Da ChatGPT a AutoGPT: addio agli operatori umani. L'automazione del servizio clienti e non solo

scritto da Gilberto Pierazzuoli

Parte terza, qui la prima, qui la seconda.

L'hype non cessa di crescere. Al bar dello sport si parla più di AI che di calcio! Intanto sgombriamo il campo sul significato dell'acronimo che può creare confusione. L'AI sta per *Artificial Intelligence,* mentre IA ne è la semplice traduzione: Intelligenza Artificiale. Al bar circolano, racconti e leggende, storie di paura e infatuazioni. Il fatto sta che tutto questo rumore qualche cosa lo provoca. E così il prezzo delle azioni di Nvidia, il produttore dei chip su cui si basano le schede video dei nostri computer, sono salite del 60%. Sì perché ormai i super computer si basano sulle GPU (graphics processing unit) (i chip delle nostre

schede video), su migliaia di GPU come quelle che Nvidia fornisce per la costruzione del super computer della Microsoft. Nello stesso tempo, si sfregano le mani tutti i possessori di data center.

Ad un incontro un po' particolare al quale ho partecipato dove si cercava di spiegare a un pubblico generico di che cosa si parlasse a questo proposito, una signora ha dichiarato una cosa che assomigliava molto a un luogo comune ma che in realtà coglieva il nocciolo della questione: le macchine non eguaglieranno mai l'intelligenza umana perché noi siamo diversi e proviamo emozioni che le macchine non provano. Con questo non si nega l'intelligenza delle macchine; di forme di intelligenza diversa da quella umana ce ne sono infatti tantissime: le intelligenze collettive e collaborative di molti animali sociali, formiche, api, stormi di uccelli. Quella decentrata dei polpi dove ogni tentacolo ha capacità di Agency autonoma. Poi ci sono quelle imperscrutabili, ma non si tratta di *deep learning*, e della relativa *black box*, di cui abbiamo già parlato, si tratta invece, per esempio, dell'intelligenza di una mucillagine, la *Physarum Polycephalum* (vedi anche qui), insomma, l'intelligenza intesa come capacità di adattarsi a situazioni nuove e di modificare la situazione stessa quando questa presenta ostacoli all'adattamento, non è un carattere esclusivo dell'animale umano. Anche imparare dai propri errori non è un appannaggio soltanto umano e/o soltanto biologico, così come la trasmissione del sapere. Certo, quest'ultima, è un carattere che si fa evidente nei mammiferi che dedicano molto tempo a questo aspetto tanto che un carattere specifico dell'animale umano sarebbe la neotenia, ovvero il suo protratto infantilismo che lo fa rimanere più tempo nella cosiddetta età dell'apprendimento.

Quello che non è vero, come abbiamo visto, è che le intelligenze si assomiglino. Anche le intelligenze macchiniche sono più di una. Ma quella che interessa al capitale è quella che in qualche modo si presenti come forma simile a quella umana nel senso che la possa supplire se non soppiantare. L'intelligenza nell'ambito del mercato è quella cosa che offre un servizio, la capacità di svolgere un compito o quella di automatizzare una mansione non soltanto meramente meccanica, quella che sostituiva cioè la forza lavoro muscolare umana, ma anche quella che suppliva a dei compiti più complessi nei quali si dovevano prendere delle decisioni. Il software dava questo guizzo cognitivo alla macchina – all'hardware. Un hardware munito di sensori di feedback che lo informavano sugli effetti del suo agire in maniera tale da poterlo adattare allo svolgimento del compito a lui attribuito. Ma la AI fa delle cose ancora più sofisticate. Faccio un

esempio: la capacità di riconoscimento facciale nei sistemi di messa a fuoco delle macchine fotografiche moderne. È una facoltà molto diversa da quella del riconoscimento facciale come facoltà delle telecamere di controllo e sorveglianza. Si tratta semplicemente di tenere a fuoco il viso di un individuo che è all'interno di una inquadratura, privilegiando questo dato rispetto ad altri elementi come lo

