INGEGNERIA E CYBER SECURITY TRA ETICA E INNOVAZIONE: FRONTIERE

TECNOLOGIE CRITICHE E INTELLIGENZA ARTIFICIALE: IL PUNTO DI VISTA DI LUCA MANUELLI SULL'INNOVAZIONE E IL FUTURO DELL'INDUSTRIA

di Mafalda Meduri,
giornalista, capo redattore di A&B

Abbiamo incontrato il prof. Luca Manuelli, a margine del meeting "Ruolo dell'Ingegneria nello Sviluppo delle Tecnologie Critiche" tenutosi a Genova a dicembre. Tra i relatori dell'evento, con lui abbiamo approfondito i temi toccati dal suo intervento e approfondito il ruolo dell'I.A. nella trasformazione industriale e nei processi decisionali, con un focus su tre aspetti centrali: gli impatti sull'automazione industriale, l'etica delle decisioni autonome e la trasformazione dei servizi

Il 3 dicembre 2024, il Palazzo della Borsa di Genova ha ospitato l'evento "Dialoghi sull'Ingegneria. Ruolo dell'Ingegneria nello Sviluppo delle Tecnologie Critiche", un momento cruciale per riflettere sul contributo della professione ingegneristica nell'affrontare le sfide dell'era digitale. L'incontro mirava a informare e sensibilizzare stakeholder e società civile sui rischi e le opportunità legati alle tecnologie critiche, con un'attenzione particolare ai temi di sicurezza, etica e sostenibilità.

In un contesto di rapida evoluzione tecnologica, l'evento si è sviluppato attraverso tre panel interconnessi, dedicati a *cyber security*, Intelligenza Artificiale (I.A.) e Tecnologie Biomedicali. Nel panel sull'Intelligenza Artificiale, è intervenuto il prof. Luca Manuelli, direttore dell'Osservatorio Gailih (Generative artificial intelligence learning and innovation hub) promosso da Unimarconi. Questi ha esplorato il ruolo dell'I.A. nella trasformazione industriale e nei processi decisionali, con un focus su tre aspetti centrali: gli impatti sull'automazione industriale, l'etica delle decisioni autonome e la trasformazione dei servizi. L'abbiamo incontrato al termine dell'evento.

Qual è stata la sua impressione generale sull'evento "Dialoghi sull'ingegneria" a Genova? In particolare, come considera il contributo dei panel dedicati a *cyber security*, Intelligenza Artificiale e Biomedicale nel delineare le prospettive future delle tecnologie critiche?

È stato molto molto interessante. Tra l'altro, due settimane prima avevo organizzato sempre a Genova un evento su Intelligenza artificiale Blue economy, al quale avevano preso parte alcune importanti realtà del territorio come Fincantieri, il RINA, la stessa Università di Genova e delle presenze istituzionali importanti.

"Dialoghi sull'Ingegneria" ha confermato che in questo momento c'è una fortissima attenzione rispetto al tema dell'Intelligenza artificiale. E la Liguria – che conosco bene perché ci ho vissuto dieci anni prima di tornare a Roma – da circa due anni si conferma una realtà che è molto attenta all'innovazione e cerca di intercettare le opportunità che questo tipo di innovazione può portare sul territorio. Nel caso specifico dei tre panel, facevo parte di quello relativo all'Intelligenza artificiale.

Secondo me, sono stati ben articolati perché hanno creato dei collegamenti logici e di approfondimento per le evidenti aree di sovrapposizione di sinergia che ci sono fra i diversi temi, in particolare, ovviamente sulla *cyber security*.

A riguardo, ho dato un piccolo contributo alla creazione del Competence Center ligure START 4.0. E la visione del competence Center era quella di un approccio olistico alla sicurezza quindi una declinazione d'insieme di *cyber security*, sicurezza fisica e sicurezza delle persone sul lavoro.

Ora lo START 4.0 è nato all'indomani del crollo del ponte Morandi per cui c'è stata ovviamente anche una reazione di natura emotiva che ha portato a questo tipo di missione, ma io credo che questo tema, ovvero il collegamento fra i diversi tipi di sicurezza, sia sempre fondamentale.

