizzazione di alcuni gruppi di individui, o paesi, a discapito di altri. Infine, l'ultima posizione riguarda le tematiche di privacy e *data governance*. Questi principi sono tra i più controversi e dibattuti perché in contrapposizione con quelli di sicurezza e validazione, poiché questi ultimi richiederebbero la raccolta di enormi quantità di dati, mentre le regole di privacy ne esigono una riduzione e regolamentazione più rigida.[74]

Alcune regole generiche, tuttavia, per definire i requisiti legali che un sistema d'armi deve rispettare e raggiungere prima della sua implementazione esistono già. Il framework più generico per la revisione di nuove armi, prima della loro entrata in uso, è l'articolo 36 del Protocollo Aggiuntivo (I) alla Convenzione di Ginevra 1977, in base al quale *"Nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato, in talune circostanze o in qualunque circostanza, dalle disposizioni del presente Protocollo (I) o da qualsiasi altra regola del diritto internazionale applicabile a detta Alta Parte contraente".*[75]

Le due regole sostanziali che devono far parte dell'articolo 36 e della revisione di nuove armi sono la regola contro le armi non discriminatorie, ovvero la messa al bando di tutte le nuove armi non in grado di distinguere i propri target, differenziando civili da militari seguendo il principio della distinzione, in base all'articolo 54 (3b) del Protocollo (I), e l'articolo 35 (2) del Protocollo (I) che proibisce qualsiasi tipo d'arma la cui natura possa infliggere violenza o danni innecessari e superflui, seguendo il principio legale della proporzionalità.[76] Stando alle posizioni dei più scettici, però, questa struttura legale internazionale non è sufficientemente regolativa per i sistemi d'arma autonomi.

Al centro del dibattitto normativo e legale riguardo i sistemi autonomi, l'attenzione principale oltre ad essere rivolta a una regolamentazione più generale dell'IA, trova le posizioni più scettiche e pessimiste nei confronti dei sistemi d'arma autonomi letali, o LAW. Vi sono generalmente quattro principali critiche che si ripetono e vengono utilizzate contro LAW per richiederne la messa al bando. La prima sostiene che i sistemi di programmazione non raggiungeranno mai i livelli etici, morali e legali richiesti per il loro utilizzo nei campi di battaglia. Assunzione *a priori* basata su livelli di sviluppo che non verranno mai raggiunti, a detta dei sostenitori di questa posizione, escludendo quindi la possibilità di progresso e

---

[74] Gilli A., Pellegrino M. e Kelly R. (2019), "Intelligent Machines and the Growing importance of Ethics", in Gilli A. et al., *The Brain and the Processor: unpacking the challenges of human-machines interactions*, NDC Research Paper, Roma: NATO Defense College; Luca de Biase (2021), "Where ethics meet algorithms", *Aspenia*, Vol. 94, pp. 128-135.

[75] United Nations (1977), *Protocol Additional to the Geneva Conventions of the 12 August 1949, and relating to the protection of victims of international Armed Conflict (Protocol I),* of 8 June 1977, UN.

[76] Anderson K. e Waxman M. (2013), *Law and ethics for autonomous weapon systems, Why a ban won't work and how the laws of war can*, Task Force on National Security and Law.

perfezionamento che l'IA potrebbe sviluppare nel lungo periodo. La seconda posizione, invece, è contraria alla possibilità di escludere parzialmente o del tutto la presenza del controllo umano, ovvero di agenti morali, in scenari di guerra e non solo. Questa critica è più ampia e richiederebbe una decisione collettiva, nazionale e internazionale sul livello di sviluppo di sistemi autonomi desiderabile da raggiungere: Difatti, le auto senza conducente, per fare un esempio, sono già entrate nello spazio commerciale e vengono generalmente accettate. La terza argomentazione si ricollega a uno dei principi etici che queste nuove tecnologie dovrebbero seguire, ovvero il problema dell'attribuzione di responsabilità. In caso di errori, malfunzionamenti, targeting di civili e quindi crimini di guerra, determinare la persona materialmente e legalmente responsabile di tali azioni diventerebbe ancora più complicato se non impossibile. Questo problema potrà forse un giorno essere risolto migliorando la programmazione, il *deep learning* o i dati a disposizione, ma un'attenzione eccessiva volta a limitare l'IA rischia di rallentarne anche quegli sviluppi con potenziali risultati positivi. Infine, l'ultima obiezione sostiene che l'accelerazione nello sviluppo dei sistemi d'arma autonomi comporterà sul lungo termine un aumento dei conflitti e confronti armati, poiché la maggior precisione nei sistemi d'arma e la possibilità di ridurre la presenza fisica di soldati, e quindi di danni collaterali a questi e ai civili, diminuirebbe il disincentivo alle guerre.[77]

Questi esempi etico-normativi presentano uno scenario ancora in fase di definizione e per questo incompleto. Le principali potenze europee e atlantiche hanno interesse a rendere lo sviluppo e l'impiego di queste nuove tecnologie legalmente regolato. Se da un lato troviamo i più scettici e pessimisti che richiedono la messa al bando dei *killer robots*, dall'altro potrebbe invece esserci spazio per un'azione multilaterale più regolamentare che limitativa, nonostante raggiungere un accordo, specialmente per nuove tecnologie di uso sia commerciale che militari, preveda varie difficoltà.

Le argomentazioni a favore della messa a bando dell'IA si concentrano maggiormente sulle conseguenze che questa potrebbe avere, in particolare applicata al dominio militare, tuttavia, lo stadio di sviluppo di questa tecnologia, ancora prematuro, non giustifica questo pessimismo diffuso ed eccessive limitazioni rischiano di ledere futuri progressi.

[77] Anderson K. e Waxman M. (2013), *Law and ethics for autonomous weapon systems, Why a ban won't work and how the laws of war can*, Task Force on National Security and Law.

Conclusioni:

- I tre presupposti su cui poggiano la maggior parte delle critiche volte all'impiego dell'intelligenza artificiale in campo militare, presentano chiari limiti.
- Lo stadio reale di sviluppo dell'intelligenza artificiale non giustifica il pessimismo diffuso che predomina il dibattito riguardo questa tecnologia.
- La struttura etico-legale per l'impiego dell'IA nel dominio militare ha margine di miglioramento multilaterale

Capitolo IV

New warfare: potenziali rischi e mitigazioni

di Enrico Savio ed Enrico Comin

Sintesi: Lo sviluppo e l'applicazione delle tecnologie disruptive stanno già ridefinendo gli scenari di Difesa e Sicurezza. Scenari in cui - in un futuro prossimo - velocità, efficienza e precisione delle operazioni militari arriveranno a livelli mai raggiunti prima, e dove le capacità - sempre più sofisticate - della macchina potrebbero superare l'elemento umano, il suo controllo, la sua responsabilità (man-out-the-loop). Si tratta di un radicale cambiamento dei paradigmi tattici e strategici, con profonde implicazioni etiche e morali. Il presente capitolo intende innanzitutto illustrare e analizzare lo stato dell'arte di tali tecnologie e il loro potenziale impatto nel futuro warfare. Al contempo, mira a mettere in luce i rischi, le principali sfide e le possibili strategie per gestire le evoluzioni già in atto, nella piena consapevolezza che la tecnologia vada orientata e sviluppata, nel quadro di norme, valori e principi etici e morali condivisi.

1. LE TECNOLOGIE *DISRUPTIVE* NELLA DIFESA

Lo sviluppo tecnologico è da sempre motore di profondi mutamenti nelle caratteristiche dei conflitti armati e degli equilibri geopolitici. Gli ultimi anni, in particolare, sono stati testimoni di cambiamenti sostanziali nell'ecosistema tecnologico globale, a causa di un sempre più rapido progresso e di un crescente tasso di diffusione. L'innovazione oggi, rispetto al passato, è infatti sempre più guidata dal settore commerciale e sta contaminando - in maniera sempre più pervasiva - il settore della difesa dando vita a nuove sfide di sicurezza mai concepite prima.

Come sottolineato dalla *National Defence Strategy* Statunitense del 2018, lo scenario di sicurezza del futuro sarà profondamente influenzato sia dai rapidi progressi tecnologici che dal carattere mutevole della guerra. Le nuove tecnologie, che includono l'informatica avanzata, l'analisi dei *"big data",* l'intelligenza artificiale, i sistemi autonomi, la robotica, l'energia diretta, l'ipersonico e la biotecnologia saranno i frangenti su cui si combatteranno e vinceranno le guerre del futuro.[78] In un report per il *Center for a New American Security,* Ben FitzGerald e Shawn Brimley hanno definito le *Disruptive Technologies* nel settore della difesa come "una tecnologia o un insieme di tecnologie applicate a un problema rilevante in un modo che altera radicalmente la simmetria del potere militare tra i concorrenti" e che "valica immediatamente le politiche, le dottrine e l'organizzazione di tutti gli attori coinvolti".[79]

[78] United States Department of Defense (2018), *"Summary of the National Defense Strategy"*.
[79] FitzGerald, B. Et al. (2013), *"Game Changers: Disruptive Technology and U.S. Defense Strategy"*, Center for a New American Security.

Il concetto di tecnologia dirompente, tuttavia, non è frutto dei nostri tempi ma è sempre stato valido nel corso della storia. Infatti, come rilevato dallo storico francese Jacques Le Goff, sotto il profilo propriamente militare, è da scartare la tesi d'una cavalleria nata "naturalmente" nel corso dell'VIII secolo dal bisogno di contrastare le rapide incursioni degli Arabi di Spagna. È l'invenzione di un oggetto, la staffa, che consentendo una maggiore stabilità in sella - e quindi un più efficiente attacco - rivoluzionò sostanzialmente il ruolo del cavaliere sia sul campo di battaglia che nella società.[80]

Tornando ai nostri tempi, la permeazione di queste tecnologie dirompenti nel panorama globale della difesa sta generando numerosi e sostanziali quesiti riguardo la gestione dei futuri conflitti e più in generale degli equilibri di potere fra Stati. In tale contesto, l'obiettivo dei seguenti paragrafi è di elencare le principali tecnologie considerate *disruptive* nel settore della difesa con le relative definizioni, provvedendo a un'analisi delle loro caratteristiche principali.

2. INTELLIGENZA ARTIFICIALE

Nonostante non esista una definizione univoca e condivisa di intelligenza artificiale, generalmente il termine IA viene utilizzato per riferirsi a un sistema informatico con capacità cognitive al livello umano. L'IA è divisa in due categorie: IA ristretta e IA generale. I sistemi rientranti nella prima categoria possono eseguire solo il compito specifico per il quale sono stati addestrati; mentre i secondi, tramite apprendimento autonomo, potrebbero un giorno essere in grado di eseguire una vasta gamma di compiti, compresi quelli per i quali non sono stati specificamente addestrati.

L'IA ristretta è attualmente integrata in numerose applicazioni militari, che includono ma non sono limitate - a intelligence, sorveglianza e ricognizione, logistica, operazioni informatiche, comando e controllo e sistemi semi-autonomi e autonomi. Queste tecnologie sono destinate in parte a supportare o sostituire gli operatori umani, i quali saranno maggiormente chiamati a svolgere un lavoro più complesso e cognitivamente impegnativo. I sistemi abilitati dall'IA potrebbero reagire molto più velocemente di quelli che si basano sull'input dell'operatore, far fronte a un aumento esponenziale della quantità di dati disponibili per l'analisi, e

[80] Le Goff, J. (1997), *"L'Uomo Medievale"*, Editori Laterza.

abilitare nuovi concetti operativi, come lo *swarming*[81], che potrebbe conferire un vantaggio tattico sopraffacendo gli apparati difensivi avversari. In questo contesto, è significativo il risultato evidenziato nel programma di ricerca del DARPA *"AlphaDogfight",* incentrato sulle capacità di combattimento aereo tramite IA, dove - in una serie di duelli aerei simulati fra un velivolo pilotato tramite intelligenza artificiale e l'altro da un pilota umano - ha prevalso, con risultati stupefacenti, il velivolo controllato tramite intelligenza artificiale.[82]

L'IA, tuttavia, potrebbe introdurre una serie di sfide trasversali come, ad esempio, la vulnerabilità a distorsioni cognitive e bias derivanti dai set di dati su cui gli algoritmi vengono addestrati.[83] Infatti, diversi ricercatori hanno ripetutamente individuato casi di pregiudizi razziali nei programmi di riconoscimento facciale tramite IA, principalmente dovuti alla mancanza di diversità nelle immagini su cui i sistemi sono stati allenati, mentre alcuni programmi di elaborazione del linguaggio hanno sviluppato pregiudizi di genere.[84] Questo tipo di vulnerabilità potrebbe avere implicazioni significative per le applicazioni dell'IA in un contesto militare. Ad esempio, incorporare inconsciamente pregiudizi non rilevati in fase di test potrebbe condurre a casi di identificazione errata dei bersagli. Nei sistemi militari, tali algoritmi potrebbero produrre, allo stato attuale, risultati imprevedibili e non convenzionali in grado di generare fallimenti inaspettati. Inoltre, queste vulnerabilità potrebbero essere sfruttate intenzionalmente da attori malevoli o avversari per interrompere l'identificazione, la selezione e l'ingaggio di obiettivi tramite o col supporto dell'IA. Ciò potrebbe, a sua volta, sollevare preoccupazioni etiche, o potenzialmente, portare a violazioni delle leggi sui conflitti armati, se il sistema selezionasse e ingaggiasse un obiettivo o una classe di obiettivi che non sia stata approvata da un operatore umano.

Recenti notizie e analisi hanno ulteriormente evidenziato il ruolo dell'IA nel consentire falsificazioni e manipolazioni digitali di foto, audio e video con risultati sempre più realistici: tali prodotti fittizi sono noti come *deep fakes*.[85] Queste

---

[81] Per *swarming* si intende il comportamento cooperativo in cui i sistemi senza equipaggio comunicano, collaborano e si coordinano autonomamente prendendo decisioni collettive per raggiungere un compito specifico.

[82] Hitchens, T. (2020), *"AI Slays Top F-16 Pilot In DARPA Dogfight Simulation"*, Breaking Defense, https://breakingdefense.com/2020/08/ai-slays-top-f-16-pilot-in-darpa-dogfight-simulation/.

[83] I dati di addestramento sono dati utilizzati per insegnare ai modelli AI o agli algoritmi di apprendimento automatico a prendere decisioni corrette. Possono essere integrati da serie successive di dati chiamati set di validazione e di test.

[84] Congressional Research Service (2020), *"Emerging Military Technologies: Background and Issues for Congress".*

[85] *Deep fake* è un tipo di intelligenza artificiale utilizzata per creare immagini, audio e video convincenti e spesso non distinguibili. Il termine, che descrive sia la tecnologia che il contenuto falsificato risultante, è un portmanteau delle parole *deep learning* e *fake*.

capacità di IA potrebbero essere impiegate come parte di operazioni mirate a minare le capacità informative. Infatti, la tecnologia *deep fake* potrebbe essere usata per generare notizie false, influenzare l'opinione pubblica, erodere la fiducia dei cittadini e tentare il ricatto di funzionari governativi. Per questo motivo, alcuni analisti sostengono che le piattaforme di social media, oltre a impiegare strumenti di rilevamento dei *deep fakes*, dovrebbero rafforzare le soluzioni di classificazione e autenticazione dei contenuti.[86]

A complicare ulteriormente i problemi di prevedibilità e sicurezza, le tipologie di algoritmi di IA che hanno le prestazioni più elevate non sono attualmente in grado di spiegare i loro processi. Per esempio, Google ha creato un sistema di identificazione dei gatti che ha raggiunto risultati impressionanti nell'identificazione dei felini su YouTube. Tuttavia, nessuno degli sviluppatori del sistema è stato in grado di determinare quali tratti di un gatto lo strumento abbia utilizzato nel suo processo di identificazione.[87] Questa mancanza della cosiddetta "esplicabilità", che è comune alla maggior parte degli algoritmi di IA, ha portato la Defense Advanced Research Projects Agency (DARPA) a condurre investimenti in ricerca con durata quinquennale per produrre strumenti di IA "esplicabili" *(explainable AI).* Un'insufficiente esplicabilità può creare ulteriori problemi in un contesto militare, poiché l'opacità nel funzionamento dell'algoritmo potrebbe indurre gli operatori ad avere una eccessiva o scarsa fiducia nel sistema. Oltre a ciò, essa può mettere in discussione diversi altri passaggi dell''interazione uomo-macchina, tra i quali:

- **allineamento degli obiettivi** → l'uomo e la macchina devono avere una comprensione comune dell'obiettivo, il quale, in un ambiente dinamico, tende a cambiare, rendendo necessario un simultaneo adattamento sia da parte dell'uomo che della macchina, sulla base di un quadro condiviso dell'ambiente in cui si opera;
- **allineamento dei compiti** →l'uomo e la macchina devono capire i confini dello spazio decisionale dell'altro, specialmente quando gli obiettivi cambiano. In questo processo, gli esseri umani devono essere perfettamente consapevoli dei limiti del progetto della macchina per evitare di riporre una fiducia inappropriata nel sistema;
- **interfaccia uomo-macchina**→ a causa del requisito di decisioni tempestive in molte applicazioni militari dell'IA, le interfacce tradizionali possono rallentare le prestazioni. È quindi necessario considerare delle soluzioni per garantire un coordinamento in tempo reale fra uomo e macchina.

---

[86] Ivi; Roth, Y., Achuthan, A. (2020), *"Building rules in public: Our approach to synthetic & manipulated media",* Twitter, https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

[87] Congressional Research Service (2020), *"Emerging Military Technologies: Background and Issues for Congress".*

Infine, l'esplicabilità potrebbe sfidare la capacità di verificare e convalidare le prestazioni dei sistemi di IA prima dell'utilizzo operativo. Infatti, l'attuale mancanza di un output spiegabile non permette di generare una traccia di controllo per i test mirati alla verifica degli standard di prestazione. Aumentare la capacità di spiegare i processi cognitivi sarà quindi una delle attività chiave per elevare a livelli appropriati la fiducia in tali sistemi. In tutti i casi, la sicurezza dell'Intelligenza Artificiale da un punto di vista cyber (nel suo design, addestramento e operazioni) è di primaria importanza per garantire che essa si comporti in accordo a come è stata disegnata ed addestrata. Questa priorità è, tra l'altro, un evidente supporto alla necessità di disporre di sovranità tecnologica in tale campo e, di conseguenza, di devolvere ad esso attenzione e fondi adeguati.

