Premessa

Vediamo, nell'esperienza quotidiana del digitale, dal web ai social ai sistemi di messaggistica, come stia aumentando sempre di più la nostra dipendenza dalla tecnologia. In parallelo stanno aumentando (anche se non tutti lo sanno) le minacce informatiche che causano ogni giorno danni significativi alle organizzazioni, ai governi e ai singoli individui. L'evoluzione del contesto in cui viviamo è descritta nella prima parte del libro, «Principi di cybersecurity e sviluppi dell'IA».

Oggi, l'integrazione dell'intelligenza artificiale (IA) con la cybersicurezza è una delle evoluzioni più promettenti. L'IA è già utilizzata in cybersecurity: per rilevare gli attacchi informatici, per una risposta più veloce ed efficace in caso di attacco e per prevenire danni considerevoli come quelli originati dai *ransomware*. L'IA ha però anche utilizzi malevoli, cui il responsabile della cybersecurity deve prestare molta attenzione: per esempio, una delle minacce emergenti più insidiose è quella dei *deep fake*, una tecnica che impiega l'IA generativa per creare identità sintetiche che riproducono, nella voce e nelle sembianze, persone reali.

Le capacità di cybersecurity possono essere ampiamente incrementate con l'ausilio dell'IA in svariati ambiti: dalla gestione degli incidenti alla *cyber threat intelligence*, dal rilevamento delle minacce all'individuazione e alla risoluzione di vulnerabilità. Anche per quanto riguarda la sensibilizzazione sui temi della sicurezza informatica e l'addestramento delle persone l'IA generativa è uno strumento di grande ausilio. L'introduzione dell'IA a fianco delle attività e delle misure di cybersecurity deve però avvenire tenendo conto di una serie di limiti e di sfide: in generale, come spesso avviene, non basterà dotarsi di queste tecnologie, bisognerà contestualizzare le soluzioni e calarle nel quotidiano e nel contesto specifico. Questi temi sono approfonditi nella se-

conda parte, «IA e GenAI, utilizzi avanzati delle tecnologie per rafforzare la cybersecurity».

Se l'IA si sta dimostrando un efficace ausilio per la cybersecurity, viceversa, l'utilizzo di sistemi IA in molteplici ambiti aziendali non può prescindere da un'attenta valutazione dei rischi e dall'impiego di specifiche metodologie e misure di sicurezza. Serve una profonda conoscenza della cybersecurity, dei suoi metodi e strumenti, oltre che delle norme da applicare, per garantire uno sviluppo e un utilizzo sicuro dell'intelligenza artificiale in molteplici campi, da quelli più critici (come può essere un sistema per prevenire le frodi) a quelli più banali (una chat che risponde su un sito di e-commerce alle domande dei clienti). Questi temi sono analizzati nella terza parte: «I rischi dell'IA nelle aziende e le strategie per prevenirli, rispondere, mitigare questi rischi».

Il futuro della cybersecurity sarà sempre più legato alle evoluzioni dell'IA: man mano che le minacce informatiche evolveranno, diventando più sofisticate, le soluzioni basate sull'IA potranno apprendere dall'esperienza e continuare a progredire. Obiettivo del libro, che si avvale dei contributi di numerosi esperti e responsabili aziendali della cybersecurity, è quello di approfondire come bilanciare intelligenza artificiale e cybersicurezza, perché questi due approcci metodologici e tecnologici possano convergere e rendere più sicuro il mondo digitale che ci aspetta.

Introduzione

di Bruno Frattasi
Prefetto e Direttore Generale dell'Agenzia per la cybersicurezza nazionale

Le trasformazioni globali degli ultimi decenni hanno favorito l'affermazione di uno «spazio nuovo», lo spazio virtuale, che incide sulla geopolitica e sulla stessa sicurezza degli Stati, delle istituzioni, delle imprese e dei cittadini.

All'interno di questo ecosistema digitale complesso si è già registrato il significativo impatto dell'intelligenza artificiale (di seguito anche IA) con le conseguenti nuove sfide per la cybersicurezza. Si tratta di sfide che richiedono risposte tanto sul piano della governance e delle policy quanto su quello tecnico e tecnologico senza mai tralasciare – come peraltro emerge già dal titolo di questo importante volume – il necessario bilanciamento tra l'impiego di sistemi di IA e le necessarie garanzie di sicurezza.

Sebbene in un contesto cyberdinamico come quello attuale non sia possibile delineare un *numerus clausus* delle sfide poste dai sistemi di IA, è interessante rilevare come nei diversi capitoli dell'opera gli autori si soffermino con elevato grado di approfondimento sulle principali questioni che tale fenomeno scientifico e tecnologico sta già ponendo.

