COME DIFENDERSI DAGLI ABUSI DELL' INTELLIGENZA ARTIFICIALE?

Data 20 aprile 2023
Categoria Medicinadigitale

E' probabile che i servizi di intelligenza artificiale vengano gia' usati, all' insaputa altrui, per far passare per propri lavori elaborati invece dal computer. E' ininfluente? No, e vediamo il perche'... Ed esigiamo una adeguata difesa.

Leggevo su un social, alcuni giorni fa, la lamentela di un utente che protestava contro il blocco di CHATGPT voluto dal Garante: "Devo presentare la mia Tesi Universitaria tra una settimana; come faccio senza CHATGPT?"

Francamente sono rimasto interdetto: la risposta che mi veniva su, da persona cresciuta con i vecchi metodi e' stata "Be', fattela da solo, come si e' sempre fatto! Con i libri e magari con Internet!"

Poi ho approfondito il pensiero: questo studente Aveva in progetto di prendere la laurea presentando come proprio un lavoro non suo (in questo caso dell' IA) e poi avrebbe fatto carriera continuando magari a spacciare per propri degli studi di cui in realta' sapeva poco o nulla e che magari nascondevano errori o inesattezze. Magari, come medico, avrebbe curato i suoi pazienti delegando tutte le sue scelte, nel bene e nel male, al computer.

Che differenza c'e' , pensavo, con quelli che plagiavano le tesi scopiazzando sui testi altrui? E perche' punire severamente i "plagiari del libro" e promuovere invece i plagiari informatici?

La differenza fondamentale, mi e' sembrato, e' che la IA si sa mascherare molto bene.

Sa elaborare i testi in modo apparentemente originale, sa presentare citazioni innumerevoli a sostegno, anche se magari a volte non sono neanche giuste. E tutto questo sa farlo senza particolare fatica da parte dell' umano "committente".

Se lo studente protestatario dell' inizio avesse portato avanti la faccenda, si sarebbe laureato, avrebbe fatto carriera continuando con lo stesso metodo, si sarebbe affermato come "esperto" nel suo campo scavalcando magari tanti altri che esperti lo erano davvero.
Tutto cio' si sarebbe verificato, a ben vedere, essenzialmente per il fatto che quanto prodotto da una IA e' pressoche' indistinguibile, almeno apparentemente, da quanto potrebbe essere prodotto da un essere umano.

E non mi soffermo sui recenti fatti di cronaca in cui immagini, filmati o sonori fasulli e generati dall' IA sono state utilizzate per truffe o ad altri fini criminosi.

Come e' possibile evitare tutto cio?
Non credo sia possibile o auspicabile annullare i progressi del settore ma e' indispensabile regolamentarne severamente l' uso. E questo si potrebbe ottenere, almeno provvisoriamente e in attesa di una soluzione definitiva, con un sistema semplicissimo: imporre a tutti i prodotti creati mediante IA un marchio facilmente e palesemente riconoscibile.

I filmati "fasulli" che simulano comportamenti inappropriati di questo o quel personaggio, devono portare un marchio che li renda immediatamente riconoscibili come non autentici; gli scritti devono riportare la "firma" dell' IA sia palese che nei metadati del file; i files sonori devono riportare sullo sfondo un suono riconoscibile. La mancanza o l' alterazione di questi elementi raffigurerebbe di per se' un tentativo di raggiro, sanzionabile con i mezzi legali attuali o, meglio, con normativa (possibilmente internazionali) appositamente aggionate.

Tutto cio' e' certamente nelle possibilita' e nelle capacita' dei programmatori, e anche se certamente esisteranno sempre i soliti "furbetti" si otterra' la possibilita' di scoraggiare i non-esperti e di rendere piu' facilmente riconoscibili i prodotti artificiali.
Lo scopo sarebbe quello di evitare ricatti, raggiri, diffamazioni (attualmemente facilmente effettuabili da chiunque mediante gli appositi programmi sparsi in giro) senza comunque inibire la liberta' di espressione: la satira non verrebbe inibita, pero' dovrebbe essere sempre visibile che si tratti di una satira, e non di un reale comportamento inappropriato o imbecille del soggetto preso di mira.

Potremmo cosi' anche essere piu' tranquilli che la telefonata di aiuto apparentemente inviata da qualche nostro familiare sia autentica, e non una truffa.

Tutto cio' non e' facile, ma penso sia indispensabile arrivarci comunque.

Parere personale, come al solito

DanieleZamperini.