DDL "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (1717)

Audizione del 28.3.2024

Visto il breve tempo a disposizione, mi concentrerò sul solo articolo 7, il quale mira ad attribuire all'Agenzia per la cybersicurezza nazionale la funzione di valorizzare l'intelligenza artificiale (IA) come risorsa per il rafforzamento della cybersicurezza nazionale.[1]

1. Si tratta, a mio avviso, di una disposizione importante, che sarebbe opportuno mantenere, anche se non necessariamente in questo disegno di legge. L'IA costituisce invero una risorsa cruciale in tema di cybersicurezza, le cui potenzialità vanno debitamente riconosciute ed esplorate. Essa, infatti, consente lo sviluppo di quelle che in ambito NATO vengono definite "autonomous cyber capabilities", ovvero la capacità di condurre operazioni cibernetiche senza che sia necessario un intervento umano in tempo reale.[2]

Nel contesto della protezione della cybersicurezza nazionale), tale tecnologia offre due fondamentali vantaggi. Da un lato, le *autonomous cyber capabilities* forniscono al sistema la capacità di neutralizzare autonomamente un attacco e di adattare le sue strategie difensive in base ai modelli di attacco osservati. Questo è particolarmente importante in un contesto in cui – e le notizie di questi giorni ne offrono un'ulteriore conferma – gli attacchi cibernetici sono sempre più sofisticati e mutevoli. Dall'altro lato, esse possono migliorare la robustezza dei sistemi, consentendo loro di continuare a funzionare in modo efficace anche sotto attacco, attraverso l'implementazione di meccanismi di auto-test e auto-riparazione.[3]

Sul punto, mi sembra opportuna una breve precisazione. Quando si tratta di utilizzare l'IA a fini di cybersicurezza, è importante distinguere tra cyberdifese passive e attive. Mentre le difese passive si limitano a garantire la protezione e la resistenza dei sistemi agli attacchi, le difese attive vanno oltre, consentendo ai sistemi contrattaccare quella che viene identificata come la fonte dell'attività ostile.[4]

---

[1] In realtà, alla luce della Strategia nazionale di cybersicurezza 2022-2026, è forse più corretto affermare che si tratterebbe di rendere esplicito l'affidamento di una funzione che l'Agenzia ha già inteso esercitare (v. ad es. pp. 22-23).

[2] R. Livoja, M. Naagel, A. Väljataga, Autonomous Cyber Capabilities under International Law, CCDCOE NATO, Tallinn, 2019.

[3] M. Taddeo, T. McCutcheon, L. Floridi, Trusting artificial intelligence in cybersecurity is a double-edged sword, Natura, 2019, p. 557 (i quali, tuttavia, mettono opportunamente in luce alcune vulnerabilità proprie di questi sistemi).

[4] M. Stroppa, Autonomous cyber capabilities and unilateral measures of self-help against malicious cyber operations, CCDCOE NATO, Tallinn, 2023.

I sistemi di IA impiegati ai soli fini di cyberdifesa *passiva* **non sono considerati sistemi ad alto-rischio** nella bozza definitiva del Regolamento sull'IA.[5] Essi, pertanto, non saranno soggetti agli obblighi ed ai controlli previsti dal Regolamento.

Il discorso è parzialmente diverso per il loro uso ai fini di cyberdifesa *attiva*. Pur non risultando al momento indicati nell'elenco di cui all'Allegato III del Regolamento ("Sistemi ad alto rischio di cui all'art. 6, co.2"), l'attitudine di questi sistemi ad incidere negativamente sulla sicurezza, sulla salute e sui diritti fondamentali ne rende plausibile una futura inclusione.

2. Un altro aspetto della formulazione dell'art. 7 su cui vale la pena soffermarsi brevemente riguarda l'impiego dell'aggettivo "etico" per definire gli usi dei sistemi di IA ai fini di cybersicurezza. Al riguardo, sono stati sollevati dubbi sull'opportunità di introdurre nozioni non giuridiche in un testo legislativo. Si tratta, in realtà, di un'evenienza piuttosto comune in tutti gli ordinamenti giuridici, incluso quello italiano, nei quali sono numerosi i principi e le clausole generali che fanno leva su valutazioni etiche (v., ad es., la clausola dell'ordine pubblico) e non mancano esempi in cui una disposizione di legge utilizza proprio l'aggettivo "etico" (ad es. l'art. 111bis del Testo unico bancario a proposito della finanza "etica").

