Intervengo come rappresentante di una start-up che ormai è un'azienda internazionale, ma che rivendica le proprie radici italiane, nei settori della sicurezza informatica e della formazione digitale, ancora largamente dominato da realtà d'oltreoceano.

Cyber Guru nasce e cresce in Italia, con una missione precisa: trasformare l'utente finale da anello debole della catena difensiva a primo elemento di resilienza contro gli attacchi informatici.

Accompagniamo pubbliche amministrazioni e imprese di ogni dimensione ed operanti nei più diversi settori di mercato nel rafforzare la propria capacità di resistere ai sempre più numerosi attacchi. Oggi oltre 1000 organizzazioni si affidano alle nostre soluzioni, e almeno un milione e mezzo di utenti sono attivi sulle nostre piattaforme di formazione.

Non lo dico per sottolineare i successi della nostra azienda, ma per esprimere una convinzione profonda: l'Italia può avere un ruolo distintivo in questa trasformazione.

---

Mentre il dibattito globale è spesso dominato da logiche ingegneristiche, l'Italia rispetto a questo segmento, l'Italia può portare un contributo unico: una visione che coniughi etica, sicurezza, visione antropocentrica, rispetto dei diritti fondamentali e pensiero critico.

Non è solo un tratto identitario, è una leva strategica. Il nostro patrimonio culturale, di matrice umanista e rinascimentale, può diventare un valore aggiunto nella formazione di cittadini digitali consapevoli, capaci di gestire in modo maturo e responsabile le tecnologie emergenti.

---

Nel Disegno di Legge, in particolare nell'Articolo 3, si afferma giustamente che la cybersicurezza è una precondizione per lo sviluppo dell'Intelligenza Artificiale. È un passaggio fondamentale, ma dobbiamo aggiungere qualcosa. La sicurezza non può essere solo tecnica. Anche i sistemi più avanzati falliscono se le persone che li utilizzano non sono in grado di riconoscere un rischio, un errore, una manipolazione.

Lo vediamo già oggi:

- l'Intelligenza Artificiale generativa viene sfruttata per attacchi sofisticati di phishing;
- per truffe basate su deepfake, e quindi su alterazioni di prodotti audio-video;
- per strategie di disinformazione automatizzata.

Domani, potrebbero essere gli stessi algoritmi a essere corrotti, per forzare decisioni che favoriscano organizzazioni criminali o che alterino gli equilibri geopolitici. E anche questo, del resto, è un rischio contemplato nel Decreto.

In questo scenario, la persona diventa il punto più esposto, l'anello che può essere più facilmente attaccato.

Su questo specifico punto sarebbe lecito aspettarsi qualcosa di più, un riferimento specifico ai programmi di formazione come elemento fondamentale per raggiungere la resilienza.

---

Tutti i report, a partire da quello pubblicato semestralmente dal Clusit (Associazione Italiana per la Sicurezza Informatica), rappresentano una situazione molto complessa, e cioè una crescita continua degli attacchi Cyber in grado di creare danni alle organizzazioni pubbliche e private che li subiscono.

E alla radice di tutti questi attacchi, c'è, nella maggior parte dei casi un errore umano. Le statistiche più generose quantificano questa relazione al 64%, le più impietose al 90%.

Gli impatti sono sempre più nefasti, colpiscono tutti i settori, anche quelli più delicati rispetto alla tenuta del sistema paese, e negli ultimi tempi ha fatto notizia il ricorso alla Cassa Integrazione da parte di un'azienda italiana, per contenere i danni legati ad un attacco Ransomware.

In questo quadro, gli effetti di uso anti-etico dell'Intelligenza Artificiale sono ancora limitati, ma nei prossimi anni, forse mesi, ci aspettiamo una crescita esponenziale degli attacchi che sfruttino le potenzialità dell'IA.

Esiste ad esempio uno studio condotto da ricercatori della Harvard Kennedy School che ha valutato l'efficacia dell'uso dell'intelligenza artificiale (IA) per automatizzare campagne di phishing. Lo studio, intitolato *"Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects"*, ha evidenziato come l'IA possa aumentare la scala e la redditività delle campagne di phishing, rendendole fino a 50 volte più profittevoli rispetto ai metodi tradizionali. Questo solleva preoccupazioni significative per la sicurezza informatica, poiché rende più facile per i malintenzionati condurre attacchi sofisticati su larga scala.

---

Oggi vediamo affacciarsi un altro rischio, quello di un'adozione "sommersa", e quindi non governata, di strumenti di intelligenza artificiale da parte di singoli dipendenti.

Succede più spesso di quanto si immagini: un dipendente che inserisce dati sensibili in un chatbot, o che utilizza strumenti generativi senza sapere se siano sicuri, affidabili, conformi.

Nelle PMI e nella Pubblica Amministrazione, in particolare, questo fenomeno incontrollato, può aprire la porta a falle di sicurezza, violazioni normative, e perfino a minacce criminali o di spionaggio industriale.

Serve un cambio di rotta. Serve controbilanciare lo sviluppo dell'Intelligenza Artificiale con un'intelligenza umana consapevole, formata, preparata.

---

Le più recenti normative europee in ambito digitale, citiamo NIS2 o DORA, richiamano il tema della formazione.

Anche in questo DDL si fa più volte riferimento alla promozione della formazione dei lavoratori e dei datori di lavoro in materia di Intelligenza Artificiale. Abbiamo letto numerose occorrenze del termine formazione declinate in vari ambiti.

Ma in questi anni è mancato spesso il coraggio del legislatore nel definire criteri chiari su cosa si intende per formazione. E questo, purtroppo, ne riduce l'impatto reale, favorendo atteggiamenti minimalisti orientati alla conformità, piuttosto che al risultato.

La formazione non può essere un'attività una tantum, formale ma inefficace. Deve essere continua, comportamentale, esperienziale. Deve saper allenare il comportamento, non solo trasmettere informazioni.

Ecco perché riteniamo sia fondamentale lavorare su questi aspetti.

---

Chiudiamo quindi con tre proposte, semplici ma ad alto impatto:

1. Sia nel decreto che nella Strategia Nazionale per l'Intelligenza Artificiale, esplicitare in modo chiaro il ruolo necessario della formazione del fattore umano in ambito cybersicurezza.
2. Definire criteri chiari per dare vita a programmi efficaci di formazione continua sul fattore umano e sulla sicurezza comportamentale, rivolti a tutti i soggetti pubblici e privati che adotteranno soluzioni di IA.
3. Premiare chi investe in formazione, valorizzando progetti e percorsi educativi che siano in grado di dimostrare reale efficacia.

---

Siamo ovviamente disponibili a fornire il nostro contributo, con l'esperienza di un'azienda che ha dedicato tutta la sua ragione d'essere a questo specifico tema.

Chiudiamo questa memoria, sottolineando come l'Italia abbia tutte le carte in regola per guidare questo passaggio, con competenza, responsabilità e visione.