Una delle principali sfide riguarda l'importanza di dotarsi di una governance e di standard condivisi. L'intelligenza artificiale sta ridisegnando, infatti, gli assetti geopolitici mondiali influenzando gli equilibri di potere e sicurezza tra gli Stati.

In questo contesto, è necessario delineare una strategia comune fondata sulla condivisione delle conoscenze al fine di garantire lo sviluppo «controllato» di questo importante strumento destinato a incidere profondamente sul nostro prossimo futuro. L'importanza di una governance e di standard condivisi in materia di IA – tema già affrontato nel corso del Summit di Hiroshima tenutosi in occasione del G7 del 2023 sotto la presidenza giapponese e successivamente ribadito durante la prima riunione

dell'AI Safety Summit tenutosi a Bletchley Park nel novembre 2023 – è stata anche al centro del G7 2024, sotto la presidenza italiana fino al 31 dicembre scorso, nel corso del quale è stato creato, su proposta dell'Italia, il gruppo di lavoro cybersicurezza chiamato a dar vita a un coordinamento «G7 inter-agenzia» per rafforzare l'azione collettiva tra le istituzioni responsabili per la cybersicurezza, in sinergia con l'*Ise-Shima Cyber Group*.

Al termine della seconda riunione dei gruppi di lavoro, che ACN ha avuto il privilegio di ospitare lo scorso 3 dicembre, i Paesi partecipanti hanno convenuto sulla necessità di rafforzare la collaborazione internazionale anche al fine di comprendere e condividere i rischi posti dall'IA e le conseguenti misure volte a garantirne un uso consapevole e sicuro, riconoscendo l'importanza del miglioramento dei controlli di sicurezza dei sistemi di IA, nonché dell'armonizzazione degli strumenti per identificare e mitigare le vulnerabilità degli stessi.

La seconda grande sfida posta dall'intelligenza artificiale concerne, invece, lo sfruttamento delle opportunità che ne derivano e, al contempo, la prevenzione e il contrasto della minaccia cibernetica determinata da un uso malevolo dei sistemi di IA. L'uso ostile dell'IA costituisce, infatti, la più seria e attuale minaccia cui possa risultare esposta la superficie digitale di un Paese.

Il binomio IA-cybersicurezza, esaminato nei diversi contributi che compongono il volume, fa emergere la necessità di proteggere attraverso misure tecniche e procedure di cybersecurity i sistemi basati sullo sfruttamento dell'intelligenza artificiale innalzando, al contempo, il livello di resilienza nello spazio cibernetico.

In questo contesto cyberdinamico si pone, con maggiore evidenza, la necessità di sfruttare l'IA e le nuove capacità esponenziali di calcolo offerte dalla tecnologia *High Performance Computing* (HPC) al fine di prevenire e contrastare la minaccia cibernetica, favorendo, altresì, lo sviluppo di controlli, di strumenti di analisi e metodologie di test condivisi da parte delle agenzie di cybersicurezza dei Paesi G7 e dei Paesi *like-minded*.

È questa la direzione da seguire affinché l'IA superi quel livello di «astrazione» trovando applicazione in una molteplicità di casi d'uso e in settori strategici per lo sviluppo del Paese come

la sanità, il lavoro, la giustizia, le pubbliche amministrazioni e altre importanti aree nelle quali garantire un utilizzo dei sistemi di IA basato su criteri che assicurino una corretta gestione dei rischi connessi.

Dinanzi al fenomeno in argomento è determinante, altresì, individuare criteri regolatori idonei a equilibrare il rapporto tra le opportunità offerte dalle nuove tecnologie e i rischi inevitabilmente legati al loro uso improprio o dannoso, avendo chiaro che in gioco c'è il futuro dell'ecosistema digitale.

È questa la ratio del Disegno di legge (AS 1146), recante Disposizioni e delega al Governo in materia di intelligenza artificiale, al momento all'esame del Senato della Repubblica, che in linea con il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, in vigore dallo scorso mese di agosto, prevede un sistema di principi, governance e misure specifiche in tema di IA che consentano ai cittadini e alle imprese la possibilità di cogliere le opportunità che tali tecnologie possono offrire in modo corretto, trasparente e responsabile, sempre in una dimensione antropocentrica che salvaguardi il rispetto dell'autonomia e del potere decisionale dell'uomo.

Va considerato, inoltre, che questa tecnologia dirompente può incrementare sensibilmente il livello non solo quantitativo bensì anche qualitativo della minaccia cyber, aumentandone il grado di offensività, il che implica che l'attività di prevenzione svolta sulla sicurezza dei sistemi rappresenti un'istanza ancora più avvertita.