sfondo. Questo tipo di intelligenza è quella sottesa alla possibilità di considerare alcuni oggetti come smart. Lo smartphone, lo smartwatch o la smart TV, qualcosa a metà tra intelligenza e la capacità di andare in rete. Ma a sollevare il polverone mediatico non è stata questo tipo di intelligenza, più che altro è stato il lancio di ChatGPT che l'ha fatta comparare a una forma di intelligenza più complessa, simile a quella umana, del tipo che in questo ambito si suole chiamare AGI. Qui si apre un ampio spettro di possibilità, ma anche tutta una serie di interrogativi molti dei quali sia neurologici sia filosofici. Si tirano in ballo concetti come senzienza, coscienza, conoscenza. Se il test di Turing fosse bastante a dichiarare che una macchina ha facoltà intellettive simili a quelle umane, almeno in campo linguistico, le cosiddette *chatbot* ci si stavano avvicinando da qualche tempo, ma non a un livello così sofisticato. Le chatbot precedenti si limitavano a poter interloquire con un umano soltanto su un argomento particolare e in un ambito specifico. Esse tentavano di sostituire l'operatore umano dei call center riuscendovi nemmeno molto bene, proprio perché spesso la richiesta dei clienti/utenti verteva su dei casi particolari non adombrati dalle procedure automatizzate in atto. Vertevano cioè su delle eccezioni che il sistema non poteva conoscere proprio perché non contemplate, e quindi non a conoscenza delle chatbot stesse. ChatGPT è un'altra cosa. Ha infinite specializzazioni: può dialogare sia con l'uomo della strada, sia con lo scienziato o con il teologo. Ha, sembrerebbe, competenze totali. Per questo al primo impatto sbalordisce. Il suo

non appare poi come semplice competenza teorica, ha anche una competenza fattuale enorme, limitata comunque soltanto (momentaneamente?) al linguaggio. Sa scrivere testi scientifici, codice di programma, poesie, articoli, riassunti. Ha anche delle sorelle che sanno disegnare, dipingere e fotografare. Fare brevi video, comporre ed eseguire musica, correggere compiti.

La sua particolarità è che queste competenze possono essere vendute. Non soltanto con chi ci vuole giocare ma anche per coloro che ci vogliono lavorare, meglio, per coloro che possono farle fare dei lavori. Un blogger basta che abbia qualche idea di base, una notizia semplice da affidare a ChatGPT la quale scriverà i post al posto suo. I giornali e il giornalismo non di inchiesta, li potrà scrivere lei. La revisione dei codici e la scrittura di routine ma anche di interi programmi software, li potrà fare lei. Il servizio clienti di un qualsiasi produttore potrà essere sostituito in toto da lei. Da questo, come abbiamo detto, il pericolo del proliferare delle fakenews. Del valore testimoniale dei testi e delle immagini. L'amplificarsi del fenomeno del complottismo. La Federal Trade Commission avverte che la tecnologia di intelligenza artificiale come ChatGPT potrebbe "mettere il turbo" alle frodi: "L'AI fornisce una serie di opportunità, ma anche dei rischi, E credo che abbiamo già visto come potrebbe essere usata per accrescere frodi e truffe. Abbiamo avvertito gli operatori del mercato che i casi in cui gli strumenti di AI siano effettivamente progettati per ingannare le persone potranno essere oggetto di un'azione da parte della FTC", ha dichiarato Khan presidentessa della FTC (su TechCrunch).

Come ho già detto l'effetto più macroscopico di questa tecnologia non sarà quello di renderci tutti scrittori, pittori, o musicisti senza avere nessuna competenza manuale per farlo. L'effetto sarà la sostituzione di molti addetti umani con gli algoritmi che innervano ChatGPT. Sarà l'aumento della precarizzazione del lavoro, lo svilimento delle mansioni, il proliferare della gig-economy. Che, come abbiamo visto, cela il fatto che dietro queste tecnologie ci sia spesso del lavoro sottopagato fatto dagli schiavi del clic che etichettano i dati e le immagini che alimentano i data set di riferimento.