3. LE TECNOLOGIE QUANTISTICHE

L'aumento quasi inimmaginabile del tasso e dell'ordine di calcolo abilitati dalle tecnologie quantistiche (vedasi il Capitolo II) fornirebbe profondi vantaggi in aree strategicamente vitali, fra cui crittografia e decrittografia, radaristica e sensoristica, navigazione e puntamento, simulazione e *data-mining*, apprendimento automatico e riconoscimento di modelli.

In generale, tali tecnologie non hanno ancora raggiunto la necessaria maturità per il loro reale impiego in ambito militare, ma potrebbero avere implicazioni significative per il futuro delle comunicazioni, della crittografia e delle tecnologie *stealth.*[88]

In particolare, le cosiddette comunicazioni quantistiche potrebbero consentire lo sviluppo di trasmissioni sicure non intercettabili o decifrabili. La tecnologia quantistica sarebbe in grado di offrire numerose altre applicazioni nella difesa, come i sistemi radar quantistici che - si ipotizza - saranno in grado di identificare le caratteristiche prestazionali (e.g. la sezione trasversale e la velocità) degli oggetti con un livello di precisione maggiore rispetto ai sistemi radar convenzionali.[89] Se concretizzati, questi sistemi faciliterebbero significativamente il tracciamento e il puntamento dei velivoli a bassa osservabilità, o *stealth*. Analogamente, i progressi nel rilevamento quantistico riuscirebbero teoricamente consentire miglioramenti

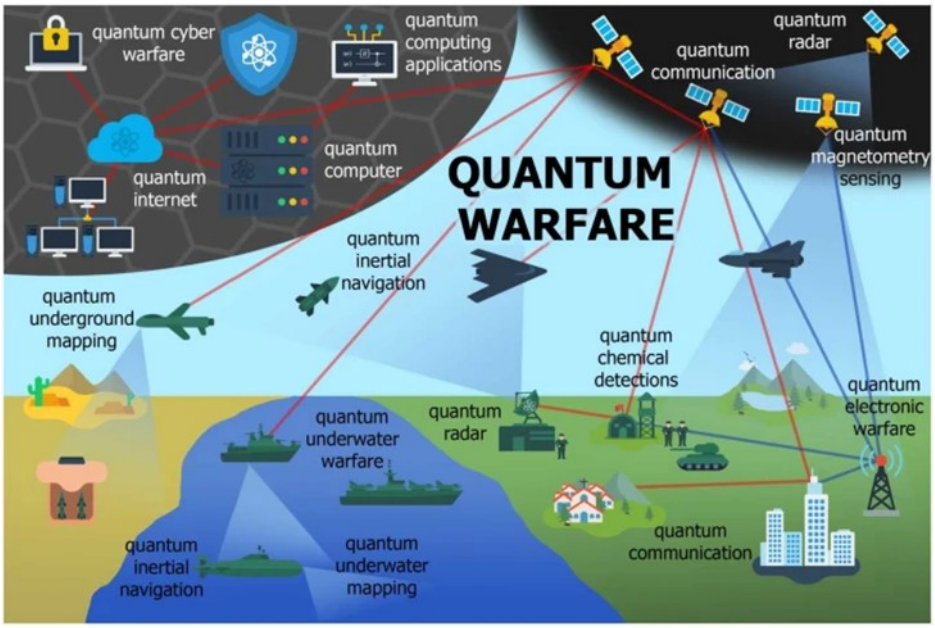
[88] la tecnologia stealth, detta anche tecnologia a bassa osservabilità, è una sotto disciplina della tattica militare e delle contromisure elettroniche passive e attive che copre una gamma di metodi utilizzati per rendere meno visibili personale, aerei, navi, sottomarini, missili, satelliti e veicoli terrestri.

[89] Krelina, M. (2021), "*Quantum technology for military applications"*, EPJ Quantum Technology 8, 24, Springer Open.

significativi nel rilevamento di tutte quelle piattaforme che operano sotto il livello del mare, rendendo gli oceani "trasparenti".[90]

Tuttavia, l'applicazione militare di queste tecnologie incontrerebbe un limite nella fragilità degli stati quantici, che possono essere interrotti da movimenti minimi, cambiamenti di temperatura o altri fattori ambientali. Come ha spiegato il fisico Mikkel Hueck, "se i futuri dispositivi che usano le tecnologie quantistiche richiederanno un raffreddamento a temperature molto basse, ciò li renderà costosi, ingombranti e affamati di energia". Di conseguenza, l'adozione diffusa richiederà probabilmente progressi significativi nello sviluppo dei materiali e nelle tecniche di fabbricazione.[91]

Figura 1, Possibili applicazioni militari delle tecnologie quantistiche. Fonte: EPJ Quantum Technology.



Le tecnologie quantistiche hanno il potenziale per influenzare profondamente molti settori dell'attività umana, in particolare quello della difesa, dove accresceranno la sensibilità e l'efficienza degli strumenti, introducendo nuove capacità e affinando le tecniche di guerra moderna. Come illustrato nella Figura 1, le possibili applicazioni della tecnologia quantistica per la difesa, la sicurezza, lo

[90] Congressional Research Service (2020), *"Emerging Military Technologies: Background and Issues for Congress".*
[91] Ibidem.

spazio e l'intelligence in diversi aspetti del new warfare sono estremamente numerose. Tuttavia, è importante considerare che molte applicazioni sono ancora più teoriche che realistiche.

Il significativo progresso in ambito quantistico raggiunto in laboratorio non sempre si traduce in un progresso simile al di fuori di esso. Il dispiegamento reale coinvolge anche altri aspetti, come la portabilità, la sensibilità, la risoluzione, la velocità, la robustezza, e il costo; senza contare che l'integrazione della tecnologia quantistica in una piattaforma militare è ancora più impegnativa, visti i requisiti ulteriori che dovrebbe soddisfare. A parte i computer quantistici - che saranno per lo più situati in *data centers* in modo simile a quelli per uso civile - l'integrazione e l'implementazione del rilevamento, dell'imaging e delle reti quantistiche affrontano diverse sfide, poste dalle maggiori esigenze dell'uso militare (in confronto ai requisiti civili, industriali o scientifici).[92] Inoltre, questo settore è ancora in uno stato embrionale: ulteriori scoperte, con accezione sia positiva che negativa, potrebbero generare ulteriori vantaggi o svantaggi.

4. LE ARMI AUTONOME LETALI (LAWS)

Anche se non esiste una definizione concordata a livello internazionale di sistemi d'arma autonomi letali, il Dipartimento della Difesa statunitense definisce i LAWS come una classe di sistemi d'arma in grado sia di identificare autonomamente un bersaglio, sia di impiegare un'arma per ingaggiarlo e neutralizzarlo, senza il controllo umano.[93] I sistemi d'arma autonomi, quindi, sono in grado di portare a termine compiti specifici in autonomia, senza l'input di un operatore.

Anche se questi sistemi non vedono ancora uno sviluppo diffuso, si prevede che giocheranno un ruolo fondamentale in contesti operativi caratterizzati da ambienti in cui i sistemi tradizionali potrebbero non essere in grado di operare. Questo livello di autonomia è noto anche come *man out of the loop* o "piena autonomia". Tali sistemi, che sono definiti sulla base del loro livello di autonomia operativa, possono essere supervisionati dall'uomo, o *man on the loop*, in cui gli operatori hanno la capacità di monitorare e fermare l'ingaggio dell'arma; o essere

[92] Van Amerongen, M. (2021), *"Quantum technologies in defence & security"*, NATO Review, https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

[93] United States Department of Defense Directive 3000.09 (2012-2017), *"Autonomy in Weapon Systems"*.

sistemi semi-autonomi, definiti *man in the loop*, che ingaggiano solo singoli obiettivi o gruppi specifici di obiettivi, che sono stati selezionati da un operatore umano.

I LAWS utilizzano algoritmi informatici di IA e suite di sensori per classificare un oggetto come ostile, prendere una decisione di ingaggio e utilizzare un'arma sul bersaglio. Come sottolineato da diversi analisti, i sistemi d'arma autonomi potrebbero permettere di colpire obiettivi militari in modo più accurato, riducendo quindi il rischio di danni collaterali o vittime civili.[94] Circa 25 Paesi e 100 organizzazioni non governative hanno chiesto un divieto preventivo sulle LAWS, mossi da preoccupazioni etiche, come la possibile percezione di una assenza di responsabilità per l'impiego e una eventuale incapacità di rispettare i requisiti di proporzionalità e distinzione.[95] Alcuni analisti hanno anche sollevato preoccupazioni circa i potenziali rischi operativi posti dalle armi letali autonome, che si concretizzano in "hacking, manipolazione del comportamento da parte del nemico, interazioni impreviste con l'ambiente operativo, o semplici malfunzionamenti ed errori del software".[96] Tali rischi potrebbero essere presenti nei sistemi automatizzati, ed essere intensificati nei sistemi autonomi, nei quali se l'operatore umano non fosse in grado di intervenire fisicamente, potrebbero generare conseguenze indesiderate, come effetti distruttivi più ampi, casi di fuoco amico e vittime civili.

Un'altra dimensione fondamentale dei sistemi autonomi è il loro grado di complessità - sia quella del sistema stesso sia quella dell'ambiente in cui opera - che influenza la capacità dell'operatore umano di prevederne e controllarne il comportamento. In generale, sistemi più semplici - che operano in ambienti più semplici - saranno più facili da prevedere e, anche se probabilmente più limitati nelle tipologie di operazioni che potranno eseguire, il loro funzionamento sarà presumibilmente più trasparente per gli operatori. Tuttavia, anche la gamma di ambienti e situazioni in cui potranno operare sarà verosimilmente più limitata. Per operare in una vasta gamma di scenari e svolgere missioni più difficili sono necessari sistemi autonomi più sofisticati che, per necessità, sono inevitabilmente più complessi. Questa complessità può rendere il sistema meno trasparente nei suoi processi anche per gli operatori addestrati. Di conseguenza, prevedere il comportamento del sistema, in particolare quando opera nel mondo reale in ambienti complessi e non strutturati, può essere più difficile.[97]

---

[94] U.S. Government (2018), *"Humanitarian Benefits of Emerging Technologies in the Area of Lethal Autonomous Weapons"*, United Nations Convention on Certain Conventional Weapons.
[95] Congressional Research Service (2021), *"Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems"*.
[96] Scharre, P. (2016), *"Autonomous Weapons and Operational Risk"*, Center for a New American Security.
[97] *Ibidem*

Per limitare tali rischi, i sistemi autonomi dovrebbero essere testati e valutati per garantire il loro funzionamento, come previsto in ambienti operativi realistici e contro avversari mutevoli. Dovrebbero altresì completare gli ingaggi in un lasso di tempo coerente con le intenzioni del comandante e dell'operatore e, se non fossero in grado di farlo, terminare le loro attività o cercare un ulteriore input dell'operatore umano prima di continuare. Tali sistemi, infine, dovrebbero essere resilienti al punto da riuscire a ridurre al minimo i guasti in grado di causare ingaggi involontari o perdita di controllo, a tutto vantaggio di attori non autorizzati. Qualsiasi modifica dello stato operativo, per esempio a causa dell'apprendimento automatico, richiederebbe che il sistema passi nuovamente attraverso un processo di test e valutazione per accertarsi che abbia mantenuto le sue caratteristiche di sicurezza e la capacità di funzionare come inizialmente previsto.[98]

Con l'avanzare della tecnologia, è necessario vagliare attentamente i rischi dell'impiego di tali sistemi. Gran parte del dibattito corrente si concentra su questioni legali, morali o etiche. Tuttavia, le armi autonome sollevano anche importanti questioni di controllabilità e sicurezza, soprattutto in caso di guasto. In un periodo di impiego operativo abbastanza lungo, alcuni fallimenti sono inevitabili e utilizzare armi autonome significherebbe accettare le conseguenze di questi fallimenti[99]

È necessaria una maggiore trasparenza tra gli Stati su come affrontare il tema dell'autonomia nei sistemi d'arma. Sono pochi i Paesi che hanno approntato politiche nazionali chiare sull'uso di tali strumenti. Dato il potenziale di interazioni pericolose tra sistemi autonomi e i rischi precedentemente menzionati, è particolarmente urgente giungere ad una regolamentazione coerente e condivisa a livello internazionale sul loro impiego. Il confronto e la competizione tra le Grandi Potenze in tema di Difesa e Sicurezza porta naturalmente ad una corsa verso la conquista di maggiore efficienza delle proprie Forze Armate: un potenziamento che passa attraverso una maggiore velocità operativa che, a sua volta, richiede una maggiore automazione, spingendo tale corsa ad un'ulteriore accelerazione del ritmo della battaglia. Il risultato di questo continuo incremento di velocità e automazione potrebbe sfociare in una situazione di instabilità, allorché, interazioni inaspettate tra sistemi autonomi o hacking potrebbero condurre a una "guerra lampo", portando un eventuale conflitto a sfuggire rapidamente dal controllo umano.

---

[98] Congressional Research Service (2021), *"Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems"*.

[99] Scharre, P. (2016), *"Autonomous Weapons and Operational Risk"*, Center for a New American Security.

5. L'IPERSONICO

Si definiscono ipersoniche tutte quelle armi che sono in grado di spostarsi ad una velocità di almeno Mach 5, pari a cinque volte la velocità del suono. La maggior parte dei missili balistici tradizionali vola a velocità ipersoniche, mentre generalmente i missili da crociera tradizionali volano a velocità subsoniche (meno di Mach 1) e supersoniche (da Mach 1 a 5). In pratica, il termine "armi ipersoniche" si riferisce per ad armi che volano a quota minore dei missili balistici intercontinentali, maggiore dei tradizionali missili da crociera e che sono in gran parte destinate ad un uso regionale piuttosto che intercontinentale.[100] Ci sono due categorie di armi ipersoniche: i velivoli a planata ipersonica (HGV), che sono lanciati da un razzo prima di planare verso un obiettivo; e i missili da crociera ipersonici (HCM), che sono alimentati da motori ad alte prestazioni per tutta la durata del volo.[101] I sistemi a planata ipersonica (HGV) sono tipicamente lanciati con un razzo nell'atmosfera e rilasciati a un'altitudine tra i 40 e i 100 km da dove planano verso il loro obiettivo. Gli HGV hanno una portata paragonabile ai missili balistici, ma volano a un'altitudine inferiore. Una porzione trascurabile del loro percorso di volo segue una traiettoria balistica. Inoltre, tali sistemi sono manovrabili durante la fase di planata e possono essere reindirizzati in volo verso un obiettivo diverso da quello inizialmente previsto. I missili da crociera ipersonici (HCM), invece, in quanto alimentati per l'intero volo, devono essere spinti alla velocità di circa Mach 5 prima che un motore a reazione *(ramjet, scramjet)* possa subentrare per mantenerla. Gli HCM potrebbero essere lanciati da terra, dall'aria o da una nave e probabilmente volerebbero a un'altitudine di 20-30 km, oltre la portata della maggior parte degli attuali sistemi di difesa missilistica aria-superficie e sarebbero in grado di raggiungere obiettivi che si trovano a 1000 km di distanza in pochi minuti.[102]

I missili balistici seguono una traiettoria balistica parabolica largamente prevedibile, volando in alto sopra l'atmosfera prima di precipitare di nuovo verso la Terra. Ciò permette a chi è all'estremità ricevente di seguire più facilmente il missile balistico -nella sua fase intermedia di volo - attraverso i radar e di ricavare previsioni ragionevoli su dove atterrerà la testata. Gli HGV, invece, non seguono una traiettoria balistica parabolica e possono essere manovrati durante la rotta verso l'obiettivo, diminuendo significativamente la prevedibilità della traiettoria e rendendo quindi difficile l'applicazione di contromisure ed una eventuale difesa.

---

[100] Congressional Research Service (2020), *"Emerging Military Technologies: Background and Issues for Congress".*

[101] Ibidem.

[102] Congressional Research Service (2021), *"Hypersonic Weapons: Background and Issues for Congress".*

Bugos, S. et al. (2021), *"Understanding Hypersonic Weapons: Managing the Allure and the Risks"*, Arms Control Association Report.

Inoltre, sono presumibilmente meno rilevabili dai radar a causa della rotta a bassa quota rispetto ai missili balistici.

Ci sono pareri contrastanti riguardo le implicazioni strategiche delle armi ipersoniche. Alcuni analisti hanno identificato due fattori che potrebbero avere conseguenze significative: 1) il breve tempo di volo dell'arma che, a sua volta, comprime i tempi di risposta e 2) la sua imprevedibile traiettoria di volo, che potrebbe generare incertezza sull'obiettivo dell'arma e quindi aumentare il rischio di errori di calcolo o di escalation involontaria in caso di conflitto.[103] Altri analisti sostengono, invece, che le implicazioni strategiche delle armi ipersoniche sono minime. Non varierebbe, infatti, la già presente capacità di colpire con missili balistici intercontinentali che, se lanciati in massa, potrebbero sopraffare le difese missilistiche.[104]

Lo sviluppo e il potenziale dispiegamento futuro delle armi ipersoniche mettono in luce una serie di temi e questioni più ampie che meritano attenzione. L'implementazione e l'adozione di tali strumenti sta favorendo la ricerca e lo sviluppo di tecnologie per difendersi da esse: tra queste citiamo gli intercettatori cinetici, *railgun* elettromagnetici e laser ad alta potenza che, come verrà approfondito nel prossimo paragrafo, possono anche avere un potenziale utilizzo come armi offensive. Come accennato precedentemente, in taluni scenari le armi ipersoniche possono ridurre i tempi di risposta rispetto agli attuali missili da crociera e balistici, comprimendo significativamente le tempistiche di decisione e quindi contribuendo alla tendenza a fare sempre più affidamento sull'intelligenza artificiale - sia per informare i decisori umani che per automatizzare alcuni processi - sollevando preoccupazioni circa i rischi insiti nel processo decisionale sottoposto a pressione temporale.