Una delle minacce più temute – anche in considerazione del fatto che l'utilizzo malevolo di sistemi di IA aumenta sensibilmente il rischio di derive criminali – è rappresentata dal *ransomware*, duplicemente insidiosa perché compromette gravemente la stabilità di due fondamentali pilastri di un sistema complesso: la sicurezza dei dati, la cui esfiltrazione e crittazione è funzionale al ricatto estorsivo, e la sicurezza economica, che ne viene incrinata in misura notevole[1].

---

[1] Per tali evidenti ragioni, il fenomeno del *ransomware* è oggetto di una forte attenzione anche sul piano nazionale dove, con la Legge 28 giugno 2024, n. 90, si è realizzato un intervento legislativo di rafforzamento della risposta

Possiamo, dunque, affermare che la sfida più grande che l'intelligenza artificiale pone è quella di mettere a frutto misure e procedure di sviluppo e controllo che garantiscano sistemi e modelli di IA sicuri e affidabili, in aderenza a un principio di sicurezza *by design* che deve accompagnare il loro intero ciclo di vita.

È appunto per le succitate ragioni che reputo il Regolamento europeo (AI Act) un caposaldo dello sviluppo dei sistemi di IA, perché è in quella trama normativa che sono definiti i confini, non oltrepassabili, dell'*uso intelligente* – cioè non distruttivo, né autodistruttivo, e perciò eticamente accettabile da parte dell'intero consorzio umano – dell'intelligenza artificiale. Intendo riferirmi a quel sistema di regole, efficacemente denominato *guardrail dell'IA*, che stabilisce limiti e confini di un corretto sentiero da percorrere.

Anche questo delicato e nevralgico aspetto viene giustamente trattato nell'ambito dell'esauriente panoramica che offre questo volume. Ho definito tale aspetto in questi termini perché è riguardo a esso che si confrontano – anche all'interno del mondo occidentale – visioni diverse, le quali rischiano di rivelarsi troppo distanti se non opposte qualora, ed è questo il punto più spinoso, prendano il sopravvento le tentazioni, già peraltro ampiamente paventate, di trasformare l'IA in una tecnologia di controllo e di dominio.

L'Unione europea si è affermata nell'agone mondiale come la prima potenza che ha posto delle regole, e quindi dei vincoli, all'avvento di questo formidabile strumento di progresso. Ciò tuttavia non ne fa, irrimediabilmente, una «fabbrica di regole», relegandola a un ruolo solo marginale nella ricerca e nella produzione industriale.

Come sostenuto da voci autorevoli, l'Europa può aggregare forze e capacità importanti grazie alle quali incrementare gli investimenti e così accrescere la sua statura competitiva nell'high-

---

punitiva che ha modificato il delitto di estorsione di cui all'art. 629 c.p., introducendo al comma 3 una nuova fattispecie di reato, la cosiddetta estorsione informatica, con un severo inasprimento di pena.

tech, in generale, come anche nello sviluppo dell'IA, in particolare.

Nello scenario globale l'Europa, come soggetto politico, non sembra avere altra via che quella di proporsi davvero come un'entità unitaria. Ed è in questa chiave che mi permetto di richiamare il progetto *IT4LIA AI Factory* che ha visto coinvolti insieme all'Agenzia per la Cybersicurezza Nazionale, il Ministero dell'Università e della Ricerca, la Regione Emilia-Romagna, il Consorzio Cineca, l'Istituto Nazionale di Fisica Nucleare (INFN), l'Agenzia Italia Meteo, la Fondazione per l'IA, la Fondazione Bruno Kessler e il Centro Nazionale di Ricerche in HPC Big data and Quantum Computing (ICSC).

Il cuore del progetto – coordinato dall'Italia in collaborazione con Austria e Slovenia – sarà un supercomputer all'avanguardia, progettato per l'IA e con sede presso il Tecnopolo di Bologna, già leader europeo in super computing, big data e calcolo quantistico. Questa infrastruttura avanzata sarà una delle prime al mondo e leader in Europa per capacità di elaborazione in ambito IA.

Con la selezione del progetto *IT4LIA AI Factory* da parte della Commissione europea, il nostro Paese si posiziona al centro dello sviluppo dell'intelligenza artificiale in Europa. Si tratta di una grande infrastruttura che sarà al servizio della Pubblica Amministrazione, delle istituzioni, delle Università e del mondo della ricerca nonché delle startup, delle Pmi e dell'intero settore produttivo italiano, favorendo una crescita più competitiva e sostenibile.