Questo avviene per il bisogno di monetizzare i servizi che le piattaforme web offrono, ma non nel senso di una giusta remunerazione – concetto per altro molto aleatorio – ma della massimizzazione del profitto all'interno di una offerta che si veste dei panni attuali, non per soddisfare un bisogno o una aspirazione da parte della maggioranza della popolazione, ma costruendo un apparato che

velocemente diventa indispensabile. Non si tratta soltanto di creare bisogni indotti, ci sono infatti delle aggravanti come quella di non mostrare gli effetti collaterali, spesso deleteri, quando non catastrofici. L'utilità della plastica è indiscutibile, non così le isole di plastica nel pacifico e altrove, non così le microplastiche nei nostri organismi, e così ad libitum.

Le bacheche dei social sono piene di offerte di AI per le aziende. Pensavo fosse un'AGI e invece era un'API, intitola Guerre di Rete. Dove sta la differenza? Le API (Application Programming Interfaces) sono interfacce che permettono alle applicazioni di interagire con altre applicazioni. In questo caso di trasferire le competenze di ChatGPT in applicazioni di tipo aziendale per svolgere automaticamente una serie di compiti non precedente automatizzati. Qui si monetizza la tecnologia, si vendono le capacità "cognitive" di ChatGPT. In questo momento ChatGPT è l'app con la crescita più veloce di sempre! Sono stati raggiunti 100 milioni di utenti in questo poco tempo. Non solo, è messa a disposizione la versione plus a venti dollari al mese che permette di avere una priorità d'accesso e una velocità superiore di quella degli utenti generici. Mentre il Garante per la protezione dei dati personali blocca l'accesso in Italia a ChatGPT, alcuni dirigenti del settore, esperti molti importanti di Intelligenza Artificiale, gente come Elon Musk, i ricercatori di DeepMind e altri, hanno pubblicato una lettera aperta dove si chiede una moratoria di sei mesi allo sviluppo di AI superiori a GPT4. La mossa è di difficile interpretazione, molti l'hanno intesa come il bisogno da parte dei concorrenti di open.ai di recuperare il

ritardo delle loro AI nei confronti di GPT4, ma secondo me ci sono anche altri motivi. Come abbiamo già detto questo tipo di algoritmi lavorano sulla sintassi e non sulla semantica, tanto che quello che dicono è apparentemente sensato ma non per questo vero. Per questo si dice che le AI soffrono di allucinazioni, vedono cose che non esistono. Ma anche tra quelle che esistono, o esistono soltanto potenzialmente, ci sono cose eticamente corrette e altre meno. Le commissioni deputate al controllo dei social moderano la pubblicazione cercando di escludere frasi, video o immagini che inducono alla violenza, all'odio raziale e tante altre belle cosine. Il problema è moderare l'output di AI di tipo LLM come ChatGPT. Nel calderone infinito di dati che le alimentano sono contenute probabilisticamente anche sequenze sintattiche che rimandano ad ogni genere di schifezza. Come fare a evitare che la macchina ne faccia uso? Non è semplice. I tecnici non riescono infatti a trovare il modo per evitare almeno i problemi che potrebbero allarmare una pubblica opinione che, per quanto condizionata, potrebbe non essere sorda di fronte all'emergenza di questi loro comportamenti. Ecco allora l'appello agli stati, alla politica. Fate voi quello che reputate più giusto, così noi ce ne laviamo le mani. Ma attenzione a non esagerare. Queste tecnologie sono alla base dell'attuale sviluppo e mettere troppi bastoni tra le ruote potrebbe essere pericoloso. Qui il testo della lettera.