6. LE ARMI A ENERGIA DIRETTA (DEW)

Il Dipartimento della Difesa statunitense definisce le armi a energia diretta (DEW) come quelle che utilizzano energia elettromagnetica concentrata, anziché cinetica, per "disabilitare, danneggiare, o distruggere attrezzature, strutture e personale nemico".[105] Una DEW, quindi, è un sistema d'arma che utilizza un sistema di puntamento per controllare l'emissione di energia (elettromagnetica,

[103] Brehm, M., de Courcy Wheeler, A. (2019), *"Hypersonic Weapons – Discussion Paper for the Convention on Certain Conventional Weapons (CCW)"*, Article36.
[104] Ibidem.
[105] United States Department of Defense (2020), *"Joint Electromagnetic Spectrum Operations"*, Joint Chiefs of Staff Publication 3-85.

laser, microonde, energia fotonica e radiazioni nucleari) come mezzo per danneggiare o distruggere attrezzature e strutture o ferire il personale nemico. Ci sono diversi tipi di design per un sistema DEW, in grado di produrre diverse forme e livelli di energia. Queste variazioni di design sono ciascuna più efficiente in base alle molteplici applicazioni di impiego: dai sistemi a bassa energia per il controllo delle folle e per interrompere temporaneamente il funzionamento dei sensori elettro-ottici, fino ai sistemi ad alta energia per causare danni materiali. Alcuni di questi progetti sono già stati introdotti in servizio da diverse Forze militari in tutto il mondo.

Una DEW non è un'arma a detonazione: non c'è esplosione, energia cinetica, frammentazione, impatto o penetrazione: c'è solo energia termica e luce, che causano effetti ed eventualmente danni non cinetici. L'esplosione, la frammentazione e i danni termici aggiuntivi possono verificarsi come effetti secondari derivanti dall'interazione iniziale fra l'energia e i materiali di cui è composto il bersaglio stesso. Il meccanismo di danno da energia termica si basa sulle proprietà termiche dei materiali di cui è composto il bersaglio. Se tali materiali risultano vulnerabili all'assorbimento di calore - concentrato in una piccola superficie e in un breve lasso di tempo - vengono riscaldati fino al punto di combustione o fusione.[106]

Tali armi si suddividono in ulteriori categorie:

- laser ad alta energia (HEL)
- radiofrequenza ad alta potenza (HPRF)
- microonde ad alta potenza (HPM)

Tali armi potrebbero essere utilizzate dalle forze di terra nella difesa aerea a corto raggio (SHORAD), contro i sistemi aerei senza equipaggio (C-UAS), o nelle missioni contro razzi, artiglieria e mortai (C-RAM). Le armi ad energia diretta potrebbero inoltre ridurre i costi relativi al munizionamento e, presumendo la disponibilità di un'alimentazione sufficiente, garantire autonomia quasi illimitata.[107] In contrasto con i sistemi convenzionali esistenti, potrebbero consentire un efficace strumento di difesa missilistica o verso eventuali sciami di sistemi senza pilota. Teoricamente, le armi DE basate sui laser potrebbero anche fornire opzioni per l'intercettazione di missili in fase di lancio, dato il loro tempo di percorrenza pari alla velocità della luce. Tuttavia, come nel caso della difesa missilistica ipersonica, gli esperti non sono in accordo sull'accessibilità, la fattibilità tecnologica e l'utilità di

[106] Spencer, M. (2020), *"Directed Energy Weapons: Playing with Quantum Fire"*, Australia Air Power Development Center.

[107] Congressional Research Service (2021), *"Department of Defense Directed Energy Weapons: Background and Issues for Congress".*

Congressional Research Service (2020), *"Emerging Military Technologies: Background and Issues for Congress".*

questa applicazione. Le armi a microonde ad alta potenza - un sottoinsieme delle armi ad energia diretta - potrebbero essere usate come mezzi non cinetici per disabilitare l'elettronica, i sistemi di comunicazione e i dispositivi esplosivi improvvisati, o come sistemi non letali per neutralizzare gli obiettivi.

Le armi ad energia diretta hanno da tempo catturato l'attenzione militare - e i budget - e sono ora all'apice della maturità tecnologica. Mentre rimangono dubbi sul fatto che alcuni modelli possano essere pienamente operativi, recenti test di prototipi di DEW hanno dimostrato che questa forma di armamento è andata oltre il concetto teorico. Man mano che la tecnologia sottostante matura e viene sottoposta a test al di fuori dei laboratori, probabilmente attirerà una maggiore attenzione da parte di Forze Armate e Governi che aspirano a raggiungere superiorità tecnica sugli avversari, anche sviluppando soluzioni per eventuali impieghi nello Spazio.

7. SISTEMI A GUIDA AUTONOMA

I progressi nell'ambito delle tecnologie disruptive influenzano il settore della robotica e delle capacità autonome modificando gli equilibri militari e le dinamiche belliche presenti e future. I sistemi senza pilota, dotati di un grado di autonomia variabile, sono oggi un fattore comune per gli eserciti del mondo e, nelle loro forme aeree, marittime e terrestri, sono utilizzati per svolgere vari tipi di missione: *intelligence*, sorveglianza e ricognizione (ISR), ricerca e salvataggio (S&R), logistica, sminamento e distruzione di ordigni esplosivi improvvisati (IED), pattuglia armata e distruzione mirata obiettivi.

Un esempio attuale di impiego di tali sistemi è il conflitto in Ucraina, che vede l'esercito di Kiev contrastare le truppe di Mosca tramite l'utilizzo dei Javelin e droni turchi "Bayraktar TB2" già impiegati nel 2021 dall'Azerbaigian contro l'esercito armeno. D'altro canto, l'esercito russo sembra impiegare il KUB-BLA, *"loitering munition"* della ZALA Aero, dotato di intelligenza artificiale, che lo rende capace di rilevare, riconoscere oggetti e quindi individuare target in tempo reale. Il KUB-BLA, sparato da un lanciatore portatile, è in grado di volare per 30 minuti, raggiungendo una velocità di 130 Km/h, e schiantarsi contro un bersaglio autonomamente identificato.

Stati Uniti, Cina, Russia, Regno Unito, Israele e Turchia, negli ultimi anni, hanno progressivamente aumentato gli investimenti in tale campo, progettando sistemi tecnologicamente all'avanguardia dotati di intelligenza artificiale, in grado di colpire obiettivi a distanza di centinaia di chilometri. Tali sistemi includono flotte di navi, veicoli terrestri, missili, aerei e droni guidati da intelligenza artificiale. Noto esempio di impiego di tali sistemi è quello di marzo 2021, in cui un drone turco Kargu-2 è

stato usato in Libia per ingaggiare attacchi autonomi contro obiettivi terrestri quali soldati e mezzi.

I progressi in tecnologie quali intelligenza artificiale, robotica e fusione dei dati sono in grado di rivoluzionare l'impiego dei sistemi a guida autonoma, consentendo a un gran numero di droni di operare in modo collaborativo, coordinato e reattivo per raggiungere obiettivi comuni. Anche se è alle prime fasi di sviluppo e applicazione sperimentale, lo sciame è un concetto che - se pienamente sviluppato - può avere profondi effetti tattici e strategici, offrendo maggiori opzioni difensive e offensive alle forze militari.

Coordinamento e reattività rappresentano gli elementi peculiari dello sciame: i droni che lo compongono sono interconnessi e in costante comunicazione tra loro per la condivisione *real-time* delle informazioni provenienti dai loro sensori e un *decision-making* collettivo guidato dall'intelligenza artificiale. Ogni elemento dello sciame ha uno specifico ruolo in un sistema più grande, che auto-coordina le azioni dei suoi elementi in modo dinamico. Ad esempio, alcuni elementi possono impiegare i propri sensori per la localizzazione e il tracciamento di bersagli, altri svolgere compiti di *jamming* e guerra elettronica, altri ancora ingaggiare forze ostili. Nel suo insieme, lo sciame reagisce dinamicamente ai cambiamenti nello spazio di battaglia, eseguendo complesse manovre non lineari e contro-intuitive.

L'efficacia dello sciame, come detto, dipende dalla connessione stabile tra le sue componenti e il corretto funzionamento dell'IA che lo governa, rendendolo così vulnerabile a *spoofing, jamming, cyber*-attacchi o malfunzionamenti tecnici: sarà dunque necessario compiere nuovi sforzi per sviluppare contromisure efficaci man mano che gli sciami saranno dispiegati e diventeranno più avanzati. Considerate l'intrinseca decentralizzazione degli sciami e la loro capacità di reagire rapidamente in modo complesso, non è escluso che l'arma *counter-swarm* diverrà un altro sciame.

Data la complessità tecnica e gli elevati costi del *know-how* necessario, è lecito ritenere che lo sciame sarà appannaggio delle maggiori potenze militari, che godranno di un notevole vantaggio sia contro le forze regolari prive di capacità analoghe, sia contro gli insorti grazie alla capacità dello sciame di garantire un monitoraggio quasi permanente e reattivo su una vasta area. Infine, alla luce dell'interesse che le maggiori potenze militari stanno esprimendo verso il potenziale degli sciami di sistemi *unmanned*, è prevedibile che tale tecnologia emergente diventerà *game-changer* della guerra dei prossimi decenni.

8. LE IMPLICAZIONI E GLI IMPATTI DI TALI TECONOLOGIE SUGLI ATTUALI PARADIGMI TATTICI E STRATEGICI: IL PASSAGGIO ALL'HIPERWARE

Le implicazioni dello sviluppo e dell'applicazione delle tecnologie *disruptive* nella Difesa sono molteplici e stanno cambiando le "regole del gioco". I temi della velocità, dell'efficienza e della precisione, così come la necessità del controllo umano sulle capacità militari alimentate dall'IA e, non ultimo, le implicazioni etiche dell'utilizzo di tali strumenti rappresentano il cuore della questione nell'attuale dibattito sulle applicazioni dell'intelligenza artificiale e la sicurezza nazionale. Le nostre società - sempre più interconnesse - stanno promuovendo una "democratizzazione" della tecnologia: il tasso di diffusione e disponibilità di soluzioni ad alto impatto tecnologico sarà sempre maggiore e "multi-settoriale". L'applicazione di queste tecnologie ai nuovi strumenti e metodi di guerra sta incentivando una dinamica internazionale di corsa agli armamenti, sia nelle armi convenzionali sia nelle *disruptive technologies*, mettendo in discussione gli attuali paradigmi strategici e gli equilibri di potere. Concetti come la difesa missilistica *"left of launch"*[108] e la disabilitazione delle strutture di comando e controllo nucleare con mezzi informatici potrebbero rafforzare un approccio *"use it or lose it"*[109] per le relative capacità di *first strike*[110].

Inoltre, diversi esperti hanno sollevato preoccupazioni riguardo la possibilità di impiego di *deepfakes* per manipolare e influenzare i processi di comando e controllo e i sistemi di allarme rapido, nonché per alterare i dati su cui opera l'IA, causando conseguenze indesiderate e potenzialmente dannose.[111] Per rispondere efficacemente ai rischi generati da tali contingenze, l'era digitale richiede la creazione di elevate capacità di "cyber deterrenza". Infatti, il combattimento non si sta solo muovendo verso la robotica, ma sta anche diventando "etereo". Ad esempio, durante la sua incursione in Georgia nel 2008, la Russia è diventata la prima nazione a schierare attacchi cibernetici sui sistemi di comando, controllo e comunicazione del nemico per supportare un'invasione di terra. Allo stesso modo, per ritardare il programma nucleare iraniano, gli Stati Uniti e Israele hanno

---

[108] La strategia *"left of launch"* si basa su un attacco preventivo con nuove tecnologie non cinetiche, come la propagazione elettromagnetica, cyber così come la forza offensiva per sconfiggere le minacce di missili balistici nucleari prima del loro lancio.

[109] *"Use it or lose it"*, letteralmente "usalo o perdilo", è l'idea che, se uno Stato dovesse temere che il suo arsenale nucleare possa essere neutralizzato, preferirebbe usare le sue armi nucleari all'inizio di una crisi prima di perderle.

[110] Il *"first strike"*, noto anche come attacco nucleare preventivo, è un attacco indirizzato all'arsenale nucleare di un opponente che impedisce effettivamente la ritorsione contro l'attaccante.
Vienna Center for Disarmament and Non-Proliferation (2021), *"Deterrence Stability and the 21st Century Technology Boom"*.

[111] Singh Tanwar, S. (2020), *"Disruptive Technologies: Impact on Warfare & Their Future in Conflicts Of 21st Century",* Centre for Land Warfare Studies.

presumibilmente lanciato il virus *Stuxnet*, che ha compromesso le capacità delle centrifughe impegnate nel processo di arricchimento dell'uranio. La Cina è entrata in possesso di grandi database di informazioni sul personale governativo degli Stati Uniti, oltre a penetrare nelle reti degli appaltatori della Difesa, delle compagnie aeree e delle aziende tecnologiche statunitensi.

Questi esempi, che rappresentano solamente "la punta dell'iceberg", illustrano i sostanziali progressi nella tecnologia delle armi negli ultimi due decenni, a cui gli osservatori a volte si riferiscono come una "rivoluzione negli affari militari".[112] Con l'avvento dell'IA e di altre tecnologie emergenti, tuttavia, le definizioni tradizionali a cui siamo abituati sono destinate a cambiare. Ad un livello fondamentale, la battaglia, la guerra e il conflitto sono processi competitivi in termini temporali. Da tempo immemorabile, infatti, gli esseri umani hanno cercato di essere più veloci nella competizione derivante dal combattimento, sia in senso assoluto che relativo. E, a questo proposito, l'IA cambierà drasticamente la velocità della guerra, non solo modificando il ruolo dell'uomo nel conflitto, ma facendo anche leva sulla tecnologia come mai prima d'ora. E ciò avviene non solo perché la tecnologia sta cambiando, ma anche a causa dell'accelerazione del suo tasso di trasformazione.

Questo è il tema centrale che si pone dinanzi per l'approntamento ai futuri conflitti armati: l'attore che sarà in grado di creare, padroneggiare e sfruttare un equilibrio, citando Clausewitz, tra la natura della guerra e il carattere della guerra - soprattutto all'interno del nuovo ambiente di IA, analisi dei dati e *supercomputing* - inevitabilmente prevarrà nel conflitto.[113] In uno scenario geopolitico sempre più definito da tecnologie nuove ed emergenti, la Difesa nazionale si pone come una delle aree di sviluppo più logiche per il XXI secolo. È quindi di fondamentale importanza valutare gli impatti rivoluzionari dell'intelligenza artificiale e di altre tecnologie emergenti su ogni aspetto della sicurezza nazionale e dei conflitti armati, compreso il ritmo accelerato della guerra e il ruolo critico del continuo controllo umano. Con l'avvento dei *big data* e del *deep learning*, la terza rivoluzione militare permetterà una "sinergia digitale" di IA e altre tecnologie rivoluzionarie per raccogliere, elaborare ed interpretare *zettabyte*[114] di dati in pochi secondi. Nei conflitti del futuro, incentrati sulle decisioni - dove una rete adattiva

---

[112] Rabkin, J., Yoo, J. (2017), *"Disruptive Technologies to Upend Rules of War"*, National Defense Magazine.

[113] Allen, J., West, D. (2020), *"Op-ed: Hyperwar is coming. America needs to bring AI into the fight to win — with caution"*, CNBC. https://www.cnbc.com/2020/07/12/why-america-needs-to-bring-ai-into-the-upcoming-hyperwar-to-win.html

[114] Lo *zettabyte* è un'unità di misura dell'informazione o della quantità di dati, il termine deriva dalla unione del prefisso zetta con byte ed ha per simbolo ZB. *"Zetta"* è un cosiddetto prefisso decimale, il significato del quale è definito nel sistema internazionale di unità di misura, e che corrisponde a 10^{21} *byte* ovvero 1.000.000.000.000.000.000.000 (un triliardo) di *byte*.

formerà la "spina dorsale" connessa di comandanti, operatori e armi - prevarrà chi sarà in grado di sfruttare l'infrastruttura tecnologica per arrivare per primo a prendere le decisioni migliori.[115]

Se questa è l'ultima frontiera cognitiva, qual è il ruolo umano nel mosaico delle decisioni prese in pochi secondi e delle battaglie condotte in pochi minuti? Nel loro trattato del 2017 "*On Hyperwar",* il generale dell'USMC John Allen e il fondatore di SparkCognition Amir Husain ridefiniscono l'iper-guerra come "un tipo di conflitto in cui il processo decisionale umano è quasi del tutto assente dal ciclo "osservare-orientare-decidere-agire" (OODA).[116] Di conseguenza, il tempo associato a un ciclo OODA sarà ridotto a risposte quasi istantanee".[117] L'hyperwar propaga il tradizionale OODA *loop* ed espande le strutture decisionali monolitiche in reti resilienti, scalabili e adattabili, con la discrezionalità automatizzata di selezionare, mirare e impegnarsi con le forze avversarie più velocemente delle loro controparti umane.[118] L'hyperwar si basa su un sistema di sistemi e incorpora vari livelli di autonomia meccanizzata per liberare i vincoli logistici, coordinare i movimenti, analizzare i dati e riconoscere i modelli. Le macchine penseranno e agiranno più velocemente degli umani, adattandosi alla compressione del tempo operativo, in un contesto in cui la velocità e la complessità saranno elementi fondamentali del campo di battaglia. Uno "stack decisionale" calcolato e modulare - abilitato dalle macchine - libera i vincoli di comando per consentire alla componente umana la risoluzione di problemi astratti di livello superiore. Se sfruttato correttamente, il vantaggio finale del processo decisionale militare meccanizzato è un aumento della "larghezza di banda strategica".[119] Infatti, mentre le decisioni tattiche saranno automatizzate, le decisioni strategiche rimarranno dominio degli umani.

L'hyperwar, o il combattimento condotto sotto l'influenza e il supporto dell'IA - dove il processo decisionale umano è quasi del tutto assente dal ciclo osservare-orientare-decidere-agire (OODA) - sta già iniziando a permeare nelle operazioni militari. La dimensione umana della guerra sarà messa a dura prova in tale futuro ecosistema di iper-guerra, sarà quindi necessario uno sforzo notevole nel reclutare, educare, addestrare e guidare il talento umano.

---

[115] Steel, C. (2021), *"Hyperwar: How Militarized AI is Transforming the Decision-Making Loop"*, American Security Project.