È altresì vero, tuttavia, che in assenza di ulteriori specificazioni, il solo riferimento all'uso etico dell'IA può risultare piuttosto generico e, dunque, suscettibile di interpretazioni abusive. Sarebbe dunque opportuno chiarire questo aspetto inserendo un esplicito richiamo alle Linee Guida adottate nel quadro dell'Unione europea[6] o nell'ambito di altre organizzazioni internazionali di cui l'Italia è parte,[7] nonché agli atti legislativi che si occupano di "uso etico e corretto" dell'IA, in corso di approvazione sia a livello nazionale che dell'Unione europea, *in primis* il Regolamento sull'IA.[8]

3. Infine, e in considerazione del fatto che si sta intervenendo sulle funzioni dell'Agenzia, si potrebbe valutare la possibilità di includere un riferimento al contrasto alle minacce ibride in ambito cibernetico. Le minacce ibride rappresentano una sfida complessa e in continua evoluzione nel panorama della sicurezza internazionale. Si tratta di una varietà di condotte ostili, poste in essere da attori statali e non statali, che mirano a danneggiare i

---

[5] V. i paragrafi preambolari nn. 33° e 34 della bozza licenziata il 26 gennaio 2024 (reperibile sul sito: https://artificialintelligenceact.eu/).

[6] Gruppo di esperti ad alto livello sull'intelligenza artificiale, Orientamenti etici per un'IA affidabile, 8 aprile 2019.

[7] V. ad es. UNESCO, Recommendation on the Ethics of Artificial Intelligence, UN Doc. SHS/BIO/PI/2021/1, 23 novembre 2021.

[8] In questo modo, si dovrebbero forse lenire le preoccupazioni di chi ha sentito l'impellente necessità di metterci in guardia dal rischio che nella disposizione in parola possa annidarsi "una sorta di ideologia nazista".

paesi democratici sfruttandone le vulnerabilità, senza ricorrere all'uso della forza così come definita dal diritto internazionale.[9]

Tra queste condotte, oltre agli attacchi cibernetici, viene in rilievo la diffusione di disinformazione online, finalizzata a influenzare l'opinione pubblica e ad interferire con i processi democratici. Questo tipo di minaccia è particolarmente insidioso in quanto sfrutta le vulnerabilità della società digitale, come la dipendenza dai social media e l'accesso illimitato alle informazioni online, per diffondere narrazioni distorte e manipolative. Il risultato è un indebolimento della fiducia nelle istituzioni democratiche e la creazione di profonde spaccature all'interno della società. La Strategia nazionale adottata dall'Agenzia per la cybersicurezza nazionale ha già affrontato questo tema, riconoscendo l'importanza di "[c]ontrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida".[10] Appare tuttavia opportuno esplicitare questa competenza, attribuendo *per legge* all'Agenzia un ruolo specifico nel contrasto delle minacce ibride in ambito cibernetico.

Daniele Amoroso
Associato di diritto internazionale
Dipartimento di Giuriprudenza
Università degli studi di Cagliari
R.U. Progetto PRIN/PNRR "HYbrid threats versus Democratic Resilience: An analytical and practical toolkit" (HYDRA)

[9] Sulle "minacce ibride", v. Commissione europea, Quadro congiunto per contrastare le minacce ibride La risposta dell'Unione europea, JOIN/2016/018 final, 26 aprile 2016. V. inoltre le attività dell'European Centre of Excellence for Countering Hybrid Threats, istituito nell'ambito del Consiglio d'Europa, di cui l'Italia fa parte dal 2018 (https://www.hybridcoe.fi/).
[10] Strategia nazionale di cybersicurezza 2022-2026, p. 11.