Per quanto riguarda l'Intelligenza artificiale, la *cyber security* costituisce minaccia e opportunità perché tutto ciò che in questo momento, in particolar modo l'Intelligenza artificiale generativa, può essere facilitato tramite un'interfaccia naturale fra uomo e macchina, vale a maggior ragione per gli hacker.

Mentre prima gli hacker dovevano avere un alto livello di competenza e di preparazione per poter essere pericolosi. Molto rilevante adesso è la barriera all'ingresso.

L'Intelligenza artificiale può garantire un supporto al rafforzamento dei sistemi di difesa e quindi un'integrità. Soprattutto, per quanto riguarda gli aspetti dei data center, l'integrità dei dati dei model che sono gli asset strategici, però, mi permetto di dire che vale sempre lo stesso problema.

L'80% degli incidenti di *cyber security* avvengono a causa di un comportamento umano che non è coerente con le policy o con le regole o con le norme. **Perciò è fondamentale che ci sia informazione e formazione**. Formazione delle competenze della *cyber security* a tutti i livelli, non solo per gli operatori ma anche per gli utenti.

L'ultimo tema, inerente alla tecnologia, è quello più stimolante. I potenziali ambiti applicativi dell'Intelligenza artificiale e i possibili progressi che in campo medico sanitario può apportare sono notevoli. E non solo con l'Intelligenza artificiale ma anche con le varie tecnologie digitali di cui disponiamo. Ormai, allo stato dell'arte, siamo pronti per valutare una nuova fase che dovrà poi avere delle importanti evoluzioni sotto tutti i profili (organizzativi, normativi), perché mai come in questo momento la differenza la farà chi è in grado di utilizzare l'Intelligenza artificiale rispetto a chi non è in grado.

In che modo la programmazione umana influisce sulle potenzialità e sull'efficacia dell'Intelligenza artificiale?

È il tema più generale del rapporto uomo-macchina ma soprattutto della visione antropocentrica dell'Intelligenza artificiale che in questo momento si sta portando avanti a diversi livelli sia a livello politico sia a livello etico. Per quanto riguarda il ruolo che le diverse organizzazioni devono garantire, è chiaro che è uno dei rischi grossi che l'Europa sta correndo, non solo l'Italia come parte dell'Europa.

La partita dell'Intelligenza artificiale e del rapporto equilibrato fra uomo e macchina non va gestito tramite norme che comunque devono in qualche maniera definire o confermare che ci sono dei paletti o, come li chiamano, dei guardrail, cioè dei principi fondamentali che devono essere garantiti nell'applicazione di queste tecnologie.

Ma è fondamentale investire e accrescere le capacità di sviluppare e di applicare questa tecnologia che a differenza delle altre tecnologie digitali ha un forte contenuto tecnico ma ha anche un forte impatto e delle implicazioni multidisciplinari che altre tecnologie non avevano mai avuto in termini di applicazione.

Quindi, il rischio di sovra regolamentazione e di una continua rincorsa perché la tecnologia cambia tutti i giorni e ovviamente le norme devono essere costantemente adeguate. Il rischio è grosso e rischia poi di diventare un gap competitivo proprio per l'Europa.

Come se ne esce? Stilando un Regolamento che contenga dei principi fondamentali, da applicare, ma soprattutto individuando una strategia e io auspico che l'Italia sia in grado di coinvolgere anche gli altri Paesi leader dell'U.E. nello sviluppare una strategia che permetta di avere un posizionamento competitivo di alcuni campioni europei, perché altrimenti noi subiremo l'ondata lunga dei grandi player americani e, con ogni probabilità, di quelli cinesi di cui sappiamo ancora poco.

Insomma, l'Europa deve essere in grado di avere una visione di sistema e di definire delle linee guida strategiche e dei programmi anche di collaborazione a livello internazionale per avere capacità e competenze adeguate nei vari settori, quelli dello sviluppo delle varie componenti tecnologiche di Intelligenza artificiale e poi soprattutto nell'ambito applicativo. Ovvero, l'impatto sul mondo del lavoro dell'Intelligenza artificiale.

