AI: come contrastare i rischi legati alla sicurezza informatica

Un recente studio dell'Università dell'Illinois ha sollevato interrogativi fondamentali sull'impiego dell'intelligenza artificiale per identificare e sfruttare le vulnerabilità nei sistemi informatici. La ricerca ha dimostrato che i modelli linguistici avanzati sono in grado nell'87% dei casi di rilevare e utilizzare le vulnerabilità descritte negli avvisi di Common Vulnerabilities and Exposures. Questo dato solleva preoccupazioni sull'eventuale utilizzo malevolo

dell'intelligenza artificiale in ambito di sicurezza informatica, evidenziando la possibilità che tali tecnologie possano essere manipolate per scopi dannosi. Il rapporto sottolinea in particolare la questione legata alle vulnerabilità di tipo «one-day», che sono quelle pubblicamente note ma ancora non mitigate. La capacità dei modelli di IA di sfruttare queste vulnerabilità prima che vengano corrette rappresenta un rischio significativo, spingendo le organizzazioni a adottare risposte tempestive e proattive per proteggere i loro sistemi.

L'indagine ha altresì evidenziato la crescente popolarità dei giochi live-service, che si caratterizzano per frequenti aggiornamenti e acquisti in-app. Ciò pone l'accento sulla necessità di implementare misure di sicurezza robuste e aggiornamenti costanti al fine di salvaguardare questi sistemi dalle minacce emergenti. Gli autori dello studio hanno argomentato contro la limitazione dell'accesso alle informazioni sulla sicurezza, proponendo invece la necessità di adottare strategie di sicurezza più proattive e di mantenere una collaborazione stretta tra sviluppatori, ricercatori e organizzazioni, per contrastare efficacemente i rischi associati all'uso dell'intelligenza artificiale nella sicurezza informatica.

C.G.

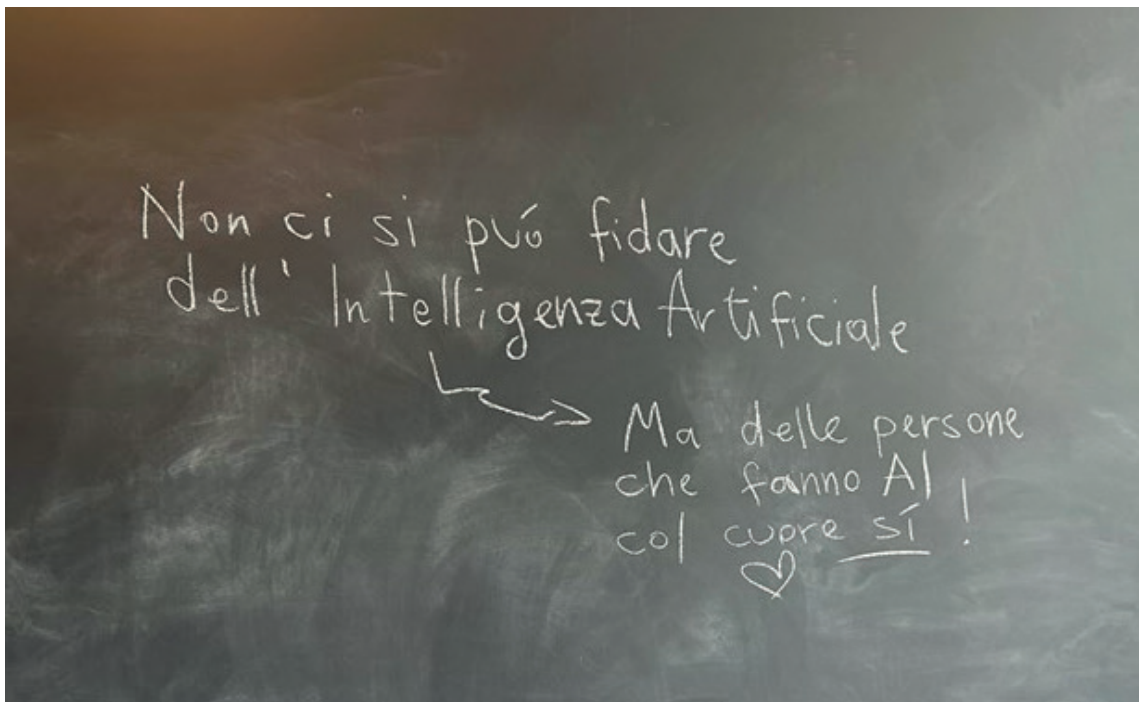
APOSTOLATO DIGITALE

condividere codici di salvezza

ANALISI – È SOLO UNO STRUMENTO PER RISOLVERE PROBLEMI COMPLICATI: SE SI USA CON COSCIENZA

Intelligenza Artificiale? Non ci si può fidare...

Della Intelligenza Artificiale non ci si può fidare». Era questo il titolo di un post che pubblicai sulla pagina del social network LinkedIn, corredato di una foto della lavagna su cui in azienda pensiamo i nostri algoritmi. Uno strano post per chi dirige una società che si occupa essenzialmente di AI. Persino i miei dipendenti mugugnavano «cosa penseranno i nostri clienti? Perché vuoi lanciare un messaggio di questo tipo?». Effettivamente una certa dose di provocazione c'era, però nella fotografia sulla lavagna si leggeva «… ma delle persone che fanno IA col cuore invece sì».