[116] Il ciclo OODA è il ciclo osservare-orientare-decidere-agire, sviluppato dallo stratega militare e colonnello dell'aeronautica degli Stati Uniti John Boyd. Boyd ha applicato il concetto al processo delle operazioni di combattimento, spesso a livello operativo durante le campagne militari. L'approccio spiega come l'agilità può superare la potenza nel trattare con gli avversari umani. Il concetto, inoltre, è particolarmente applicabile alla sicurezza informatica e alla guerra informatica.

[117] Allen, J. R., Husain, A. (2017), *"On Hyperwar"*, U.S. Naval Institute.

[118] Ibidem.

[119] Steel, C. (2021), *"Hyperwar: How Militarized AI is Transforming the Decision-Making Loop"*, American Security Project.

La comprensione di quali decisioni e scelte siano necessarie per costruire ed operare nel nuovo scenario operativo - che include questi tipi di sistemi e richiede questo tipo di decisioni implementative - si può riscontrare in via embrionale in alcuni livelli della comunità della Difesa. Tuttavia, tale capacità decisionale dovrà essere costruita all'interno di un sistema che comprenda sia la Difesa sia l'Industria - in modo reciprocamente comprensibile e concordato - onde evitare il rifiuto di soluzioni assolutamente necessarie, dubbi sulle performance che possano mettere a repentaglio le operazioni o, peggio, lacune che potrebbero verificarsi laddove le applicazioni non includessero le caratteristiche che una parte ritiene siano state realizzate o eseguite dall'altra parte. Infatti, mentre l'Industria sta sfruttando in modo relativamente veloce la "rivoluzione digitale", a cominciare dai processi e dalle operazioni, la trasformazione digitale non è stata ancora pienamente affrontata in ambito Difesa, in tutte le sue sfaccettature e problematiche, incluse quelle etiche.

9. LA DETERRENZA NEL FUTURO CONTESTO HYPERWAR

Mentre gran parte del dibattito sulle armi abilitate da tecnologie disruptive si è concentrato sull'impatto umanitario, tali strumenti sollevano anche considerevoli questioni di stabilità strategica e deterrenza. Gli Stati hanno una lunga storia di cooperazione per regolamentare, vietare o sviluppare norme e aspettative comuni per una varietà di sistemi ad alto impatto sulla stabilità internazionale. Tuttavia, questa convergenza di tecnologie avanzate potrebbe incrementare significativamente le capacità militari di una nazione e generare quindi profondi mutamenti nel bilanciamento strategico internazionale, cambiando i presupposti dell'escalation e rendendo plausibile l'eventualità di una "guerra lampo".

Dalla balestra alle armi nucleari, infatti, lo sviluppo della tecnologia militare ha sempre aggravato il dilemma della sicurezza.[120] Se, ogni progresso nello sviluppo della tecnologia bellica porta con sé l'incertezza su come verrà impiegata o su quanto sarà potente, le nuove tecnologie disruptive introducono un grado di incertezza ancora maggiore sulle capacità che saranno in grado di generare. Ad esempio, all'inizio della Guerra Fredda, sia gli Stati Uniti che l'Unione Sovietica erano a conoscenza delle capacità distruttive delle armi nucleari e temevano che l'avversario potesse svilupparne di più potenti; il risultato fu la corsa agli armamenti nucleari. L'IA, dal canto suo, genera entrambe le forme di incertezza: nessuno sa ancora esattamente come le armi abilitate dall'IA saranno usate sul campo di battaglia, tanto meno quanto saranno potenti.[121] L'intelligenza artificiale introduce un ulteriore livello di incertezza anche in virtù del fatto di essere una tecnologia abilitante. Infatti, piuttosto che costituire un singolo sistema d'arma in sé, l'IA può essere incorporata in molteplici sistemi e infrastrutture come i centri di comando e controllo e nelle soluzioni logistiche. Eppure, non è facile determinare come queste innovazioni cambieranno la natura dei conflitti bellici. Che effetto avranno sciami di sottomarini senza equipaggio sulla guerra navale? Cosa succederà quando l'IA non sarà solo integrata negli armamenti e nei centri di comando e controllo esistenti, ma inserita in essi tramite un processo *bottom-up*? Quale esercito sarà in grado di integrare l'IA in maniera più efficiente e veloce nei suoi sistemi d'arma e nelle sue tattiche e con quale vantaggio sul campo di battaglia? Questa incertezza su come l'IA sarà impiegata e quanto sarà efficace genera quindi sfide significanti per gli Stati, in particolare nella strategia militare.[122]

---

[120] Meserole, C., (2018), *"Artificial intelligence and the security dilemma"*, Brookings.
[121] Ibidem.
[122] Ibidem.

Le tecnologie emergenti e *disruptive* stanno sfidando il modo in cui la deterrenza, la Difesa e, più in generale, le strategie di sicurezza sono formulate e applicate a livello nazionale e multilaterale. Le dimensioni territoriali non rappresentano più il fattore principale per determinare il potere di uno Stato. Lo sviluppo tecnologico, l'agilità di manovra nonché la velocità e l'accuratezza del processo decisionale conteranno più delle risorse a disposizione.[123] Pertanto, un attore di piccole dimensioni - ma con notevoli capacità tecnologiche - potrebbe essere in grado di sfidare con successo una grande potenza. Le nuove tecnologie non solo determineranno il modo in cui i conflitti futuri saranno combattuti e vinti, ma avranno anche effetti dirompenti sulla strategia delle grandi potenze e sulla guerra stessa, ponendo inevitabilmente l'accento sul processo di rivoluzione della tecnologia militare. A questo proposito, oltre che all'effetto di tali tecnologie in ambito bellico, è necessario dedicare particolare attenzione anche verso le implicazioni che sorgono da quei sistemi che sono *dual-use* e prerogativa di entità e innovazioni in ambito commerciale.

Inoltre, dalla prospettiva della stabilità strategica, potrebbero mutare anche le valutazioni intraprese dagli Stati per determinare un deterrente minimo e credibile. Queste stime cambieranno significativamente nell'era dell'*hyperwar*, così come le tipologie e gradi di protezione che sarà necessario garantire ai sistemi e alle infrastrutture strategiche.

La situazione è resa ancora più complicata dall'ambiente multipolare della competizione e del conflitto. Un'azione intesa a scoraggiare un avversario potrebbe produrre preoccupazioni inaspettate tra gli altri attori.[124] La deterrenza nucleare ha prodotto stabilità strategica adoperando una combinazione di negoziazione, dichiarazioni pubbliche e programmi mirati all'acquisizione di armamenti. Nell'ambiente attuale e del prossimo futuro, acquisire più armi non produrrà maggiore stabilità e la capacità di negoziare su questioni strategiche e di controllo degli armamenti con gli avversari è significativamente ridotta rispetto al passato. Trovare un modo per coordinare questo nuovo ambiente strategico e rafforzare la stabilità internazionale non è intuitivo. Infatti, considerando che gli Stati stanno cercando di ampliare la deterrenza contro rischi emergenti e contro nuove armi non nucleari, il vecchio paradigma della stabilità è ormai compromesso e dovrà essere rinnovato tenendo conto delle armi abilitate da tecnologie dirompenti e dei loro effetti sulla deterrenza.

---

[123] Hasan, S. (2020), *"How Disruptive Technologies Affect Deterrence, Defence and Security"*, Beyond the Horizon.

[124] Lewis, J. (2014), *"Disruptive Technologies and the Future of Deterrence"*, James Lewis, Center for Strategic and International Studies.

Dandashly, A. Et al. (2021), *"Multipolarity and EU Foreign and Security Policy: Divergent Approaches to Conflict and Crisis Response"*, JOINT Research Papers No.6.

Come sottolineato da diversi osservatori, c'è una tendenza a pensare al conflitto in modo lineare come un percorso diretto verso l'escalation della crisi.[125] Tuttavia, la complessità tecnologica potrebbe permettere agli attori in campo di saltare alcuni step nel processo. Potrebbe infatti verificarsi un allontanamento dai percorsi prevedibili e un avvicinamento a una dinamica *"wormhole"* dell'escalation delle crisi, in cui gli stati in competizione potrebbero muoversi fra livelli di conflitto sub-convenzionali e strategici.[126] L'idea di percorsi non lineari di escalation guadagna ulteriormente plausibilità quando sono coinvolti attori non statali e l'attribuzione diventa un processo lungo e complesso, che richiede un mix di competenze tecniche, sociali e politiche.[127] Alla luce di tale complessità, i fattori che incoraggiano l'*hyperwar* possono prestarsi allo sviluppo di una sorta di "iper-coercizione", in cui sarà plausibile la capacità di prevedere e anticipare le mosse di un avversario.[128] Nel fornire ai decisori politici e militari opzioni tattiche e strategiche alternative - basate su una valutazione ad ampio raggio di una quantità inimmaginabile di dati e informazioni - l'IA può persuadere gli attori in comando a delegare alcuni compiti alle macchine, rendendo necessaria un riconsiderazione degli attuali presupposti e piani riguardanti l'automazione in guerra.

Inoltre, l'IA può generare - a lungo termine - una consapevolezza situazionale basata sull'analisi predittiva.[129] Infatti, grazie alla fusione e analisi di informazioni sul comportamento passato e corrente degli avversari, l'IA consentirà una concreta capacità di anticiparne eventuali mosse. I difensori saranno così in grado di rispondere preventivamente influenzando e scoraggiando la postura ed eventualmente dissuadere l'avversario dal perseguire determinate azioni ostili.

L'IA introduce quindi la capacità di influenzare la deterrenza militare e la coercizione in modi unici: può alterare i calcoli costi-benefici eliminando la *fog of war*, imponendo la razionalità sulle decisioni politiche e diminuendo il costo umano dell'impegno militare.[130] Può ricalibrare l'equilibrio tra misure offensive e difensive, facendo pendere l'ago della bilancia a favore della prevenzione, e minare i presupposti esistenti nella deterrenza convenzionale e nucleare. In altre parole, l'IA potrebbe fornire agli utilizzatori la capacità di agire sulla base di informazioni raccolte, sintetizzate ed elaborate in tempo reale, aumentando la certezza e la

[125] Kubiak, K., Mishra, S. (2021), "*Emerging & disruptive technologies and nuclear weapons decision making: Risks, challenges & mitigation strategies*", European Leadership Network.
[126] Ibidem.
[127] Ibidem.
[128] Wilner, A., Casey, B. (2020), *"New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour"* in *"Deterrence in the 21st Century-Insights from Theory and Practice"*, Netherlands Annual Review of Military Studies.
[129] Ibidem.
[130] Ibidem.

severità delle strategie di coercizione e comprimendo la distanza tra l'*intelligence*, le decisioni politiche e l'azione coercitiva.[131]

In linea generale, il contesto del prossimo futuro richiede quindi il mantenimento di un primato tecnologico credibile, in grado di alimentare una deterrenza efficace che induca eventuali aggressori ad effettuare - prima delle rispettive iniziative - una valutazione costo-beneficio. Senza questo primato, l'asimmetria esistente tra sistemi autocratici e democratici sarà difficilmente mitigata da qualsivoglia diplomazia e forma di diritto internazionale. L'altra asimmetria da considerare, sul piano strategico, è data dallo sbilanciamento - per lungo tempo – tra i Paesi già tecnologicamente avanzati e quelli ancora ancora indietro nella corsa all'avanzamento tecnologico. L'hyperwar, lungi dal poter controllare e contrastare realtà più primitive, rischia di trovarsi di fronte quanto di più analogico e basico l'uomo possa utilizzare nel conflitto. Ecco perché la consapevolezza tecnologica deve essere accompagnata da una prima comprensione degli ecosistemi geo-economici e geo-politici. Senza un impianto di consapevolezza sarà difficile mantenere una soglia di deterrenza credibile a difesa del sistema valoriale cui le differenti comunità del globo sentono di appartenere, specie se incardinate su di una struttura democratica e pacifica. A differenza della deterrenza nucleare, che oggi possiamo definire alquanto statica nel suo potenziale distruttivo, la deterrenza tecnologica e digitale troverà costante evoluzione e conseguenti esperienze di adattamento che partiranno dalle comunità scientifiche e militari.

[131] Ibidem.

10. TECNOLOGIE DISRUPTIVE, DIFESA E SICUREZZA: QUESTIONI ETICHE E MORALI

" Oggi, la domanda chiave per l'umanità è se avviare una corsa globale agli armamenti abilitati dall'IA o impedirne l'inizio"[132]: questo il messaggio al cuore della lettera firmata da oltre mille esperti e ricercatori di alto profilo nel campo dell'intelligenza artificiale - tra cui Elon Musk (CEO e CTO della compagnia aerospaziale SpaceX, CEO e product architect della casa automobilistica Tesla), Steve Wozniak (co-fondatore di Apple), Demis Hassabis (CEO e co-fondatore di Google DeepMind), Stephen Hawking (cosmologo, fisico, matematico, astrofisico scomparso nel marzo 2018) e Stuart J. Russell (docente di computer science presso la University of California, Berkeley) - alla Conferenza internazionale congiunta sull'intelligenza artificiale, tenutasi a Buenos Aires nel luglio 2015. "L'IA *ha raggiunto un punto in cui il dispiegamento di armi autonome è - praticamente se non legalmente - fattibile entro anni, non decenni, e la posta in gioco è alta: le armi autonome sono state descritte come la terza rivoluzione nella guerra, dopo la polvere da sparo e le armi nucleari"*[133]. L'IA - argomentavano i sottoscrittori del documento - può essere impiegata per rendere il campo di battaglia un luogo più sicuro per il personale militare. Tuttavia, l'abbassamento della soglia di rischio per gli operatori in campo potrebbe tradursi in un incentivo ad azioni offensive, in grado di provocare una maggiore perdita di vite umane sul fronte avversario. In tale scenario, se una potenza militare iniziasse a sviluppare sistemi in grado di selezionare obiettivi e operare senza il controllo umano diretto, avvierebbe una corsa agli armamenti simile a quella per gli armamenti nucleari.

Si tratta di una posizione molto netta che, tuttavia, negli anni successivi, ha visto alcuni tra gli stessi autori della lettera mutare il loro orientamento del tutto o in parte, ma comunque riconoscere unanimemente l'enorme potenziale positivo dell'Intelligenza Artificiale per il progresso sostenibile del Pianeta.

A distanza di sette anni dalla Conferenza di Buenos Aires, resta aperto, in ogni caso, il tema centrale del loro appello: l'IA rimuoverà del tutto l'uomo dai processi decisionali? Non è questo il caso, al momento, come spiega il generale John R. Allen, presidente della Brookings Institution ed ex comandante della NATO International Security Assistance Force and U.S. Forces - Afghanistan (USFOR-A*): "a dispetto del loro ampio ricorso alla tecnologia dei droni, gli Stati Uniti ad oggi richiedono un essere umano informato per ogni sistema che viene impiegato. È un punto morale di grande importanza sostenuto dai valori americani e dalle norme*

[132] Berkeley Engineering (2015), *"Open Letter on AI"*.
[133] Ibidem.

internazionali, e un limite voluto all'uso di certe tipologie di tecnologie"[134]. Il fatto stesso di dover sottolineare la centralità dell'elemento umano nel nuovo scenario, sempre più caratterizzato dall'impiego di tecnologie disruptive, rende ancor più evidente l'impatto che l'IA stia avendo sulla dottrina militare americana. In passato il simbolo assoluto della superiorità militare degli Stati Uniti era rappresentato dalla *"Triade strategica",* ovvero i tre pilastri della sua strategia di deterrenza nucleare, squadriglie missilistiche, flotte di bombardieri, sommergibili dotati di missili balistici. Oggi questa triade è raddoppiata, e ai tre strumenti menzionati si devono aggiungere l'Intelligenza Artificiale, l'analisi dei big data e il super computing: una rivoluzione a tutto tondo, sempre più pervasiva, che potrebbe - progressivamente e una volta per tutte - sostituire l'uomo *"dal processo di analisi ambientale, portando a valutazioni più accurate, ampie e a tempi di reazione molto più veloci"*[135]*.* In altre parole, la macchina supera l'elemento umano, con il rischio di portare con sé, in questo salto quantico, responsabilità ben definite e scelte basate su principi etici e morali, vale a dire tutto ciò che rende la nostra civiltà un lungo processo di evoluzioni storiche, culturali e sociali.

D'altro canto, la consapevolezza dello sviluppo tecnologico può diventare una delle chiavi di interpretazione della democrazia digitale. L'approccio passivo e di mero utilizzo del potenziale tecnologico, nel confronto tra gruppi organizzati (ma anche tra individui, cioè cittadini digitali), rischia di riprodurre "l'eterna rincorsa tra lo scudo e la lancia", con la differenza che l'ingegno umano e la capacità di controllarlo, indirizzarlo, volgerlo alle realizzazioni rischia di essere soppiantato dalla crescente capacità generatrice della macchina. Assieme alla consapevolezza, dunque, la focalizzazione sui fattori emotivi dell'intelligenza appare un altro cardine morale sul quale innestare parte della conoscenza digitale autonoma rappresentata dall'IA. Ciò al fine di mantenere il primato dell'originalità primogenita dell'essere umano sulla capacità esponenziale di elaborazione attuale ed empirica della macchina autonomamente intelligente. Così, forse, il cammino dell'umanità potrebbe non smarrirsi e non confondersi in galassie nebulose di dati che, nei volumi qualitativi e quantitativi attesi rischiano di esporre la superficie del pensiero autonomo umano alla confusione più totale. Se oggi siamo ancora forti della certezza di un'autonomia del pensiero è bene sfruttare questo tempo per porre le basi (umane) dell'*Hyper-thinking*, un modo totalmente nuovo e prevedibilmente integrato con le capacità AI per la produzione del pensiero umano.

Per inquadrare la portata del dibattito, è forse necessario allargare il nostro orizzonte di osservazione oltre il campo militare, considerando la trasformazione digitale come una porzione del più articolato ed ampio quadro dell'innovazione delle organizzazioni, il cui punto di partenza è sempre l'individuo, la sua cultura e

[134]Allen, J. R. (2018),*"Intelligenza Artificiale, una nuova era per la guerra"*, ISPI.
[135] Ibidem.

la sua consapevolezza. La crescente centralità del ruolo delle macchine mette a dura prova l'attuale visione antropocentrica, una visione in cui gli umani - dotati di empatia e capaci di gestire eccezioni ed ambiguità - hanno, fino ad oggi, governato ogni scelta decisiva, anche e soprattutto negli scenari più complessi. Possiamo immaginare un futuro in cui le macchine raggiungeranno questo livello di discernimento? Una domanda che diviene ancor più cruciale, se torniamo sul territorio della Difesa.