Fondamentalmente avrà due possibili effetti: il primo, la creazione di nuovi posti di lavoro come in parte si sta già vedendo. Il secondo, viceversa, è l'automazione di attività più ripetitive che sarà più efficiente svolgere utilizzando l'Intelligenza artificiale rispetto all'uomo. Di conseguenza, viene fuori il tema se l'Intelligenza artificiale toglierà lavoro all'uomo. È un tema mal posto, secondo me.

La differenza la faranno quei lavori, quelle professioni dove l'uomo è in grado di avvalersi delle intelligenze artificiali, quindi di aumentare le sue capacità. Ovviamente ci sono dei grossi rischi.

Quali sono, secondo lei, i principali fattori che determinano il successo o i limiti di un sistema di IA?

È evidente che in questo momento la situazione è in parte supportata dalla comunicazione dal fenomeno mass mediatico dell'Intelligenza artificiale. Oggi, riguarda prevalentemente i grandi big e i grandi player tecnologici quindi tutti coloro che a partire da OpenAI – che ha inventato chat GPT – a tutte le grandi big tech come Meta, Google, Microsoft, Amazon e Apple.

Con quest'ultima che non credeva molto, secondo me, al fatto che ci sarebbe stata questa drammatica accelerazione e quindi adesso sta correndo ai ripari perché poi Apple è fra i big Tech, quello che ha fatto della sicurezza informatica il suo cavallo di battaglia.

Cioè dei sistemi chiusi e quindi, in teoria, ha un gap competitivo perché non è in grado di integrare soluzioni tecnologiche di terze parti. E deve sviluppare necessariamente all'interno. In buona sostanza, in questo momento c'è un fortissimo investimento da parte dei grandi player tecnologici. Dal lato della domanda, quello che noi esaminiamo come Osservatorio – anche sulla base delle esperienze operative di molti dei nostri membri – è, invece, un forte interesse e una grande attenzione a capire i vantaggi di dove può essere applicata l'intelligenza artificiale. C'è sicuramente una visione complessiva, quindi la volontà (potenzialmente) di applicarla sia ai processi interni che a maggior ragione verso quelli che riguardano prodotti o servizi da offrire al mercato.

Ma una delle variabili fondamentali è quella della fattibilità economica, ovvero dei benefici che possono essere generati a fronte dei costi che peraltro in questo momento sono ancora molto elevati, quindi, arrivare a un livello tale da permettere effettivamente un'applicazione estesa in tutto il mondo delle aziende.

Alcuni settori sono più avanti degli altri come il settore finanziario e, se vogliamo, anche il settore della comunicazione ma per esempio nella manifattura abbiamo dei dati – e non solo in Italia – che registrano un notevole ritardo nella prova di queste tecnologie ed essendo evidente che, alla fine, domanda e offerta si dovranno incontrare bisognerà individuare anche delle applicazioni che abbiano dei costi accessibili soprattutto per le piccole e medie imprese che anche culturalmente sono un po' lontane da questo mondo. In questo senso, diventerà molto importante la capacità di dare immediati benefici sia per la componente di ottimizzazione di efficientamento e di riduzione dei costi, sia per la componente di creatività di generazione dell'Intelligenza artificiale.

Queste nuove tecnologie sono in grado di produrre dei contenuti nuovi, originali, veramente impressionanti. Ogni giorno sta uscendo una nuova tecnologia. E quello che è molto importante è capire il costo di accesso e chi potrà accedere a queste tecnologie.

L'ultimo punto è una specie di mantra: le competenze. Credo che chiunque voglia essere un player perché sviluppa questa tecnologia o voglia utilizzarla al meglio, debba rapidamente capire il tipo di impatto sull'organizzazione, sui processi e soprattutto sulle competenze.

