

## La Rivoluzione Nascosta della Pubblicità nell'IA

Esistono argomenti sui quali le opinioni sono radicalmente diversificate e le contrapposizioni attraversano tutti i settori dell'opinione pubblica. Anche i ricercatori, che dovrebbero avere un approccio "razionale" ed esprimere pareri sulla base di considerazioni esclusivamente scientifiche, manifestano opinioni e aspettative contrapposte. Questo avviene in quei campi nei quali più forti sono le implicazioni sociali, come nel caso del nucleare e della valutazione della crisi climatica.

Per quanto riguarda l'IA, la situazione è ancora più complicata: per la prima volta ci si trova di fronte a una tecnologia che mette in discussione la nostra superiorità intellettuale. Anche con i computer c'era stato qualche accenno di inquietudine, ma in ultima analisi era abbastanza evidente che si trattava di processi di tipo meccanico e deterministico; il nome stesso di "calcolatori" ne è una conferma. Solo nei film di fantascienza si faceva cenno a possibili superamenti delle capacità umane.

Con l'IA le cose sono diverse: sembra proprio che le macchine insidino l'uomo nel suo settore più peculiare. Trionfano e si diffondono test per verificare la riconoscibilità delle cose scritte dall'IA da quelle umane. Il test di Turing (fino a oggi abbastanza sconosciuto) sembra essere superato dall'IA. Recentemente, un articolo scientifico generato dall'IA ha superato i requisiti per la pubblicazione in riviste scientifiche.

In questa situazione, nella quale è quanto mai vero che "il cuore ha le sue ragioni che la ragione non conosce", la strada più corretta è quella di confessare le proprie ragioni senza pretendere una razionalità asettica del tutto impossibile; una pretesa che quasi sempre serve solo a nascondere le proprie ragioni del cuore.

"La materia si fa spirito": questa potrebbe essere la definizione più suggestiva di quello che rappresenta l'IA. Il suo riferimento a una frase fondante del cattolicesimo, con la sua inversione di termini, è estremamente evocativo e per certi versi inquietante, forse diabolica. Inoltre l'IA è in rapidissima evoluzione e questo rende ancora più problematico individuarne il suo impatto sociale, per questo è più saggio analizzare qualche aspetto particolare riconducibile a situazioni analoghe.

Implementare il software per l'IA è molto costoso, così come è costoso distribuirla. I modelli linguistici di grandi dimensioni (chiamati LLM - Large Language Model) richiedono mesi di addestramento su migliaia di processori specializzati, con costi che possono raggiungere centinaia di milioni di dollari per un singolo modello. Questi costi non si fermano allo sviluppo. Ogni interazione con ChatGPT o Gemini genera costi operativi significativi. Moltiplicati per milioni di utenti al giorno, diventano insostenibili senza un modello di business solido.

D'altra parte, è essenziale per la sua stessa natura che l'IA sia utilizzabile dal più grande numero possibile di persone, non solo per la naturale vocazione delle imprese a distribuire il proprio prodotto, ma perché per la sua stessa natura è avida di dati. I dati sono il suo vero nutrimento e questi si possono ottenere solo con una diffusione di massa.

In questo contesto, le imprese dell'IA si trovano in difficoltà: è impossibile coprire le

spese utilizzando canoni per l'uso dell'IA e, d'altra parte, canoni alti ne limiterebbero la diffusione. Se ci si riflette, è una situazione simile a quella della televisione privata, e la soluzione è la medesima: utilizzare la pubblicità.

Ma l'IA, almeno per quanto riguarda il suo uso nelle chat, nella generazione di immagini, video e musica, presenta una gestione della pubblicità completamente diversa dalle esperienze precedenti, sia quelle della carta stampata sia quelle su Google o sulle varie app che si possono utilizzare.