Come affermato dal teologo Paolo Benanti[136], la sicurezza nazionale è un *"tema trasversale, nelle sue accezioni di sicurezza fisica, digitale, sociale"* [137]. E l'innovazione tecnologica gioca un ruolo sempre più centrale per continuare a garantire il massimo livello di sicurezza a cittadini e territori. Tuttavia, la tecnologia resta lo strumento, non il fine. E va orientata e sviluppata*, "avendo ben chiari gli obiettivi strategici e mantenendo salda la rotta valoriale"*[138]. Una rotta che chiama in causa il tema della scelta delle regole, che devono essere commisurate alle prospettive e aspirazioni nazionali e principalmente alla stessa Etica, che può mutare nei diversi momenti storici e nelle differenti geografie del mondo. Si tratta di sfide globali che le nazioni non possono affrontare in solitario: per sfruttare le potenzialità e mitigare i rischi connessi all'applicazione dell'IA è opportuno valorizzare l'influenza reciproca in ottica d'interconnessione e interoperabilità a livello internazionale. Il confronto odierno avviene ed avverrà infatti con attori e regole diverse, in una cornice legale ancora da costruire, specialmente per quanto attiene le minacce ibride.

Siamo dunque di fronte a molte variabili, che concorrono a creare un contesto in costante evoluzione. L'innovazione tecnologica è infatti, per sua natura, un elemento dinamico. Altrettanto lo sono gli scenari geopolitici e le diverse evoluzioni culturali che determinano le scelte dei singoli Paesi. La definizione di regole e principi etici è un cammino articolato, che è necessariamente destinato ad attraversare tale complessità per trovare un terreno comune, una sintesi capace non già di rincorrere, bensì di accompagnare e favorire l'avanzamento tecnologico in ogni campo. Da qui l'esigenza di una "consultazione permanente" tra tutti gli attori che concorrono alla definizione delle regole del vivere civile e di quelle che governano, di conseguenza, le regole del conflitto: giuristi, militari, politici, diplomazia e, non ultimo, i tecnologi: coloro che ricercano, studiano, progettano e realizzano i sistemi di difesa. Insieme, queste diverse sfere devono operare per la stessa causa: costruire una logica dinamica, circolare e iterativa che adatti il

---

[136] Francescano del Terzo Ordine Regolare, teologo, si occupa di etica, bioetica ed etica delle tecnologie. In particolare, i suoi studi si focalizzano sulla gestione dell'innovazione: internet e l'impatto del Digital Age, le biotecnologie per il miglioramento umano e la bio-sicurezza, le neuroscienze e le neurotecnologie

[137] Report del 1° Workshop sull'Innovazione della Difesa 2021, *"Intelligenza Artificiale, Difesa e Sostenibilità. Implicazioni Etiche, Legali e Psicologiche"*, aprile 2021 - Centro Innovazione della Difesa (CID), con la collaborazione dell'European Institute for Innovation and Sustainability (EIIS)

[138] Ibidem.

linguaggio delle macchine alle esigenze umane, tenendo conto delle questioni etiche. Un processo circolare che non deve fermarsi mai, che deve considerare scenari sempre più complessi e che permetta all'uomo di mantenere il senso del limite nella propria idea di potenza e dell'uso della forza.

In conclusione, le nuove tecnologie seguiteranno ad avanzare e a raggiungere nuovi traguardi, nuove potenzialità, sulla spinta di future esigenze e adattamento continui. Fermare questo processo non è auspicabile né immaginabile. Al contrario, è necessario favorire e supportare l'accesso generalizzato e paritetico alle innovazioni, avviando un percorso virtuoso e costante che consenta agli organismi sociali e geopolitici di *"metabolizzare"* il progresso tecnologico al loro interno. L'economista Giacomo Becattini e il sociologo Luigi Burroni[139], nella loro analisi dei distretti industriali italiani, si riferivano a tale *"metabolizzazione"* come la capacità dei territori – Istituzioni, Imprese, Accademia, Cittadini – di saper accogliere, comprendere, gestire ed integrare l'innovazione tecnologica attraverso "spazi di decodifica", necessari per acquisire *"la consapevolezza di un processo complesso e articolato come quello del cambiamento tecnologico"*. Se riconduciamo questa riflessione al contesto che stiamo analizzando, il percorso per raggiungere tale consapevolezza non può che passare per una piattaforma di dialogo permanente, che coinvolga tutti gli attori chiave che contribuiscono alla costruzione di tali scenari - Governi, Forze Armate, Mondo Accademico e della Ricerca, Imprese - in un quadro di confronto multilaterale. È infatti su tale consapevolezza condivisa che potremo basare l'asse morale ed il perimetro di principi etici entro i quali operare e delimitare l'impiego delle nuove tecnologie nei futuri scenari di Difesa e Sicurezza.

[139] "*I distretto industriale come strumento di ricomposizione del sapere sociale*", Periodico "Sociologia del lavoro" - Anno: 2003, Fascicolo 92

Conclusioni:

- Le implicazioni dello sviluppo e dell'applicazione delle tecnologie disruptive nella difesa sono molteplici e stanno cambiando le "regole del gioco": velocità, efficienza e precisione delle operazioni militari, così come la necessità del controllo umano sulle capacità militari alimentate dall'IA, rappresentano il cuore della questione nell'attuale dibattito sulle applicazioni dell'intelligenza artificiale e la sicurezza nazionale.
- Il tradizionale paradigma della stabilità internazionale è messo in discussione e dovrà essere rinnovato tenendo conto delle armi abilitate da tecnologie dirompenti e dei loro effetti sulla deterrenza.
- Il contesto del prossimo futuro richiede il mantenimento di un primato tecnologico credibile, in grado di alimentare una deterrenza efficace che induca ipotizzabili aggressori ad effettuare-prima delle rispettive iniziative - una valutazione costo-beneficio.
- Il confronto avverrà con attori e regole diverse, in una cornice legale ancora da costruire, specialmente per quanto attiene le minacce ibride: da qui l'esigenza di una "consultazione permanente" tra tutti gli attori che concorrono alla definizione delle regole del vivere civile e le regole del conflitto, come giuristi, militari, politici, diplomazia e coloro che ricercano, studiano, progettano e realizzano i sistemi di difesa.

Capitolo V

La regolamentazione dell'INTELLIGENZA ARTIFICIALE oltre i confini dell'UNIONE EUROPEA: UN ESAME COMPARATIVO

di Antonio Malaschini

Sintesi: Non esiste, al di fuori dell'Europa, una proposta di regolazione generale dell'Intelligenza Artificiale. In Cina, Stati Uniti, Regno Unito e Russia si fa riferimento a norme già esistenti; all'ampliamento in via interpretativa delle tutele dei diritti personali e sociali; a standard di produzione e uso; a indirizzi e incentivi di natura diversa. Frutto questo anche del carattere duale, civile e militare (nonché di controllo sociale) dell'IA che induce i paesi con forte proiezione internazionale a grande cautela nel disciplinare e limitare queste tecnologie.

1. IL QUADRO NORMATIVO GLOBALE

Non esiste al momento una normazione nel campo dell'Intelligenza artificiale che abbia carattere ed uniformità globali[140]. Possiamo anzi dire che nei paesi ai quali faremo riferimento non troveremo, neanche al loro interno, una compiuta disciplina dei diversi aspetti della IA: da quello etico a quello della ricerca, da quello giuridico a quello della sua utilizzazione, da quello dei rischi potenziali a quello delle tutele, da quello della protezione dei diritti e delle libertà a quello del rapporto tra soggetti pubblici e privati e così via. Non esiste neanche una concorde definizione giuridica di cosa si intenda per IA, e solo nel periodo più recente si è consolidata l'opinione sulla necessità di una normazione: si riteneva fino ad oggi, e da alcuni ancora si ritiene, che si potesse fare riferimento alle norme esistenti, come quelle sulla cybersecurity e sulla commercializzazione e l'uso dei prodotti informatici; all'ampliamento, anche in via interpretativa, della disciplina a tutela dei diritti personali o sociali; a standard di produzione e utilizzazione già pensati per altri beni; alla istituzione di innumerevoli comitati, commissioni, gruppi di esperti che producevano pregevoli rapporti, indirizzi, proposte e risoluzioni quasi mai finalizzati ad una disciplina compiuta. Solo l'Unione Europea, come vedremo in seguito, ha avanzato nell'aprile del 2021 una proposta di ragionevole organicità. Nelle conclusioni accenneremo brevemente a quelle che riteniamo essere le ragioni di questo ritardo normativo. Ma vediamo quale è al momento il quadro nei Paesi al di fuori della UE.

[140] M.C. Buiten, "Towards intelligent regulation of Artificial Intelligence", in www.Cambridge.org/core, 15 aprile 2021.

2. CINA

Non c'è oggi in Cina una legislazione che disciplini in modo diretto l'IA, nonostante il paese si ponga tra i primi per i finanziamenti, la ricerca e l'utilizzazione di questo strumento [141].

Pur in assenza di una fonte specifica, esiste tuttavia un insieme di disposizioni ed indirizzi che indicano con sufficiente chiarezza il quadro di riferimento normativo sulla IA: dalla Cybersecurity Law (Csl) entrata in vigore il 1 giugno 2017, al Libro Bianco del National Industrial Information Security Development Center del gennaio 2021, che ha delineato le linee di sviluppo della IA per i prossimi decenni, fino alla recente Personal Information Protection Law del 20 aprile 2021 ed alla Data Security Law del 29 aprile 2021 [142]. E da ultimo, la circolare del Consiglio di Stato (il Governo) del 12 gennaio 2022 sugli sviluppi del 14esimo Piano Quinquennale e sul ruolo che in esso dovrà avere l'economia digitale, l'IA e la *quantum information* [143].

Il principale punto di riferimento in materia resta però il "New Generation AI Development Plan" (Aidp) adottato dal Consiglio di Stato il 20 luglio 2017, che indica le linee strategiche per fare della Cina entro il 2030 il paese più avanzato nel campo della IA [144]. È un documento che non ha una immediata valenza prescrittiva ma, nel modello cinese, condiziona fortemente il comportamento degli attori pubblici e privati del settore.

Il Piano è guidato da un Comitato di Consulenza Strategica istituito nel novembre 2017 e coordinato dal Ministero della Scienza e della Tecnologia. La strategia del governo pone in primo piano il settore privato e i governi locali, ed utilizza per la sua realizzazione strumenti di indirizzo piuttosto che normativi. Nel settore privato sono stati identificati dei Campioni Nazionali sostenuti dal governo per progetti specifici nel campo della IA: ad esempio Baidu per la guida autonoma, Alibaba per le smart cities, Tencent nel campo medico. In cambio del loro impegno le società godranno di contratti pubblici preferenziali, di accesso facilitato ai finanziamenti e di riserve di quote di mercato [145] . Analogo sistema di incentivi e agevolazione consente ai governi locali di realizzare iniziative decentrate.

Tre sono le aree indicate nell'Aidp come prioritarie. La prima è quella della competizione internazionale, ed è legata allo sviluppo militare di questa tecnologia

---

[141] Y. Luo, Z. Yu "An interview with Covington & Burling discussing Artificial Intelligence in China", in Lexology, 27 novembre 2020.

[142] G. Zou, H. Zhang, "China: a closer look at governamental and regulatory support of AI", in managingip.com, sponsored by Liu Shen IP, 3 marzo 2021.

[143] Agenzia Xinhua, www.gov.cn, 12 gennaio 2022.

[144] Nella traduzione di G. Webster, R. Creemers, P. Triolo, E. Kania in www.newamerica.org/cybersecurity-initiative/digichina/blog

[145] H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, L.Floridi, "The Chinese approach to AI: an analysis of policy, ethics and regulation" in AI & Society, 36 (2021) pp. 59-77.

duale: militare, appunto, e civile. Più che competere con gli Stati Uniti negli armamenti tradizionali, la Cina preferisce sviluppare una politica che le assicuri una decisa superiorità nell'IA [146].

Rilevante è poi il programma per l'uso dell'IA ai fini dello sviluppo economico: secondo una ricerca di PriceWaterhouseCooper la Cina potrebbe assicurarsi sfruttando il suo utilizzo un aumento del PIL del 26% per il 2030 [147].

La terza area di intervento, la governance sociale, è quella che suscita in occidente il maggior interesse. Qui il Piano richiama l'uso dell'IA nell'amministrazione della giustizia, suggerendo la sua utilizzazione in base al principio "giudizi simili in casi simili"[148] ; ne collega l'uso al cosiddetto Social Credit System, il sistema di crediti sociali che analizza i comportamenti individuali e collettivi attribuendo o togliendo punti in base a metri di giudizio stabiliti dalle autorità; ne suggerisce l'adozione per comprendere le dinamiche e la psicologia di gruppo o individuale (profiling); per migliorare i sistemi di apprendimento e di valutazione scolastici e lavorativi; per la security e la gestione delle tecniche di sorveglianza anti-criminali ed antiterroristiche, anche attraverso il discusso riconoscimento facciale [149]. Quest'ultimo ha visto negli ultimi anni, unitamente a quello del riconoscimento biometrico, un significativo sviluppo sottolineato da una recente decisione della Corte Suprema del Popolo che ne indirizza l'uso [150].

Nel Piano viene peraltro anche richiamata l'esigenza di definire un quadro di riferimento etico che possa condurre ad un codice di condotta per disciplinare i rapporti tra IA ed umani. Su questo punto va ricordato che, nel settembre 2021 il Ministero della Tecnologia ha emanato, attraverso la Commissione Nazionale di Guida per l'IA della Nuova Generazione", le "Norme etiche" per integrare questi principi nel *lifecycle* dell'IA.

È comunque, come ricordato, un impianto regolatore non vincolante, che presuppone da parte dei soggetti pubblici o privati un'adesione volontaria. Ma è una adesione volontaria "con caratteristiche cinesi", in quanto la mancata osservanza può portare a misure sanzionatorie di diverso tipo, come quelle previste ad esempio in caso di violazione dello "spirito delle Personal Information Security Specifications", informato alla tutela di quell'indefinito "significativo

---

[146] D. J. Blackout, "Technology determines tactics: the relationship between technology and doctrine in Chinese military thinking", in Journal of Stratford Studies, 34, 3, 2011, pp. 355-382

[147] PriceWaterhouseCooper, Sizing the Prize, 2017

[148] S. Yuan, "AI assisted sentencing speed up cases in judicial system", in China Daily,18 aprile 2019.

[149] Y. Zeng, E. Lu, Y. Sun, R. Tian "Responsible Facial Recognition and Beyond", Institute of Automation, Chinese Academy of Sciences, 2020

[150] "Provisions of the People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving the Processing of Personal Informations Using Facial Recognition Technology", luglio 2021

pubblico interesse", spesso alla base delle politiche di controllo cinesi nei più diversi campi[151].

Questo indirizzo è stato ribadito nel marzo 2021 nel corso delle "due sessioni", le riunioni parallele dell'Assemblea Nazionale del Popolo e della Conferenza Politica Consultiva del Popolo Cinese che, nel lanciare l'iniziativa Digital China, hanno con forza sottolineato l'esigenza che tutti gli attori in questo settore si conformino allo spesso richiamato, ma mai ben specificato, *vital public interest.*

Concludendo questa sommaria ricostruzione, possiamo dire che non esiste in Cina al momento una legislazione che disciplini in modo specifico il tema. Riferimenti possono rinvenirsi, come ricordato, nella Cybersecurity Law, nella Personal Information Protection Law[152,] nella Data Security Law e nell'Aidp. E in strumenti, come la definizione degli standard di produzione ed utilizzazione, che puntano ad "indirizzare" secondo le esigenze del governo le iniziative pubbliche e private [153]. Un approccio quindi non normativo, ma di forte discrezionalità amministrativa e sanzionatoria.

3. STATI UNITI

Anche negli Stati Uniti non esiste al momento una normativa organica sulla IA. Si confrontano qui con chiarezza le due linee contrapposte che caratterizzano in tutti i paesi il dibattito sulla sua disciplina: da una parte la prevalenza data nelle proposte di normazione, come in Europa, alla tutela dei diritti dell'individuo, delle diverse libertà, della stessa democrazia nei confronti di una tecnologia estremamente invasiva; dall'altra la dimensione militare e strategica di uno strumento "duale", militare e civile, che non può consentire ad una potenza globale come sono appunto gli USA di veder prevalere i propri avversari. Da qui il ruolo centrale che nell'attività di regolamentazione assume l'Esecutivo, consapevole più di altri della necessità di difendere il ruolo internazionale del paese.

---

[151] H. Yang, "China: the privacy, data protection and Cybersecurity law review", Edition 6, The Law Reviews, 2019

[152] Questa legge, come sopra detto, è stata approvata il 20 aprile 2021 ed è entrata in vigore il 1 novembre dello stesso anno. Punta tra le altre cose a disciplinare, riconoscendone peraltro la possibilità d'uso, il riconoscimento facciale e quello biometrico.

[153] Va a questo proposito ricordata l'adozione l'8 agosto 2021 da parte di diverse strutture pubbliche, a cominciare dal Ministero dell'Industria e della Tecnologia, di linee guida per la definizione di standard nazionali ed industriali e di indirizzi organizzativi nel campo della IA. Vedi Y. Luo e Z. Yu: "An interview with Covington & Burling discussing artificial intelligence in China", in Lexology, 5 gennaio 2022.

3.1 INIZIATIVE DI REGOLAMENTAZIONE

Nel 2016, sotto la presidenza Obama, escono due documenti sulla IA: uno del 12 ottobre [154] che si conclude con 23 raccomandazioni che sottolineano il ruolo che il governo deve avere per favorire il dibattito e il coordinamento tra i diversi attori pubblici e privati; il secondo [155], del giorno successivo, che all'interno del quadro indicato nel precedente documento propone un Piano con sei obiettivi strategici: stimolare gli investimenti a lungo termine; sviluppare modelli effettivi di collaborazione uomo-IA; affrontare le implicazioni etiche, legali e sociali; assicurare sicurezza e affidabilità; sviluppare un ambiente condiviso dei dati; misurare e valutare le tecnologie in questione attraverso *benchmarks* comuni. Nella tradizione americana, il governo mira a creare un "campo da gioco corretto".

