

INTELLIGENZA ARTIFICIALE/ La posizione più pericolosa dopo 50 anni di internet

Si è tornati a parlare negli ultimi giorni dei progressi dell'intelligenza artificiale. È bene non minimizzare il tutto come se non si corressero rischi.

Possiamo immaginare che quando i ricercatori di Open AI, un'organizzazione no profit sostenuta dal fondatore di Tesla Elon Musk, hanno osservato il primo prodotto di GPT-2 abbiano provato lo stesso orgoglio dei genitori di un bambino prodigio. Tuttavia qualche tempo dopo la fierezza è subentrata la preoccupazione perché queste "creature" hanno sempre [qualcosa di inquietante](#). In questo caso non si è trattato di un fanciullo molto dotato, ma di una nuova intelligenza artificiale la cui specializzazione è la manipolazione dei testi (scrittura, lettura, sintesi, ecc.).

Dal punto di vista dei ricercatori la tecnologia sviluppata per GPT-2 è talmente potente che potrebbe facilmente essere utilizzata per scopi illeciti: dalla generazione massiva di fake news fino alla costruzione di campagne di spamming e phishing molto sofisticate. Il risultato è stato che gli scienziati si sono rifiutati di rendere pubblico tutto il codice sottostante, ma soltanto una parte, giusto per mettere in condizione altri sviluppatori di valutare l'approccio.

Il lavoro condotto da Open AI sembra l'inevitabile conseguenza di una serie di successi partiti da molto lontano. Già nel 2012 un algoritmo stilometrico per il riconoscimento testuale era stato in grado, analizzando 100 mila blog, di identificare in modo automatico l'ottanta per cento degli autori dei post. Da alcuni anni le società specializzate in sicurezza informatica stanno mettendo a punto sistemi che proteggano gli utenti dagli [attacchi di phishing](#). Il mezzo sono sempre algoritmi capaci di riconoscere i diversi stili degli autori dei messaggi per intercettare le falsificazioni. Come sempre accade nella storia dell'umanità la medaglia della tecnologia mostra le sue due facce e il dibattito che ne consegue è sempre interessante.

Nel caso specifico si possono distinguere tre posizioni. Gli apocalittici che evocano lo spettro di un futuro come quello rappresentato nella cinematografia stile *Terminator* e *Matrix*. Gli ottimisti a oltranza che, forse sopravvalutando la razionalità umana, pensano che di fronte a macchine tanto potenti l'uomo sarà capace di introdurre dei sistemi di sicurezza, un po' come le leggi della robotica di asimoviana memoria. Infine, ci sono quelli che minimizzano perché in fondo si sta ancora parlando di "Weak AI", quel particolare tipo di intelligenza artificiale specializzata: simile a un uomo, ma soltanto rispetto a uno specifico compito, in questo caso scrivere.

Per quanto vi possa sembrare strano, i più pericolosi sono proprio questi ultimi perché si troveranno nel futuro senza accorgersene e questo significa essersi "persi". Non

dimentichiamoci che dal primo volo dei fratelli Wright al Concorde sono trascorsi appena 66 anni e quest'anno Internet ha già compiuto cinquant'anni.

Alessandro Curioni

22.02.2019-

<https://www.ilsussidiario.net/news/hi-tech/2019/2/22/intelligenza-artificiale-la-posizione-piu-pericolosa-dopo-50-anni-di-internet/1850893/>