In tutti i casi precedenti, la pubblicità è esplicita sia nella forma che nei contenuti, è invasiva, spesso fastidiosa, ma non si nasconde. Anzi, cerca in ogni modo di colpire l'attenzione. Quando facciamo una ricerca su Google compaiono nelle prime pagine gli inserzionisti che hanno pagato; quando si va su un link viene visualizzato il sito con le sue belle pagine di pubblicità. Per dirla in breve, la pubblicità non si nasconde.

Con l'IA le cose sono radicalmente diverse. Nel rispondere a un quesito, una chat fornisce un testo che contiene la risposta; poi, siccome ha fatto una ricerca sul web, aggiunge piccoli pulsanti per chi vuole accedere alle fonti consultate. Ma la risposta è costituita da un testo, e questo fa la differenza.

Probabilmente il sogno segreto di ogni pubblicitario è quello di far sì che il suo messaggio passi come consiglio disinteressato di un esperto neutrale: con l'IA questo può realizzarsi. Le varie chat stanno diventando sempre più brave e competenti e gli utenti tendono sempre più a utilizzarle. Probabilmente bisognerà presto inventare un neologismo per indicare l'uso delle chat, come è stato fatto con "googlare" per le ricerche su Google.

Che questa sia la situazione è dimostrato dal comportamento di Google. Pur essendo la società più avanzata nel campo dell'IA – OpenAI per sviluppare ChatGPT ha utilizzato "Transformer" che è un software di Google – è apparsa piuttosto prudente nel rendere disponibile l'IA. Probabilmente tale prudenza derivava dalla necessità di risolvere il problema di come riposizionare la pubblicità nei suoi prodotti, in particolare su Google. Attualmente sembra che abbia risolto i suoi dubbi perché si è letteralmente scatenata, inserendo i suoi modelli (Gemini) in tutti i settori, in tutti i suoi prodotti e soprattutto integrandoli nella ricerca.

L'integrazione della pubblicità nell'IA sta sconvolgendo l'intero ecosistema pubblicitario. Le agenzie tradizionali, abituate a creare campagne per spazi predefiniti (banner, spot TV, annunci stampa), si trovano di fronte a un paradigma completamente nuovo. Con l'IA, la pubblicità può essere creata dinamicamente in tempo reale, personalizzata per ogni singola interazione. Tuttavia, questo crea un paradosso: più l'IA diventa sofisticata nel generare pubblicità, meno valore aggiunto possono offrire le agenzie tradizionali.

Tradizionalmente, esisteva una separazione relativamente chiara tra contenuto editoriale e pubblicitario. Anche quando questa linea si offuscava, come nel caso del native advertising, rimanevano meccanismi di identificazione e controllo.

Con l'IA, questa distinzione diventa praticamente impossibile da mantenere. Quando un utente chiede consigli su un prodotto, la risposta dell'IA può essere influenzata da accordi commerciali senza che ci sia modo di distinguere l'informazione oggettiva dalla promozione commerciale. Il problema si aggrava quando l'IA viene utilizzata per rispondere a domande su temi di attualità, salute, finanza o politica. Le decisioni commerciali delle aziende tecnologiche iniziano a influenzare non solo cosa vediamo, ma

come interpretiamo la realtà. A differenza dei media tradizionali, dove l'orientamento editoriale era relativamente trasparente, l'IA presenta le sue risposte con un'aura di oggettività scientifica che nasconde le influenze commerciali sottostanti.

L'impatto sui mezzi di informazione tradizionali sarà devastante. Giornali e televisioni vedranno diminuire drasticamente il traffico online quando gli utenti otterranno risposte dirette dall'IA senza bisogno di consultare fonti originali. Questo crea un circolo vizioso: meno ricavi pubblicitari per i media tradizionali significa meno investimenti nel giornalismo di qualità, il che rende l'IA ancora più attraente come fonte di informazione rapida.

La pubblicità può essere integrata così sottilmente nel flusso informativo da diventare indistinguibile. Un'IA può modificare leggermente le sue risposte per favorire determinati brand senza che l'utente se ne accorga. Può enfatizzare certi aspetti di un prodotto e minimizzarne altri, tutto in modo apparentemente naturale e conversazionale.