Un indirizzo più rivolto alla dimensione strategica dell'uso dell'IA viene impresso dalla presidenza Trump. Il 27 giugno 2018 il sottosegretario alla difesa presenta un memorandum per l'istituzione di un Joint Artificial Intelligence Center, tra tutte le Forze Armate, per confrontarsi con gli altri soggetti governativi, con l'industria e con le istituzioni universitarie e di ricerca al fine di "adattare le tecnologie dell'IA alle missioni della Difesa". Poco tempo dopo, il bilancio per il 2019 identifica tali missioni: redigere un piano strategico; accelerare l'uso dell'IA al proprio interno; assicurare una governance per mantenere il vantaggio del paese su queste tecnologie, specialmente attraverso la formazione e il reclutamento dei talenti[156]. Di rilievo è l'istituzione nella stessa legge di una National Security Commission on AI, con il compito di avanzare proposte per incrementare la competitività del paese nel campo della IA, con una particolare attenzione alla necessità di tutelare il vantaggio tecnologico e la prevalenza militare americana nel confronto con gli altri stati: a questa commissione accenneremo più avanti[157].

L'anno successivo è ancora la Presidenza a rilanciare l'iniziativa con un memorandum ed un Ordine Esecutivo dell'11 febbraio 2019. Due indicazioni tra quelle che emergono da questi documenti ci sembrano particolarmente significative: la prima è la necessità di assicurare attraverso borse di studio ed altri incentivi lo sviluppo di talenti numericamente adeguati e competenti; la seconda è la definizione di un concreto piano d'azione per proteggere il paese contro "competitori stranieri e nazioni avversarie"[158]. A seguito dell'Ordine Esecutivo, nell'agosto 2019 il National Institute of Standard and Technology ha quindi adottato un piano che identifica nove aree di standard tecnici e non tecnici da

---

[154] Subcommittee on Machine Learning and Artificial Intelligence del National Science and Technology Office (NSTC): "Preparing for the future of Artificial Intelligence".
[155] "The National AI Research and Development Plan" dell'AI Task Force, un gruppo di lavoro sempre all'interno del NSTC
[156] John MacCaine National Defense Authorization Act for Fiscal Year 2019, sec. 238.
[157] Ibidem, sec. 1051.
[158] Executive Order 13859 dell'11 febbraio 2019, Federal Register, vol. 84,n. 31, e sec.7 e 8, lett. (a).

seguire, includendo tra i non tecnici quelli etici e sociali, la governance e la tutela della privacy [159].

Tralasciamo per brevità le ulteriori iniziative della Presidenza e della Camera dei Rappresentanti sul nostro tema (tra cui un aggiornamento del ricordato Piano del 2016), e veniamo agli sviluppi più recenti. Nel marzo 2020 viene presentato da alcuni parlamentari il National Artificial Intelligence Act of 2020, che entrerà poi in vigore dal 1° gennaio 2021 come emendamento al bilancio della Difesa[160]. È una proposta bipartisan, che vede uniti esecutivo e legislativo e le sue finalità costituiscono il più recente indirizzo in materia: assicurare la leadership americana nella ricerca e nello sviluppo dell'IA; fare degli Stati Uniti il paese guida nell'uso affidabile della tecnologia; sviluppare a tutti i livelli una forza di lavoro capace; coordinare la ricerca, lo sviluppo e l'utilizzo di questi sistemi tra le agenzie civili, il Dipartimento della Difesa e la Comunità dell'Intelligence. A questo fine viene istituito dal White House Office of Science and Technology un National Artificial Intelligence Initiative Office, come "punto di riferimento delle iniziative governative per i Dipartimenti e le Agenzie Federali, per l'industria, l'accademia, le organizzazioni no profit, le società professionali, i governi dei singoli stati e tutti gli altri soggetti che l'Initiative Office riterrà appropriati". Un ruolo rilevante sarà rivestito da un Advisory Committee, nominato dal governo, di cui faranno parte "istituzioni accademiche, imprese di diversi settori, associazioni no profit e della società civile, comprese quelle a tutela dei diritti civili e di quelli dei disabili, nonché strutture di ricerca federale espressione di diversità geografiche" [161]. L' 8 settembre 2021 il Segretario al Commercio ha annunciato la costituzione dell'Advisory Committe ora ricordato.

Per meglio chiarire il quadro che si va delineando negli Stati Uniti, è forse utile accennare anche ad un documento della Federal Trade Commission (FTC) del 19 aprile 2021, quando cioè erano già note le proposte europee che sarebbero state ufficializzate due giorni dopo [162]. L'invito della FTC agli sviluppatori e agli utenti dell'IA è quello di attenersi alla standard già presenti nella legislazione nordamericana per evitare pregiudizi fondati su razza, colore, religione, nazionalità, sesso, età o sul ricevere un soggetto aiuti dall'assistenza pubblica. E allora si fa riferimento al FTC Act del 1914, come modificato nel 2006 dal Safe Web Amendment; al Fair Credit Reporting Act del 1970 ed alle sue successive modificazioni; all'Equal Credit Opportunity Act del 1970 nella sua versione

---

[159] Y. Chae, "U.S. Regulation Guide: Legislative Overview and Practical Considerations", in The Journal of Robotics, Artificial Intelligence and Law, vol. 3, n. 1, gennaio-febbraio 2020. Ricordiamo, a proposito dell'attenzione data ai valori "umanocentrici", che gli USA hanno adottato nel maggio 2019 i "Principi sulla IA" dell'OECD che pongono tali valori al centro della proposta.

[160] National Defense Authorization Act for Fiscal Year 2021, Sect. 5102, nota come "Division E of the NDAA".

[161] Ibidem, sect, 5104 (b).

[162] E. Jillson, "Aiming for truth, fairness and equity in your company's use of AI", Federal Trade Commission, 19 aprile 2021, www.ftc.gov/news-events/blogs.

aggiornata. Si vuole suggerire ai produttori un approccio *ethical by design*, per adeguarsi agli standard contenuti nelle norme sopra richiamate, ritenute al momento sufficienti per eliminare i *bias* cui si è fatto riferimento. Un indirizzo ulteriore, per il momento, di contrarietà ad una disciplina generale.

Le reazioni del mondo industriale e di quello della ricerca a questo approccio normativo sono state al momento positive: le nuove indicazioni vengono infatti viste come un punto di riferimento che offre indirizzi senza imporre regole onerose che potrebbero mettere in difficolta lo sviluppo dell'IA [163]. Ed è qui evidente un atteggiamento di critica verso la nuova complessiva, più rigorosa normativa in corso di definizione presso l'Unione Europea. Un orientamento positivo favorito dal fatto che l'8 giugno 2021 l'Innovation and Competition Act ha stanziato per le ricerche nell'IA, nella robotica e nelle biotecnologie 80 miliardi di dollari [164].

3.2 LE CONCLUSIONI DELLA NATIONAL SECURITY COMMISSION ON AI

Come ricordato, la legge di bilancio della Difesa per il 2019 ha istituito una National Security Commission on AI (NSCAI) con il compito di fornire alla Presidenza e al Congresso raccomandazioni per "favorire lo sviluppo dell'intelligenza artificiale, dell'apprendimento automatico e delle tecnologie associate, al fine di affrontare in maniera complessiva i bisogni della sicurezza nazionale e della difesa degli Stati Uniti"[165]. Riteniamo utile descrivere brevemente le conclusioni della Commissione che costituiscono forse il più illuminante documento sulla strategia americana per l'IA.

È interessante notare come della Commissione facciano parte tra gli altri un ex CEO di Google, quelli di Oracle, di In-Q-Tech e di Amazon Web Services, un colonnello a riposo dei Marines già sottosegretario alla Difesa, il capo della divisione IA di Google, presidi e docenti di autorevoli facoltà scientifiche. Un insieme di esperti, per un totale di 15, che rappresentano l'avanguardia del mondo scientifico e produttivo nel campo della IA.

Le conclusioni sono articolate in due sezioni: difendere l'America nell'era della IA; vincere la sfida tecnologica. Nella prima si parla delle minacce emergenti; dei problemi attuali e futuri della Difesa; del ruolo della IA negli scenari di guerra; dei rischi dei sistemi d'arma autonomi; della relazione tra Intelligence e IA; del

[163] S. Overly, M. Heikkilä, "China wants to dominate AI. The US and Europe need each other to tame it", in Politico, 2 marzo 2021, p. 6
[164] H. M. Lyon, F. A. Waldman, "Artificial Intelligence and Automated Systems Legal Update", Gibson Dunn and Crutcher LLP, in Lexology, 11 agosto 2021.
[165] National Security Commission on Artificial Intelligence, Final Report, marzo 2021.

rapporto uomo-macchina. La seconda sezione è invece interamente dedicata alla sfida tecnologica, in primo luogo con la Cina.

Non sono conclusioni improntate all'ottimismo e riconoscono invece che "l'America non è preparata a difendersi o a competere nell'era del'IA. Questa la dura realtà che dobbiamo affrontare"[166] . E per "difendere l'America" va in primo luogo riconosciuto il ritardo della Difesa nell'acquisizione delle nuove tecnologie; nella precedenza ancora data a strutture "pesanti" come navi, aerei, mezzi meccanizzati e così via; nella carenza di una strategia efficace per reclutare i migliori talenti; in procedure di analisi, acquisizione, utilizzazione e controllo obsolete; nella necessità di superare una mentalità da "era industriale". Un ritardo che si manifesta anche nel campo dell'Intelligence.

Per quanto riguarda invece la sfida tecnologica, la seconda sezione vede il rischio di perdere nei prossimi anni il confronto con la Cina. Ciò a causa di un carente coordinamento all'interno del governo delle, peraltro, numerose iniziative sul tema; della mancanza di sinergie efficaci con il settore privato, l'accademia e i partner internazionali; dell'irrisolta questione dei "talenti" da formare e reclutare. E ancora viene sollevata la questione della proprietà intellettuale; quella degli standard e delle tecnologie associate all'IA; e, non ultima, la dipendenza americana da paesi esteri (per oltre il 90%) nell'acquisizione delle microchip.

Il sentimento complessivo è quindi di una grande preoccupazione: "dobbiamo adottare l'IA per cambiare il modo di difendere l'America". Da cui discende una non banale conseguenza organizzativa: "la competizione sull'IA reclama la leadership della Casa Bianca".

Non vengono ignorati gli aspetti etici e quelli della tutela delle libertà e dei diritti, ma "competitors are actively developing AI concepts and technology for military uses".

Sono conclusioni che stanno fortemente condizionando la discussione americana e le conseguenti decisioni sulla IA e che sembrano far prevalere al momento le preoccupazioni derivanti dal confronto globale, in primo luogo con la Cina. Preoccupazioni diverse, lo vedremo tra breve, da quelle che hanno spinto l'Unione Europea a concentrarsi invece su come tutelare i propri cittadini nell'uso di una tecnologia fortemente condizionante i diritti, le libertà e la stessa democrazia.

[166] Ibidem p.1

4. REGNO UNITO

La Brexit non potrà non avere un impatto sulla politica del Regno Unito nel campo della IA. Non si potranno infatti applicare, salvo futuri accordi o recepimenti, le norme in corso di definizione da parte dell'Unione. Va pertanto esaminato il quadro odierno della disciplina, in attesa di tali eventuali intese.

Una delle caratteristiche del Regno Unito è, nel campo della IA, il ruolo rilevante di affermate istituzioni scientifiche come l'Alan Turing Institute e l'Ada Lovelace Institute, che non solo offrono un supporto consulenziale ma sono i principali interlocutori del Governo nel settore [167].

Proprio al Turing ha fatto riferimento nel gennaio 2021 la *roadmap* del Consiglio del Regno Unito per l'IA (UK AI Council), un comitato di esperti di diversi settori, che ha presentato al governo un documento che si conclude con 16 raccomandazioni per una strategia nazionale [168]: sviluppare gli investimenti pubblici; rafforzare il ruolo dell'Alan Turing come centro di riferimento nazionale[169]; favorire la formazione interdisciplinare sulla IA; aumentare la fiducia dei cittadini verso strumenti che dovranno essere affidabili, trasparenti, accessibili e rispettosi dei diritti umani; costruire un sistema regolatorio e sanzionatorio adeguato; favorire la creazione di start up; promuovere la cooperazione internazionale; sviluppare le applicazioni legate alla salute; ma anche aumentare la sicurezza militare ed interna attraverso l'IA. Un programma, come si vede, non privo di ambizione.

A questo documento dobbiamo aggiungere le raccomandazioni nell'aprile 2021 del Centre for Data, Ethics and Innovation (Cdei) che ripropone la necessità di un modello affidabile capace di rassicurare i cittadini su questa nuova tecnologia [170]. Raccomandazioni aggiornate nel dicembre dello stesso anno, per sottolineare il ruolo che potrà avere l'IA in tre settori: il reclutamento e la gestione dei lavoratori, al fine di eliminare pratiche discriminatorie; i trasporti e la logistica, anche per aumentare l'efficienza energetica; il settore educativo [171].

Ancora, il 22 settembre 2021 è stato presentato in Parlamento dal Ministro per il Digitale un piano decennale (National AI Strategy) articolato in tre pilastri: investire a lungo termine; assicurare benefici per tutti i settori e le aree del paese; garantire

---

[167] Si veda da ultimo il rapporto dell'Ada Lovelace Institute "Regulate to innovate" sugli strumenti normativi da utilizzare, che dovrebbero partire da una chiara definizione di cosa si intende per sistemi di IA: v. Tom Whittaker e Liam Edwards, "Improving AI governance in the UK", Burges Salmon LLP, in Lexology 8 dicembre 2021.

[168] www.gov.uk/government/publications/ai-roadmap

[169] Va a questo proposito ricordato che nel gennaio 2022 il Turing è stato prescelto dal governo come "pilota" per un progetto per un nuovo centro di definizione degli standard per l'IA. V. Natalie Donovan: "New AI standards hub launched in UK", Slaughter and May, in Lexology, 14 gennaio 2022.

[170] V. Natalie Donovan, "New AI assurance roadmap published – is this the route to safe AI ?" Slaughter and May, in Lexology, 9 dicembre 2021.

[171] Sam Morrow e JP Buckley, "Artificial Intelligence Update", DWF LLP, 17 gennaio 2022.

una governance effettiva [172]. Nel Piano sono indicati alcuni obiettivi a medio termine: inserire l'IA tra le materie dei corsi di addestramento *(bootcamp)* organizzati dal Ministero dell'Educazione per settori con competenze tecniche specifiche su richiesta dagli imprenditori; predisporre linee guida per la raccolta e l'uso responsabile dei dati; aprire una consultazione pubblica (poi effettivamente tenutasi); mantenere un ruolo centrale alla proprietà intellettuale al fine di promuovere la creatività e l'innovazione [173].

Si delinea al momento un approccio diverso da quello dell'Unione Europea, anche su temi di interesse comune come appunto la stessa definizione della IA, la protezione dei dati, la trasparenza, i bias, i criteri che definiscono le responsabilità. Una normativa intersettoriale e non complessiva come quella dell'Unione, con codici di comportamento specifici per settore ed indirizzi *policy driven* che terranno conto delle peculiarità dei diversi campi di intervento [174]. Nel solco delle raccomandazioni della Camera dei Lords che già nel 2018 riteneva che "una legislazione specifica sulla IA sarebbe in questa fase inappropriata"[175].

Ed a proposito della Camera dei Lords è da notare la significativa corrispondenza di un suo documento del 18 dicembre 2020 con le preoccupate conclusioni della National Security Commission on AI americana da noi sopra riportate: nel suo rapporto sull'attività del Governo in questo campo, significativamente intitolato *"No room for complacency"*, vengono segnalati i ritardi, e le implicazioni strategiche dei ritardi stessi, che influenzano fortemente il quadro dei rapporti internazionali. Ancora una volta, nel mondo duale dell'Intelligenza Artificiale, il confronto globale con i paesi antagonisti si rivela centrale [176].

---

[172] https.publishing.service.gov.un/government/uploads/systems/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf

[173] È il tema trattato nel noto caso "Dabus", il ricorso avanzato nel 2018 da S. Thaler contro la decisione dell'Ufficio Britannico della Proprietà Intellettuale (Ukipo) di respingere la richiesta di due brevetti relativi a invenzioni asseritamente autonome frutto di un sistema di IA. In una alternanza di giudizi, la decisione ultima è al momento contraria al riconoscimento. V. Lisa Page, Thomas Kirby e Shaan Mehra "UK Court dismisses Dabus – an AI machine cannot be an inventor", Penningtons Manches Cooper LLP, in Lexology 14 dicembre 2021; Mike Pierides e Katherine B. O'Keefe, "AI and UK Intellectual Property Consultation: Copyright and Patents", Morgan, Lewis & Bockius LLP, in Lexology 14 gennaio 2022; Xin Hu Rasmussen e B. Vinti, "Update on artificial intelligence as a patent inventor", Proskauer Rose LLP, in Lexology, 18 gennaio 2022.

[174] J.McDonalds – Charles Russell Speechlys: "Regulating AI – the impact of two recent proposals: the UK's National AI Strayegy and the EU's proposed Artificial Intelligence Regulation", in Lexology, 27 ottobre 2021; e Tom Whittaker e Liam Edwards, "Improving AI governance in the Uk", cit.

[175] Select Committee on Artificial Intelligence, *AI in the United Kingdom: ready, willing and able?,* House of Lords paper, 100.

[176] Liason Committee on Artificial Intelligence, *AI in the UK: no room for complacency,* 18 dicembre 2020, session 2019-2020, HL papers 196.

5. RUSSIA

Nell'opinione degli analisti la Russia è considerata, nel campo dell'IA, un "outsider"[177] : termine che, in una interpretazione non benevola, potrebbe tradursi come "l'emarginata". Significando un ritardo rispetto ai suoi competitori strategici, in primo luogo Usa e Cina. Fin dal 2017 Vladimir Putin dichiarava tuttavia che "chi diverrà leader nell'intelligenza artificiale governerà il mondo". E nell'ottobre 2019 disciplinava con un suo decreto la "Strategia Nazionale della Federazione Russa per l'IA" [178]. Il documento parte con il riconoscimento dei consueti principi: tutela dei diritti umani, delle libertà fondamentali, della sicurezza, della trasparenza e così via. La strategia sembra fondarsi sulla prevalenza della ricerca e dello sviluppo dell'IA in campo economico e finanziario, nei servizi e nel settore sanitario e non menziona espressamente le applicazioni relative alla sicurezza e alla difesa: una omissione singolare visto lo sviluppo e l'applicazione della IA in Russia nei due settori ora citati.