Facciamo un piccolo passo indietro, per tutti coloro che non sanno bene di cosa sto parlando: l'intelligenza artificiale può rappresentare una sorta di totem, quasi un'entità che esiste prescindendo dalle attività umane, destinata «inevitabilmente» a soppiantare l'uomo in quasi ogni compito quotidiano. Non molti però conoscono i concetti di base, tuttavia detto in estrema sintesi l'intelligenza artificiale altro non è che l'applicazione di algoritmi matematici al comportamento di un oggetto: dalla sensibilità da dare alla pressione delle pinze dei freni di un'automobile quando entra in funzione il sistema ABS fino agli assistenti virtuali con cui si può dialogare e rispondono come se fossero una persona in carne ed ossa.

Se da studenti delle medie o delle superiori vi siete mai chiesti a cosa servisse studiare la matematica, la risposta è tutto intorno a voi: realizzare complesse funzioni che permettono di aiutarci in quasi tutto quello che facciamo ogni giorno: pagamenti elettronici, prenotazioni di servizi, guidare l'automobile.

Un aspetto meno intuitivo è: ma l'intelligenza artificiale da dove arriva, chi la fa? Naturalmente delle persone in carne ed ossa! La costruzione o la scelta degli algoritmi più opportuni, le informazioni a cui l'AI permette di accedere, il modo di usarle sono tutte scelte umane.

A me capita, ma sono certo di non essere il solo, di avere una connessione emotiva con alcuni oggetti che uso quotidianamente. Spesso capita di amare in modo particolare un'automobile, darle magari un nome e assegnarle una personalità, un'anima. Probabilmente mi succede quando il progettista non si è limitato a fare il compitino ma ci ha messo impegno, cuore e cervello per realizzare l'oggetto migliore possibile, non importa che sia uno spazzolino da denti, un aeroplano o … l'intelligenza artificiale.

Torno all'aspetto più professionale. Quando un tema è di moda c'è la tendenza a volerlo infilare a tutti i costi in tutto ciò che facciamo: se il colore di moda è il turchese vogliamo tutto di quel colore, un particolare film non può non essere visto, oggi per fortuna mia e dalla mia azienda tutti vogliono che ci sia un po' di intelligenza artificiale in qualsiasi prodotto. Eppure l'intelligenza artificiale è «solo» uno strumento per risolvere dei problemi, spesso particolarmente complicati ma nulla più di questo. La mia missione non è vendere l'intelligenza artificiale, ma aiutare i miei clienti a risolvere i loro problemi. Per farlo è indispensabile che chi realizza gli algoritmi ci metta tutto l'impegno, il cervello e in definitiva il cuore di cui è capace. L'intelligenza artificiale non è un pianeta che sta semplicemente lì in attesa di essere scoperto, è uno strumento che permette di scoprirne di nuovi, di pianeti.

Concludendo forse non ci possiamo fidare della intelligenza artificiale di per sé, però ci possiamo fidare di chi la fa con capacità e coscienza. Gli strumenti possono essere usati per il bene o per il male, con consapevolezza o con superficialità. La scelta sta sempre a ciascuno di noi.

Francesco PENNAROLI,
CEO di Modelway

FocusTALKS: Don Luca Peyron -La partita dell'AI

GLOSSARIO/33 – NUOVE SFIDE

Realtà aumentata ponte tra mondo fisico e digitale

La realtà aumentata è una tecnologia avanzata che integra elementi digitali o virtuali nel nostro ambiente reale, creando un'esperienza mista che arricchisce la percezione del mondo circostante. A differenza della realtà virtuale, che ci immerge completamente in un ambiente digitale, la realtà aumentata sovrappone informazioni virtuali all'ambiente fisico, permettendo agli utenti di interagire con entrambi i mondi simultaneamente. Questa integrazione viene realizzata attraverso dispositivi come smartphone, tablet, occhiali specializzati o sistemi proiettivi che utilizzano telecamere, sensori e software per rilevare, analizzare e rispondere alla realtà circostante. Gli usi della realtà aumentata sono vari e spaziano in molti settori. Nel campo dell'istruzione, ad esempio, può arricchire il materiale didattico con simulazioni interattive e visualizza-

zioni 3D, rendendo l'apprendimento più coinvolgente e intuitivo. Nel settore del commercio, permette ai clienti di visualizzare prodotti in 3D nel loro ambiente prima dell'acquisto, migliorando l'esperienza di shopping online. In ambito sanitario, assiste i professionisti attraverso visualizzazioni dettagliate durante gli interventi chirurgici o la formazione medica, migliorando la precisione e l'efficacia delle procedure. Anche nel settore della manutenzione e della riparazione, la realtà aumentata offre istruzioni passo-passo sovrapposte agli oggetti reali, facilitando compiti complessi e riducendo il rischio di errori. Nel turismo, arricchisce le esperienze dei visitatori fornendo informazioni aggiuntive, storie e visualizzazioni interattive direttamente nei loro campi visivi, trasformando le visite turistiche in esperienze immersive e informative. In conclusione, la realtà aumentata rappresenta un ponte tra il mondo fisico e quello digitale, offrendo nuove possibilità per migliorare, esplorare e interagire con il nostro ambiente.