Particolarmente preoccupante è la possibilità di manipolazione emotiva su larga scala. L'IA può essere programmata per identificare utenti in stati di vulnerabilità – stress finanziario, problemi di salute, difficoltà relazionali – e prenderli di mira con pubblicità specificamente progettate per sfruttare queste vulnerabilità.

Non è ancora ben chiaro come evolverà la pubblicità all'interno dell'IA. In ogni caso, sarà estremamente problematico disciplinarla attraverso delle leggi. Infatti, i modelli sono delle "scatole nere" e il meccanismo di generazione del testo o delle immagini non è affatto trasparente. Si conoscono, ovviamente, i principi alla base del funzionamento, ma non è tracciabile il percorso delle inferenze che portano al risultato finale.

A questo proposito circolano articoli, a volte un po' sensazionalistici, sulle capacità degli LLM di sfuggire ai controlli. È interessante un articolo sulla tendenza degli LLM a sfuggire ai controlli:

"The Illusion of Control: Why Agentic AI is Forcing a Total Rethink of AI Alignment"

<https://www.unite.ai/the-illusion-of-control-why-agentic-ai-is-forcing-a-total-rethink-of-ai-alignment/>)

Queste caratteristiche degli LLM hanno scatenato la voglia di competere. Esiste una categoria di appassionati che pratica un'attività software denominata "jailbreaking", che ha come scopo quello di creare dei prompt per le chat che permettano di violare i filtri interni degli LLM. Quelli, per intenderci, che impediscono agli LLM di usare termini sessualmente scorretti, di fornire informazioni su esplosivi o di incitare al suicidio. Insomma, tutti quei filtri che impongono a un LLM di essere una "brava persona".

In questa situazione, implementare controlli efficaci sulla pubblicità integrata nell'IA presenta sfide tecniche enormi. A differenza dei media tradizionali, dove è relativamente semplice identificare contenuti sponsorizzati, l'IA genera risposte in tempo reale attraverso processi complessi e spesso opachi. Gli algoritmi di IA operano attraverso miliardi di parametri che interagiscono in modi difficilmente prevedibili. Anche gli stessi sviluppatori spesso non sanno esattamente perché un modello produce una determinata risposta piuttosto che un'altra. Come si può quindi garantire che una risposta non sia influenzata da pressioni commerciali?

I tentativi di audit algoritmico si scontrano con problemi pratici significativi. I modelli di

IA più avanzati sono sistemi proprietari protetti da segreti industriali. Le aziende sono riluttanti a rivelare i dettagli del loro funzionamento, sostenendo che questo comprometterebbe la loro competitività e sicurezza. Anche forme ridotte di trasparenza presentano problemi. Spiegare perché un'IA ha dato una determinata risposta richiede sistemi di "explicability" che spesso forniscono spiegazioni post-hoc che potrebbero non riflettere i veri processi decisionali dell'algoritmo.

Insomma, controllare l'IA con delle regole sarà una questione decisamente complicata. Di fronte a questa situazione, le soluzioni tradizionali sono di fatto impraticabili. La richiesta di regolamentazione, per quanto sacrosanta, si basa su una visione irrealistica della realtà, immaginando per il futuro strumenti che erano adatti nel passato.

Forse una speranza può venire da quel mondo di informatici che ha sostenuto l'open source (sono riusciti a farlo digerire anche a Microsoft, che è tutto dire) e che con le loro associazioni può fornire gli strumenti per controllare in qualche modo l'IA. Per fortuna sono molte le società che si stanno muovendo in questa direzione, anche se spesso i rapporti con le società "enterprise" sono ambigui. A volte queste ultime si appoggiano a questo mondo offrendo anche soluzioni open source, un po' per fornire un'immagine democratica, un po' perché è il modo migliore per reclutare sviluppatori.

Ma che questo movimento possa essere un baluardo contro un'IA invasiva e manipolativa è un'aspettativa che appartiene senza dubbio alle "ragioni del cuore".

Giuseppe Materni