Punto rilevante di questa strategia è la creazione di un database nazionale in cui far confluire i dati, con un accesso prioritario ai dati stessi a favore delle autorità pubbliche. Il ruolo prevalente che assume lo Stato in questa "Strategia" è rimarcato dal fatto che in anni recenti il 67% del finanziamento per ricerca e sviluppo dell'IA proviene in Russia dal bilancio dello Stato, mentre le risorse private incidono in Cina per il 79% e negli USA per il 77% [179].

L'attuazione della strategia, che si proietta fino al 2030, è delegata ad una serie di organizzazioni governative con un ruolo di coordinamento svolto dalla Commissione per lo sviluppo digitale posta sotto il controllo del Ministero dello Sviluppo Digitale, che ha il compito, tra l'altro, di coordinare i 13 progetti lanciati dal governo nel 2018 per la modernizzazione dell'economia russa.

È interessante notare come la Strategia Nazionale sia stata predisposta con il rilevante contributo della Sberbank, la maggiore banca russa posseduta per il 52% dallo Stato, che intende così divenire una "società per l'intelligenza artificiale", riservando a disposizione sua e del governo una mole immensa di dati [180].

Il fatto che la Strategia Nazionale non faccia esplicito riferimento agli usi militari non significa naturalmente che questi siano esclusi dal programma: lo dimostra tra l'altro il fatto che il decreto di Putin del 2019, nell'aumentare gli stanziamenti per la ricerca nella IA da 1,3 a 6,1 mld di dollari, non distingue tra usi civili e militari e

---

[177] J. Nocetti, "The outsider, Russia in the race for AI", in Russie. Nei. Reports, n. 34, Ifri, dicembre 2020.

[178] Decreto del Presidente della Federazione Russa sullo sviluppo dell'IA, 10 ottobre 2019, in http://publication.pravo.gov.ru

[179] "Principali indicatori per la scienza e la tecnologia", OECD, 2019.

[180] E. Tofaniuk, N. Uskov, "German Greg: Transforming Sberbank is a continuing process", in Forbes,Ru, 22 novembre 2019

appare credibile che tali fondi vadano anche ad incrementare quelli già previsti nel bilancio della difesa [181].

Siamo ancora una volta, quindi, davanti a un modello con una decisa prevalenza dello Stato sul piano della normazione, dell'indirizzo e del controllo. È un trend che, sia pure con significative differenze, sembra ormai consolidarsi in Cina, negli Stati Uniti e in Russia: al quale si contrappone, come ora vedremo, quello dell'Unione Europea.

6. UNA PRIMA COMPARAZIONE

Un elemento accomuna, sia pure tra marcate differenze, l'atteggiamento dei paesi che abbiamo fin ora esaminato. Ed è quello che non li vede al momento intenzionati a promuovere al loro interno una disciplina di carattere complessivo sulla IA. Con un approccio invece che potremmo definire *"regulation by design",* stabilendo standard per i produttori piuttosto che regole rigide il cui rispetto verrà verificato *ex post* [182].

Accanto a questo, va sottolineato il ruolo centrale che gli esecutivi si sono ritagliati per guidare il processo. Ed ancora, di estremo rilievo, l'attenzione in questi paesi per gli aspetti di politica globale e del confronto strategico, che pongono in primo piano le applicazioni dell'IA nel campo militare e della sicurezza: a scapito delle preoccupazioni che questo mezzo solleva per la tutela della privacy, per la difesa delle libertà personali, economiche e sociali, per il processo di partecipazione e decisione democratica.

Certamente su questo ultimo aspetto esistono differenze estremamente significative: non può certo, ad esempio, paragonarsi l'uso ossessivo di strumenti come il riconoscimento facciale e le tecniche predittive ai fini del controllo e della repressione sociale come avviene in Cina, al sistema americano che conserva strumenti politici, giuridici, di libertà di stampa ed economica che possono intervenire a difesa delle più volte richiamate libertà. Così come l'uso spregiudicato dell'IA con obiettivi di politica internazionale capaci di influenzare la competizione elettorale, ma anche la stabilità economica e sociale, di paesi avversari come sembra accadere in Russia è ben diverso dalle preoccupazioni per la sicurezza del Regno Unito[183].

---

[181] Su questo tema, P. Luzin, "Artificial Intelligence in the Russian Army", in Riddle, 19 marzo 2021.

[182] B. Docquir, R. Garcia del Poyo, X. Pican, T. Quinn: "Legislators worldwide move to adopt regulation by design", Osborne Clarke, in Lexology, 24 gennaio 2022

[183] Sul tema dell'uso dell'IA nella guerra informatica tra le nazioni, in particolare ma non solo da parte della Russia, si veda: "This is how they tell me the world ends", di Nicole Perlroth, Waterstones,

È però indubbio che nei paesi che abbiamo finora esaminato, tutti con risalenti tradizioni di prevalenza strategica nel confronto globale, le preoccupazioni che possiamo per semplicità definire “etiche” appaiono, sia pure lo ripetiamo con diversa intensità, recessive rispetto a quelle della difesa militare.

È un dilemma che la storia ha più di una volta proposto: si pensi ad esempio all’accanito confronto degli anni ’50 e ’60 del secolo scorso sull’uso dell’energia nucleare per scopi militari e strategici o per scopi pacifici, un confronto mai definitivamente risolto e che anzi viene riproposto in questi giorni anche con riferimento al solo uso industriale.

Torneremo su questo aspetto nelle conclusioni, dopo aver esaminato la legislazione in corso di definizione nell’Unione Europea che sembra differenziarsi da quella dei paesi fin ora esaminati per una maggiore sensibilità, lo ripetiamo nuovamente, al tema della tutela dei diritti e delle libertà davanti a un fenomeno potenzialmente capace di lederli.

Conclusioni:

- Non esiste al momento nei diversi paesi una regolamentazione complessiva dell’IA.
- Cina, USA, GB e Russia puntano su strumenti di indirizzo più che di normazione.
- L’aspetto militare e di controllo sociale dell’IA condiziona fortemente la politica di questi paesi

2021, che si sofferma sull’uso dei c.d. “*zero days”* attivati attraverso la IA nel confronto strategico e nelle lotte finanziarie, industriali e commerciali.

Capitolo VI

LA NORMATIVA NEL QUADRO DI RIFERIMENTO EUROPEO E IL CASO ITALIANO

di Antonio Malaschini

Sintesi: A differenza di altri Paesi, l'Unione Europea segue la strada di una proposta di regolazione complessiva dell'IA. Il principio ispiratore è quello di una IA "umano-centrica", che metta l'individuo e i suoi diritti, personali e sociali, al centro della normativa. Cercando quindi di eliminare i "rischi" che questo strumento può comportare per i singoli e per la società. Un orientamento seguito, sia pure con qualche ritardo, anche dall'Italia.

1. LE PREMESSE

Dopo la positiva esperienza del GDPR, in materia di protezione dei dati[184], era naturale che le istituzioni europee ponessero la loro attenzione sulla necessità di guidare il relativamente nuovo, e controverso, fenomeno dalla IA anche, lo vedremo tra breve, in una prospettiva non solo interna all'Unione.

Senza voler dettagliatamente ripercorrere l'iter che poi condurrà all'adozione da parte della Commissione Europea della sua proposta di Regolamento, non possiamo non indicare alcune tappe di questo percorso, a cominciare dall'aprile 2018 quando la Commissione, accogliendo l'invito del Consiglio Europeo, ipotizzò una strategia che ponesse "i cittadini al centro dello sviluppo della IA, una IA umanocentrica"[185]. Rimarrà questa l'ispirazione di tutta la successiva elaborazione degli organismi dell'Unione, differenziandosi come abbiamo più volte ricordato da quella dei paesi ad essa esterni: più mirata a rassicurare i propri cittadini e a tutelarne in via prioritaria i diritti e le libertà; meno preoccupata delle conseguenze a livello strategico di una politica di controllo nel campo della ricerca e dello sviluppo.

Un "Piano Coordinato" per l'IA venne quindi presentato già nel dicembre 2018, indicando la cornice all'interno della quale gli Stati membri avrebbero dovuto inserire le proprie iniziative nazionali [186]. L'idea ispiratrice era quella di favorire una tecnologia affidabile, che rassicurasse e preparasse la società all'impatto con la IA.

Non possiamo però non ricordare alcune delle decisioni successivamente assunte dalla Commissione: l'istituzione nell'aprile 2018 dell'High Level Expert Group (AI Hleg), con compiti di consulenza ed indirizzo; la AI Alliance del giugno dello stesso anno, un forum di discussione aperto alla società civile; l'AI Watch, del dicembre 2018, per monitorare lo sviluppo, l'applicazione è l'impatto dell'IA in

[184] Si tratta del General Data Protection Regulation (Regolamento n. 2016/679) del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
[185] Com (2018) 237 final
[186] Com (2018) 795 final

Europa. Il primo rapporto dell'AI Hleg, dell'aprile 2019, indicava quattro principi etici che avrebbero dovuto ispirare i sistemi di IA: rispetto per l'autonomia umana; prevenzione dei danni; correttezza; spiegabilità[187]. Il rapporto sarà successivamente aggiornato nel luglio del 2020, e costituirà la base per il Libro Bianco sull'IA che la Commissione pubblicherà il 19 febbraio 2020: "Un approccio europeo per l'eccellenza e la fiducia"[188]. Troveremo molte delle conclusioni del *White Paper* all'interno della proposta di Regolamento. Va poi ricordato un ulteriore documento della Commissione del 23 luglio 2020, l'*Inception Impact Assessment*, che fa il punto sulle iniziative proposte e sui loro prevedibili effetti [189]. Secondo questo documento, i benefici economici di un intervento pubblico nel settore potranno derivare solo da un aumento della fiducia dei cittadini nel sistema.

Lo spazio non ci consente di ricordare le iniziative sul tema assunte anche dalle altre istituzioni europee: Parlamento, Consiglio Europeo, Consiglio dell'Unione Europea. Vogliamo solo accennare a quello che, nel 2020, viene definito lo "October Framework on AI" del Parlamento, che indica una serie di principi etici che troveremo nella successiva proposta della Commissione: sicurezza, trasparenza e responsabilità; garanzia contro pregiudizi e discriminazioni; responsabilità sociale ed ambientale; privacy e sicurezza dei dati; identificazione di quegli high risks da disciplinare severamente, sui quali non potrà non essere determinante il controllo umano [190]. Nel "Framework" il Parlamento affronta anche il tema dell'uso militare dell'IA, ribadendo la necessità di un assoluto controllo umano dei sistemi militari che la utilizzino e richiedendo un bando per le armi letali autonome che facciano uso dell'IA [191].

Ma veniamo finalmente alla proposta di Regolamento della Commissione [192].

---

[187] European Commission, Science for Policy Report, *AI Watch. Artificial Intelligence in Public Services,* 2020.

[188] Com (2020) 65 final. Sul punto v. V. Litvinets, "A summary of the European Commission White Paper on AI", in medium.com, 9 giugno 2020.

[189] "Proposals for a legal act of the European Parliament and the Council laying down requirements on AI", 23 luglio 2020, Cnect. A. 2

[190] Risoluzioni del Parlamento Europeo del 20 ottobre 2020.

[191] G. Olivi, "The starting package", Dentons LLP, in Lexology, 23 novembre 2020.

[192] La proposta di Regolamento non esaurisce il quadro degli interventi della Commissione sul tema della IA. Contestualmente al Regolamento è stata infatti presentato un aggiornamento del Piano Coordinato sull'IA del 2018 prima ricordato; ed è in corso di definizione una nuova Direttiva Macchine per facilitare l'integrazione dei sistemi di IA nei macchinari, ed una sulla responsabilità dei produttori (*product liability*).

2. LA PROPOSTA DI REGOLAMENTAZIONE DELLA COMMISSIONE EUROPEA

Il 21 aprile 2021 la Commissione Europea presenta al Parlamento e al Consiglio una proposta per una normativa sulla IA[193]. Vediamone in breve i punti essenziali.

In premessa, coloro ai quali il Regolamento si rivolge sono i fornitori *(providers)* che collocano sul mercato o forniscono nell'Unione servizi di IA indipendentemente dal fatto che siano costituiti all'interno o all'esterno dell'Unione; gli utilizzatori *(users)* all'interno dell'Unione; fornitori o utilizzatori di sistemi IA in un paese terzo, qualora il prodotto del sistema sia utilizzato nell'Unione. Come con il GDPR, le norme hanno quindi un ambito di applicazione extraterritoriale.

Il Regolamento propone anche una definizione dei sistemi di IA che vuole essere tecnologicamente neutrale e tale da poter essere aggiornata in futuro attraverso una apposita delega prevista per la Commissione stessa[194].

2.1 IL CRITERIO DEI RISCHI

Il modello proposto dalla Commissione è basato sui "rischi": più alti i rischi, più severe le norme. A cominciare dalle pratiche che generano rischi talmente alti da essere addirittura proibite.

Sono pertanto proibite pratiche ritenute a rischio estremo quando utilizzino tecniche subliminali per distorcere il comportamento di un soggetto (*dark pattern*, come l'uso di suoni non percepibili per influenzarne i comportamenti); che sfruttino la vulnerabilità di una persona in relazione all'età o alla disabilità fisica o mentale; che siano utilizzate dalle autorità per valutare o giudicare un soggetto in base alle sue caratteristiche personali o sociali *(social scoring)*; sono poi vietate da parte della polizia pratiche di identificazione facciale in luoghi pubblici *(facial recognition)*, salvo che non si rendano necessarie, in uno spazio temporale limitato, per ricercare vittime di un crimine, per prevenire attentati o scoprire un soggetto accusato di gravi crimini.

Vi saranno invece rischi elevati *(high risks)* quando concorreranno due condizioni. La prima è che i sistemi di IA vengano usati come componenti di

---

[193] *Proposal for a Regulation of the European Parliament and of the Council: Laying Down Armonised Rules on AI* (*Artificial Intelligence Act*) *and Amending Certain Union Legislative Acts,* 21/4/2021, Com (2021) 206 final.

[194] L'articolo 3 e l'Allegato I definiscono l'IA come un software sviluppato con una o più tecniche o approcci (compreso apprendimento automatico e apprendimento profondo) che in relazione a obiettivi definiti dall'uomo può generare risultati diversi che per contenuti, capacità predittiva, raccomandazioni o decisioni possono influenzare l'ambiente con il quale interagiscono.

sicurezza di un prodotto disciplinato da precedenti direttive dell'Unione, come ad esempio macchinari, strumenti medici, giocattoli, mezzi personali di protezione; automobili, ascensori, aerei [195]. La seconda è che siano sistemi autosufficienti, che funzionano in maniera indipendente da altre unità *(stand alone)*, la cui componente di sicurezza sia sottoposta ad una valutazione preventiva di conformità da parte di un soggetto terzo in vista di un loro ingresso sul mercato.

Saranno poi considerate sempre a rischio elevato le pratiche capaci di influenzare l'esercizio dei diritti fondamentali indicati nell'Allegato III della proposta [196].

Per poter essere consentiti i sistemi a rischio elevato dovranno in primo luogo essere sottoposti ad una validazione di conformità; adottare poi modelli adeguati di gestione dei rischi; prevedere processi continui di stima e valutazione. Sarà sempre richiesta una documentazione tecnica aggiornata e verificabile e dovranno essere disegnati e sviluppati in maniera tale da assicurare trasparenza, *accountability* ed un effettivo e continuo controllo umano.

La validazione si basa essenzialmente su *un self-assessment*, ad eccezione dei sistemi per identificazione biometrica remota e dei network di infrastrutture pubbliche, per i quali è prevista la validazione di un soggetto terzo. Vedremo tra breve le sanzioni previste in caso di inadempienza. Al fine di facilitare la ricerca anche nei settori a rischio elevato, è consentita la creazione di "ambienti di prova regolati" *(sandboxes)* [197], pur nel rispetto delle norme di salvaguardia previste.

I sistemi non considerati come proibiti o a rischio elevato, in base alle caratteristiche ora richiamate, non sono sottoposti ad una disciplina diversa da quella esistente. La maggior parte dei sistemi oggi in uso in Europa, come ad esempio video games e filtri antispam, ricade in questa categoria. L'auspicio della Commissione è che vengano assunti dalle imprese codici di condotta su base volontaria che, adottando magari le stesse cautele previste per gli high risks, aumentino la fiducia dei cittadini in queste nuove tecnologie e, conseguentemente, la loro diffusione nel mercato. Un approccio che ricorda in parte quella *"regulation by design"* cui abbiamo prima accennato.

---

[195] V. Regolamento, Memorandum esplorativo, p. 13. E DLA Piper, "The World's First Artificial Intelligence Act, in Lexology, 30 aprile 2021.

[196] Ricordiamo tra tali diritti quelli relativi all'identificazione ed alla profilazione delle persone; alla gestione di infrastrutture critiche; all'educazione e alla formazione; al reclutamento e alla valutazione del personale; all'accesso ai servizi pubblici essenziali; all'ordine pubblico; all'emigrazione, all'asilo e al controllo delle frontiere; all'amministrazione della giustizia e al processo democratico.

[197] Davis Wright Tremain, in Lexology, 6 maggio 2021.

2.2 GOVERNANCE E SANZIONI

È istituito un Consiglio Europeo per l'Intelligenza Artificiale *(EuropeanAI Board)* per assistere la Commissione nel coordinamento delle politiche nazionali, anche al fine di una uniforme applicazione della normativa.

Il Consiglio sarà composto dai responsabili delle diverse autorità nazionali di vigilanza e dal Garante europeo della protezione dei dati, e sarà presieduto dalla Commissione stessa. A livello degli Stati membri sono previste autorità nazionali per garantire una applicazione conforme delle norme, ed una Autorità di Vigilanza con compiti di sorveglianza del mercato.