Nel frattempo è arrivata una implementazione di ChatGPT forse più insidiosa. Si tratta di AutoGPT. E qui le cose si fanno ancora più pericolose. Ho già detto che ChatGPT commette sbagli, si inventa delle cose, dice delle bugie che sono difficili da scoprire perché immerse in tante verità, comprese quelle che soltanto un pubblico particolarmente competente può verificare. È così brava e sicura di sé, tanto da rendere difficile dubitare di quello che dice. Ma non sono errori di gioventù. Sono intrinsechi al modello. Derivano da quella scorciatoia della quale vi avevo parlato. In un certo senso quelle di ChatGPT sono chiacchiere, certo da non sottovalutare, la parola ha infatti anche un forte potere performativo. Ma AutoGpt può passare ai fatti. Se le dai un compito, lei cerca di realizzarlo, prova a realizzarlo e impara dai suoi sbagli diventando sempre più brava. È successo che per fare tutto ciò, a un certo punto, "l'agente artificiale" si sia accorto che occorreva servirsi di un programma specifico, assente nel computer del suo committente. Ha fatto la cosa più ovvia e cioè lo ha istallato. Insomma AutoGpt è dotato di attuatori. Le cose non le dice soltanto, le fa. L'utente può infatti pianificare degli obbiettivi e lasciare che sia il modello ad operare automaticamente per suo conto. A questo riguardo non parliamo semplicemente

di “AI” ma più propriamente di *Autonomous AI Agent*, come nel caso di *AutoGPT*. Si tratta nello specifico di una piattaforma Open Source, per il momento ancora in fase sperimentale, pensata per realizzare i “pensieri” di GPT4 in modo che esso sia in grado di raggiungere da solo il risultato atteso dall’utilizzatore. AutoGPT si può collegare alla rete potendo così accedere a informazioni aggiornate, *darsi da solo dei comandi* per completare gli obiettivi che gli vengono assegnati. Ha accesso a Internet, ricorda le interazioni e ha la capacità di scrivere ed eseguire codici per raggiungere un obiettivo. Tutte cose a prima vista straordinarie, ma è un agente che si basa su GPT il che comporta gli stessi problemi di cui abbiamo parlato sopra; in più aggiunge l’aggravante che qualsiasi sia il risultato da ottenere, esso cercherà di raggiungerlo agendo autonomamente.

Poco prima del polverone ChatGPT è uscito l’esito di una ricerca sugli algoritmi di tipo predittivo, non sto cambiando discorso: sono tutte implementazioni basate sulla medesima scorciatoia. Wang, Angelina e Kapoor, Sayash e Barocas, Solon e Barocas, Solon e Narayanan, Arvind, si esprimono in questo *paper* contro l’ottimizzazione predittiva: sulla legittimità degli algoritmi decisionali che ottimizzano l’accuratezza predittiva (4 ottobre 2022). Disponibile su SSRN. Questa è una parte dell’abstract tradotto in italiano:

> *“La nostra tesi è che l’ottimizzazione predittiva sollevi una serie distintiva di preoccupazioni normative che la rendono presumibilmente illegittima. Per*

verificarlo, esaminiamo 387 report, articoli e pagine Web di università, industria, organizzazioni non profit, governi e concorsi di modellazione e troviamo molti esempi reali di ottimizzazione predittiva. Selezioniamo otto esempi particolarmente significativi come casi di studio. Contemporaneamente, sviluppiamo una serie di critiche normative e tecniche che sfidano le affermazioni fatte dagli sviluppatori di queste applicazioni, in particolare le affermazioni di maggiore accuratezza, efficienza ed equità. La nostra scoperta chiave è che queste critiche si applicano a ciascuna delle applicazioni, non sono facilmente eludibili riprogettando i sistemi e quindi mettono in discussione la legittimità della loro implementazione. Sosteniamo che l'onere delle prove per giustificare il motivo per cui l'implementazione dell'ottimizzazione predittiva non è dannosa dovrebbe spettare agli sviluppatori degli strumenti. Sulla base della nostra analisi, forniamo una rubrica di domande critiche che possono essere utilizzate per deliberare o contestare la legittimità di specifiche applicazioni di ottimizzazione predittiva".

Nel prossimo articolo svilupperò le differenze tra intelligenze animali e quelle delle macchine attuali. In prima istanza per sfatare e mettere in discussione le aspettative di questo modello di implementazione delle tecnologie digitali, la seconda sarà invece il tentativo di mettere in luce le procedure che "contano" e per chi esse "contano"!

Le immagine sono state generate da Midjourney v5 su indicazioni testuali dell'autore