Quindi anche il motivo per cui noi nel nostro documento strategico *Formare il futuro* abbiamo suggerito al Governo di prevedere delle misure per incentivare l'adozione di Intelligenza Artificiale anche nella componente della formazione. Avendo lavorato durante Industria 4.0, come Chief Digital Officer di Ansaldo Energia, abbiamo realizzato la prima fabbrica intelligente in Italia potendo contare sulla gran parte di contributi indirizzati sull'acquisto di tecnologie di software, ma non sufficienti per supportare la formazione che è stata autofinanziata.

A mio avviso, questa volta bisogna un po' capovolgere il paradigma cioè partire dal presupposto che l'Intelligenza Artificiale e la tecnologia sono importanti, ma lo sono ancora di più le competenze. Quindi, se si vuole dare un supporto allo sviluppo dell'applicazione di queste tecnologie nel mondo economico, nell'industria e nella manifattura in particolare bisognerà privilegiare lo sviluppo delle competenze.

Luca Luigi Manuelli, Direttore dell'Osservatorio sull'I.A. Generativa, Professore presso Università degli Studi "Guglielmo Marconi" e C-Level Executive, Innovation Manager, Digital and Energy Transitions

Come possono queste tecnologie contribuire alla sicurezza e all'affidabilità delle infrastrutture critiche?

È un tema che ho affrontato in occasione della creazione di START 4.0 ma ancora prima, diversi anni fa, in Finmeccanica (oggi Leonardo) ero il responsabile della *cyber security*, tecnologia sviluppata prioritariamente nel mondo della sicurezza nazionale e della Difesa. Parliamo dell'inizio del secondo decennio degli anni Duemila, dove era evidente che il processo di digitalizzazione insieme ai benefici si portava dietro maggiori rischi derivanti dalle minacce di *cyber security* che portavano a scenari anche di guerra o di terrorismo sempre più caratterizzati dall'ambito digitale.

Per questo motivo, sono state portate avanti molte iniziative per creare una consapevolezza e poi delle azioni operative e far sì che il tema della sicurezza delle infrastrutture critiche oltre all'approccio olistico a cui accennavo prima (sicurezza fisica, del lavoro e della *cyber security* integrate) riguardasse tutta la filiera di coloro che lavorano per un'infrastruttura critica che può essere una ferrovia, un'autostrada una centrale elettrica; perché il problema grosso è che il punto di vulnerabilità, nell'ambito della catena, può portare ad avere un impatto sul complessivo problema dell'infrastruttura.

Quindi non basta difendere l'infrastruttura in sé, ma bisogna essere in grado, soprattutto dal punto di vista della *cyber security*, di avere la garanzia di avere comuni sistemi di difesa di interscambio di protezione che riguardano tutti gli attori che contribuiscono a monte e a valle alla realizzazione e alla gestione della infrastruttura. Per questo motivo, questo continua a essere un tema di attualità e lo sarà sempre di più.

Credo che le normative vigenti di riferimento per la *cyber security* abbiano da tempo recepito questo tipo di soluzioni, faccio riferimento anche a un esempio recente. Ho partecipato a un evento in cui alcuni membri del Ministero delle Infrastrutture ha convocato alcuni grandi player tecnologici a supporto della realizzazione del nuovo Ponte sullo Stretto.

E, giustamente, oltre all'opera fisica che ovviamente ha le sue complessità, si è posto il tema del Digital Twin cioè di fare come il suo gemello digitale che diventi anche un elemento di difesa dell'infrastruttura fisica. Per far questo significa che centinaia di attori, che più o meno concorrono alla realizzazione e alla gestione del ponte, allo scambio di informazioni su quelli che sono gli utenti dello stesso ponte, dovranno garantire uno scambio di informazioni in maniera sicura ed efficace per poter assicurare che questo Digital twin, questo gemello digitale del Ponte sullo Stretto, possa effettivamente costituire un elemento a difesa dell'infrastruttura.

Ecco un esempio realistico della complessità della difficoltà. Il dato positivo è che, rispetto a molti anni fa, c'è molta più consapevolezza e penso rappresenti un ottimo punto di partenza.