Per facilitare il lavoro della Commissione è istituito un *database* europeo per i "rischi elevati" derivanti dai sistemi autonomi *(stand alone)* al quale i providers saranno tenuti a registrare i sistemi stessi.

Le autorità nazionali di sorveglianza avranno un potere di controllo e di indagine sul rispetto degli obblighi e dei requisiti richiesti. Questo controllo *ex post* attribuisce ai soggetti controllanti il potere di intervenire, in particolare qualora i sistemi generino rischi inattesi.

Per quanto riguarda le sanzioni, la violazione delle norme sulle pratiche proibite o di quelle sui dati richiesti sono punite con una sanzione amministrativa fino a 30 milioni di euro o con una somma che può arrivare al 6% del totale annuo dei ricavi della società inadempiente. La violazione di norme diverse da quelle ora ricordate può portare invece ad una sanzione fino a 20 milioni di euro o al 4% dei ricavi della società. Il Garante Europeo per la protezione dei dati personali è autorizzato, in caso di inadempimento, ad elevare sanzioni nei riguardi delle istituzioni e delle agenzie dell'Unione responsabili.

Per quanto riguarda i successivi passaggi procedurali della proposta, conclusa la prevista consultazione pubblica, comincerà il consueto iter tra Parlamento e Consiglio dell'Unione Europea, e potrà qui essere utile raggiungere il consenso attraverso il "trilogo" con la Commissione [198]. Una volta terminato l'iter legislativo sarà lasciato alle aziende il tempo per adeguarsi ai nuovi requisiti e la nuova disciplina si inizierà ad applicare 24 mesi dopo l'entrata in vigore del Regolamento.

Spetterà nel frattempo agli Stati membri valutare le modifiche richieste dal Regolamento alla loro legislazione interna.

[198] Il "trilogo" è una procedura informale dell'Unione che vede coinvolti Parlamento, Consiglio e Commissione per favorire un accordo all'interno della procedura legislativa ordinaria.

2.3 LE PRIME OSSERVAZIONI CRITICHE

Le proposte della Commissione, come era prevedibile, hanno stimolato un dibattito all'interno del quale sono emerse diverse voci critiche. Al di là di quelle che fanno riferimento al linguaggio non preciso se non volutamente ambiguo delle norme proposte, le critiche avanzate possono con una qualche approssimazione dividersi in due categorie: quelle che ritengono che la nuova disciplina limiti l'esercizio di diversi diritti dei cittadini e dei principi di libertà e uguaglianza; e quelle che al contrario vedono in esse un ostacolo eccessivo alla ricerca e allo sviluppo della nuova tecnologia, determinando costi rilevanti per gli adeguamenti richiesti, particolarmente onerosi per le piccole e medie imprese [199].

E allora si sottolinea la difficoltà per le imprese, in base alle norme proposte, di bilanciare la richiesta di trasparenza con la tutela della libertà intellettuale (IP) e dei segreti commerciali [200]; l'oscurità del concetto di "spiegabilità", che dovrebbe rendere comprensibili processi e algoritmi la cui chiarezza sfugge però a volte agli stessi sviluppatori[201]; l'indeterminatezza dei criteri per distinguere tra rischi elevati e non; la difficoltà, ai fini della *accountability*, di identificare un responsabile finale; la centralità data ai *providers*, oggi superata da uno sviluppo tecnologico che sembra invece privilegiare i modelli *open source* rispetto ai tradizionali "fornitori"; il non aver preso in sufficiente considerazione come rischi elevati gli algoritmi *AI-informed* usati nei social media, nella ricerca, nelle vendite online e nelle applicazioni per dispositivi mobili e sistemi operativi [202].

Significative sono poi le critiche manifestate il 18 giugno 2021 in una *Joint Opinion*, sia pure non vincolante, dell'European Data Protection Board (Edpb), che richiede in primo luogo la proibizione di "ogni riconoscimento automatico della fisionomia umana in luoghi accessibili al pubblico, in qualsiasi contesto". Proponendo poi il divieto per i sistemi di IA che categorizzino i soggetti in relazione all'etnicità, al genere, all'orientamento politico o a quello sessuale. Ancora, segnalando il deficit di autonomia rispetto alla Commissione delle previste autorità di controllo, nonché il carente coordinamento tra la nuova disciplina per l'IA e quella in vigore per la protezione dei dati [203].

Va anche ricordato, in senso non sempre coincidente con le osservazioni da ultimo riportate, che il 2 novembre 2021 è stato presentato dal relatore Axel Voss un preoccupato e critico rapporto dello *Special Committee on AI in a Digital Age*

---

[199] *The EU's approach to AI,* International Institute for Strategic Studies, vol. 27, Comment, 24 settembre 2021

[200] V. Karen, L. Neumann, M. Tierney, H. Bonaccorsi, M. White, "European Commission proposed Regulation on AI", Lexology, 21 giugno 2021.

[201] G. Olivi, C. Bocchi, "Regulating AI in the European Union: top 10 issues for business to consider", Lexology, 1 luglio 2021.

[202] J. Buyers et al. "Debate continues over the pros e cons of regulating AI", Osborne Clarke, in Lexology 27 luglio 2021

[203] V. Horgan "Artificial Intelligence update", Bird & Bird LLP, in Lexology, 12 luglio 2021.

(AIDA) del Parlamento europeo che sottolinea il forte ritardo dell'Unione nella ricerca, nell'utilizzo e nella disciplina dell'IA, in particolare rispetto a Stati Uniti e Cina. Il rapporto, tra le altre cose, invita ad escludere dai principi limitativi della legislazione l'uso dell'IA legato alle attività militari e della sicurezza in un mondo in cui diversi sono i paesi che fanno di questo strumento un uso deciso nel campo del confronto globale e del controllo interno[204]. Dimostrandosi nel complesso meno ottimista rispetto alle valutazioni ed alle proposte della Commissione.

Da ultimo, il 29 novembre 2021 il Consiglio dell'Unione Europea ha presentato una bozza di compromesso *(Compromise Text)* su alcuni dei punti contestati. In particolare, per quanto riguarda la stessa definizione di "Intelligenza Artificiale", viene proposto un testo ritenuto più chiaro anche al fine di prevenire l'inclusione nella nuova disciplina di sistemi di software più tradizionali, normalmente non considerati di IA. Ancora, vengono suggerite modifiche che si ritiene meglio tutelino i diritti degli utenti finali precisando con maggiore chiarezza il concetto di *provider*; è esclusa la sicurezza nazionale dai fini della proposta disciplina, in quanto in base ai Trattati essa ricade nella esclusiva responsabilità degli Stati membri; viene alleggerita la disciplina per le attività legate a Ricerca e Sviluppo, al fine di favorire i processi di innovazione, escludendo i sistemi usati esclusivamente per la ricerca scientifica. Altre rilevanti proposte di modifica riguardano l'estensione del divieto di *social scoring* anche ai soggetti privati; la modifica all'Annesso III della proposta nella parte in cui si propone di considerare *high risks* anche i sistemi di IA che mettano in pericolo la tutela dell'ambiente; la previsione di un Annesso IV sulla documentazione di accompagnamento per rischi elevati, per meglio garantire l'adozione di misure di controllo umano sui sistemi di IA [205] .

Quanto ora detto sottolinea che, davanti ad una normativa che non solo ha un carattere di relativa novità ma pone problemi etici e sociali accanto a quelli scientifici, economici e produttivi, la strada dell'approccio globale seguita dall'Unione è senz'altro affascinante ma non priva di rilevanti e complessi problemi, che richiederanno un approccio realistico e non ideologico per rendere la nuova disciplina accettata da tutti: cittadini, imprese e Stati.

---

[204] EuropeanParliament, Special Committee on AI in a Digital Age, Draft Report, 21/112021 (2020/22661 (INI). Sugli aspetti dell'uso militare, v. n. 154, p. 32.

[205] William RM Long, Francesca Blythe e Subhalakashmi Kumar; "EU Council Publishes Changes to Artificial Intelligence Act Proposal", Sidley Austin LLP, in Lexology, 18 gennaio 2022; Adam Finlay e Catharine Walsh, "Council Publishes Proposed Amendments to Draft AI Regulation", McCann FitzGerald LLP, in Lexology, 23 dicembre 2021.

3. ITALIA

Come prima richiamato, nel 2018 il Piano Coordinato sull'IA della Commissione Europea prevedeva che gli Stati membri definissero una propria strategia nazionale. Il compito fu affidato in Italia al Ministero dello Sviluppo Economico, il cui titolare annunciò nel luglio 2018 una strategia italiana per l'AI e nominò quindi nel gennaio 2019 un gruppo di esperti.

Venne prodotto un documento all'interno del quale furono avanzate 82 proposte, sottoposto poi a consultazione pubblica nel settembre 2019 ed aggiornato nel febbraio 2020. Nel documento, mai ufficialmente reso noto, oltre all'esame dell'IA sotto il profilo scientifico, etico, industriale e sociale, veniva affrontato il tema della governance: dalla creazione di una cabina di regia, alla identificazione di un istituto nazionale per l'IA per coadiuvare e consigliare il governo su questi temi [206].

Le vicende legate al sorgere della pandemia da Covid-19 e i successivi sviluppi politici hanno probabilmente contribuito a porre in secondo piano la necessità di concludere l'iter di questo documento. Con il governo Draghi (13 febbraio 2021), per quanto di nostro interesse, vengono modificate le competenze dei diversi ministeri sul tema della IA, con il rafforzamento del Ministero per l'Innovazione Tecnologica che ha assorbito, unitamente al Ministero dell'Università e della Ricerca, diverse attribuzioni già di competenza del Ministero dello Sviluppo Economico, favorendo quindi la Costituzione di un Comitato Interministeriale per la Transizione Digitale tra le istituzioni ora richiamate.

Il 7 ottobre 2021 il gruppo di lavoro istituito nel luglio dello stesso anno dai Ministri interessati ha consegnato al Governo le sue raccomandazioni, successivamente approvate il 24 novembre dal Consiglio dei Ministri [207]. Nel documento vengono indicati sei obiettivi, undici priorità e tre aree di intervento, da realizzare entro il 2024.

Le tre aree di intervento sono: rafforzare le competenze e attrarre i talenti; aumentare i finanziamenti per la ricerca avanzata sulla IA; incentivare l'adozione dell'IA e delle sue applicazioni. Gli obiettivi si pongono il fine di rafforzare la ricerca di frontiera nell'IA; ridurre la frammentazione della ricerca stessa; sviluppare una IA antropocentrica e affidabile; aumentare l'innovazione fondata sulla IA e lo sviluppo della tecnologia; sviluppare la IA nel settore pubblico; creare, trattenere e attrarre ricercatori di IA.

I settori prioritari sono industria e manifatturiero; sistema educativo; agroalimentare; cultura e turismo; salute e benessere; ambiente, infrastrutture e

[206] "Proposte per una strategia italiana per l'Intelligenza Artificiale", in mise,gov.it/images/stories/documenti

[207] "Programma Strategico per l'Intelligenza Artificiale 2022-2024", in https://assets.innovazione.gov.it

reti; banche, finanza e assicurazioni; Pubblica Amministrazione; città, aree e comunità intelligenti; sicurezza nazionale; tecnologia dell'informazione.

Un punto che dovrebbe forse essere approfondito è quello della governance. Nel documento si fa riferimento ad un gruppo di lavoro permanente all'interno del Comitato Interministeriale "per dirigere, monitorare e valutare l'attuazione di questa strategia, le sue successive interazioni nonché coordinare tutte le azioni politiche sull'IA in futuro". Si afferma poi che "ciò comporta la possibilità di coinvolgere altri attori istituzionali, università e centri di ricerca nonché rappresentanti del settore privato".

È una soluzione senz'altro positiva nella parte in cui allarga il campo dei soggetti interessati. Ma lo sviluppo dell'IA nel nostro Paese richiede, in un quadro di concorrenza globale sempre più complesso, un punto di riferimento più forte ed autorevole. Come è stato recentemente fatto in materia di cybersecurity, con l'istituzione, accanto ad un Comitato Interministeriale con funzioni di consulenza, di una struttura operativa, l'Agenzia per la Cybersicurezza Nazionale, con al vertice un Direttore nominato dal Presidente del Consiglio di cui è il diretto referente. E andrebbe poi favorita, come nel Regno Unito con il Turing e l'Ada Lovelace Institute, l'identificazione di centri di ricerca avanzata con un ruolo non solo consulenziale ma anche di indirizzo.

A riprova dell'interesse che sembra finalmente accompagnare la riflessione in Italia sull'IA, va da ultimo positivamente ricordato come il Presidente del Consiglio Draghi nelle sue comunicazioni rese alle Camere il 20 ottobre 2021 ha indicato come obiettivo del Governo sull'IA "il promuovere la sperimentazione e, specialmente, renderne l'indirizzo più sicuro e trasparente. Allo stesso modo dobbiamo aumentare la fiducia dei cittadini per queste nuove soluzioni tecnologiche" [208].

[208] In questo quadro di work in progress va ricordato il documento di grande interesse, sia pur risalente al marzo 2018, dell'Agenzia per l'Italia Digitale (Agid), "L'intelligenza artificiale al servizio del cittadino". Ci si poneva qui l'obiettivo di analizzare l'impatto dell'IA nella società italiana, in particolare nella pubblica amministrazione.

4. CONCLUSIONI

Il filo ricostruttivo tra i diversi indirizzi normativi lo abbiamo già indicato. Da una parte i paesi, come l'Unione Europea, che pongono al centro dei propri interventi in materia di Intelligenza Artificiale una visione "umano-centrica", facendo da ciò derivare la necessità di tutelare in primo luogo i diritti, le libertà della persona, la stessa democrazia. Accettando anche il rischio di limiti alla ricerca, alla produzione ed all'utilizzazione dei sistemi di IA.

Dall'altra paesi che, anche in ragione di una loro passata o attuale dominanza globale, sono più attenti alle dimensioni strategiche di questo strumento. Non negano naturalmente la necessità di tutelare i diritti fondamentali in questione, ma rifiutano al momento un approccio complessivo come quello europeo preferendo interventi settoriali e di indirizzo piuttosto che di normazione generale, che non limitino la ricerca e l'uso sia in campo civile che militare.

Esistono naturalmente, lo abbiamo visto, differenze profonde tra gli indirizzi adottati in materia da Stati Uniti e Regno Unito rispetto a quelli di Cina e Russia. In questi ultimi paesi, oltre all'esigenza di non limitare la ricerca civile e militare, si assiste ad un uso deciso dell'IA ai fini della sicurezza e del controllo sociale interni. E ad una ritenuta utilizzazione nella *disruption* di sistemi produttivi, energetici, finanziari, di comunicazione ed elettorale di paesi avversari [209].

In questo complesso quadro appare in primo luogo necessaria, anche se non facile, la creazione di un tavolo internazionale di confronto in cui le preoccupazioni asseritamente comuni etiche e sociali, quelle della ricerca e della produzione possano confrontarsi. E in questo senso vanno alcune iniziative già adottate dalle Nazioni Unite, come *The UN's Secretary General's Strategy on New Technologies e il Systemwide Strategic Approach and Roadmap for Supporting Capacity Development on Artificial Intelligence* [210].

Non siamo così ingenui da ritenere che il problema dell'utilizzazione dell'IA, già complesso a livello dei singoli stati, possa così essere risolto: ma anche il solo inizio di un confronto internazionale sugli aspetti civili in questo campo sarebbe un fatto di per sé positivo. Per quelli militari, il tema di una sua regolamentazione ci riporta ai tentativi lunghi, faticosi e spesso infruttuosi che hanno accompagnato ed ancora accompagnano l'uso dell'energia atomica. Tentativi che hanno tuttavia al momento impedito l'olocausto atomico e che potrebbero dare frutti anche nel nostro campo.

Un'ultima annotazione prima di concludere. Abbiamo finora parlato di Stati, delle loro decisioni interne, del loro confronto strategico. Ci sono però altri rilevanti giocatori.

---

[209] V. Nota 42
[210] United Nations, 2018, in www.un.org/en/new technologies/pdf/

Tutti i paesi sopra ricordati, e naturalmente anche altri, sono debitori nel campo della ricerca e della utilizzazione dl'IA ad imprese le cui dimensioni sono superiori a quelle di singole, importanti nazioni. Un nuovo acronimo, MAAMA, unifica cinque società americane che dominano oggi il settore della tecnologia più avanzata: Microsoft, Apple, Amazon, Meta ed Alphabet. Lo stesso accade in Cina, con Huawei, J.D. Com, Alibaba, Tencent e China Mobile. Queste società, e naturalmente altre simili a loro anche in altri paesi, dominano il campo della ricerca e dell'uso degli strumenti fondati sulla Intelligenza Artificiale. Ad esempio, se i dati sono oggi le miniere della conoscenza e quindi dello sviluppo, siamo in questo campo di fronte ad una situazione di deciso oligopolio[211]. Non è questa la sede per esaminare in modo approfondito questo elemento. Ci limitiamo qui a segnalare un problema che ad esempio in Cina, con Alibaba ma non solo, ha indotto quel governo ad adottare dure misure di repressione e di indirizzo.

Non sono misure che riteniamo qui di per se auspicabili o possibili: ignorare questi players quando si parla di normazione sarebbe però non solo un errore ma un rischio, le cui conseguenze renderebbero forse velleitarie e inutili molte delle iniziative che i governi tentano oggi, a fatica, di adottare.

Conclusioni:

- L'Unione Europea è l'unico Paese a proporre una disciplina generale dell'IA.
- Questa disciplina si fonda sulla tutela dei diritti personali e collettivi degli individui e sulla eliminazione dei "rischi" connessi all'uso dell'IA.
- L'Italia segue, con qualche ritardo, l'indirizzo europeo

[211] Su questo tema, v. The Economist, 22 gennaio 2022.

Autori

- Enrico Prati, Professore Associato di Fisica Teorica della Materia, Università Statale di Milano
- Andrea Gilli, Senior Researcher, NATO Defense College
- Lucrezia Scaglioli, Research Assistant, NATO Defense College
- Enrico Savio, Chief Strategy and Market Intelligence Officer di Leonardo
- Enrico Comin, Strategic Planning Analyst di Leonardo
- Antonio Malaschini, Consigliere del Ministro dell'Economia e delle Finanze