AI tra inganni, omologazione e protezione dei dati personali

Donatella Salari

L'Ai fa paura un po' a tutti: politici, consumatori, sceneggiatori, attori e attrici, semplici utenti delle piattaforme digitali, mercati.

A maggio scorso, il sindacato americano degli sceneggiatori, già polemico con gli effetti retributivi perversi indotti dallo *streaming* e in stato di agitazione contro i principali *gatekeepers* come Netflix, Amazon, Apple, Disney, Warner Bros, Discovery, NbcUniversal, Paramount Plus e Sony, ha indetto uno sciopero. I motivi? Oggi il fenomeno AI interpella gli attori dello *star system* che sono sul piede di guerra perché l'intelligenza artificiale può creare situazioni seducenti, come ascoltare la voce (sintetica) del famoso regista o dell'autore dell'opera da cui è tratto il film, semplicemente elaborando dati reali, ossia , attraverso un frammento di voce, l'algoritmo creerà ciò che si desidera ascoltare, la storia che vogliamo sentire o che potremmo inventare. Anche per gli attori la situazione appare critica perché, attraverso il riconoscimento facciale, è possibile sfruttare, previa riproduzione, volti di attori famosi, la loro mimica e le loro caratteristiche.

In campo politico, dove si era salutata l'intelligenza artificiale come produttiva di democrazia attraverso il controllo positivo delle azioni dei vari leader e dell'accesso all'informazione, il suo fulgore di nuova promessa sembra tramontata insieme a quella proiezione ottimistica che pensava di sfruttare l'AI per creare un premierato che, prescindendo dal politico di turno, potesse semplicemente attuare un programma liberamente scelto dagli elettori (Joshua Davis).

Agli iniziali entusiasmi aveva certo contribuito la possibilità di sfruttare le potenzialità degli algoritmi per analizzare le esperienze politiche passate, individuarne gli errori centrando i correttivi dell'azione di governo, ma si è subito visto che la beatificazione dell'AI incontrava due ostacoli

insuperabili: i limiti dei dati utilizzabili per "alimentarla" attraverso il *deep learning*, non sempre corretti ed aggiornati, il proliferare nei dati stessi di *bias* cognitivi, per non dire pregiudizi e distorsioni, insomma, tutto un catalogo di percorsi mentali errati che vanno a nutrire l'algoritmo minandone l'attendibilità.

Si possono fare, in proposito, tanti esempi di simili errori di valutazione o di mancanza di oggettività di giudizio, che ciascuno di noi elabora ogni giorno: per esempio il *bias* dell'ancoraggio (anchoring *bias*), per cui il soggetto tende a formarsi un'opinione in base alle prime informazioni che riceve. Si tratta di un fenomeno normalissimo che riguarda anche noi magistrati al momento della decisione quando rileggiamo gli atti di parte, ma che controlliamo efficacemente attraverso il dialogo processuale del contraddittorio e, infine, con la motivazione, ossia con strumenti culturali e disciplinari.

Lo stesso meccanismo può essere osservato in politica laddove l'individuo più che formarsi una propria opinione confrontando informazioni e tesi tende, invece, a selezionare solo quelle favorevoli alla propria inclinazione, ideologia o esperienza *(confirmation bias*).

Esiste anche il *bias* della scelta (*choice-supportive bias)* dove ciascuno di noi tende ad auto confermare scelte irrazionali ed impulsive. In breve: mentiamo a noi stessi, scegliendo scorciatoie mentali di rassicurazione che sono, evidentemente, nemiche della conoscenza e dell'autostima e si potrebbe continuare con i tanti tipi di *bias* che schermano la nostra conoscenza non solo della realtà, ma di noi stessi.

Ora è chiaro che questi limiti cognitivi sono ambivalenti, ossia possono rendere inattendibili quelli del *deep learning* dell'AI, ma possono essere sfruttati dalle piattaforme estraendoli dalle nostre navigazioni nel Web (Google, Amazon, Facebook etc., meglio noti come *gatekeepers*) che controllano il mercato digitale, soprattutto per quell'ambito che riguarda l'azione dei visitatori dei siti che, accedendo, fissano il prezzo delle inserzioni pubblicitarie e che, sotto questo aspetto, divengono consumatori e produttori al contempo (c.d. *prosumers*), creando l'altro fenomeno collegato al molesto potere dei c.d. *influencers*.

Se la reciproca influenza di questi dati condiziona il mercato, non può negarsi che essa ponga il problema serissimo della loro elaborazione da parte della AI generando ciò che si chiama produzione di dati attraverso altri dati e che può rivelarsi estremamente pericolosa allorché il pericolo

della profilazione dei dati raccolti, ben evidenziata nel noto scandalo di Cambridge Analytics) sfoci nell'utilizzazione di milioni di account Facebook senza il consenso dei rispettivi utenti) ossia raccogliendo dati inerenti agli utenti di un servizio e che spesso sono ottenuti attraverso l'uso gratuito di determinati servizi, discriminando i dati stessi a seconda dei comportamenti degli utenti senza che gli interessati comprendano che se il servizio è gratis il prodotto sei tu.

La mancanza di una normativa chiara nelle interazioni fra dati e sistemi di intelligenza artificiale può così influenzare negativamente settori sensibili come quello della salute (*e.health*) nel momento stesso in cui il consumatore, irretito dalla tecnologia, interpelli la piattaforma chiedendo pareri in campo medico o farmacologico, senza rendersi conto che la condivisione delle informazioni che vengono inviate dall'utente, onde ottenere il responso, non rivestono lo stesso valore del parere ottenuto che spesso non è attendibile, esattamente come non è attendibile il correttore di windows quando coregge " notificatorio" in "notificatori". Stesso discorso per i pareri legali perché la risposta del robot lawyer non è paragonabile a quella di un avvocato specializzato.

Oggi prevale, perciò, un pensiero apocalittico di sfiducia e paura nei confronti di un AI tanto più senziente quanto onnipotente, soprattutto davanti all'effetto perverso di alcune applicazioni come chatGPT e la elezione di personaggi come Trump e Bolsonaro le cui vicende mostrano bene come i *big data* e gli algoritmi di intelligenza artificiale possano diventare strumenti di deprivazione delle democrazia se utilizzate a fini autoritari e di sorveglianza e che la tecnologia non è mai neutra nelle dinamiche tra piattaforme, utenti e voto. Per esempio, secondo la tecnosociologa Zeynep Tufecki, via *social* è molto facile creare "seguito" spingendo gli utenti a riversarsi nelle strade, ma è forte il rischio di generare movimenti immaturi perché poco strutturati come accaduto con la rivoluzione araba e, come si è visto, nelle rivolte di questi giorni in Francia, si può aggiungere.

In questo contesto nasce, attraverso l'intelligenza artificiale, un paradosso. Infatti, gli algoritmi allenati attraverso i *big data,* a loro volta alimentati da quelli prodotti attraverso gli scambi di piattaforma, risultano capaci di analizzare e tesaurizzare tutte le informazioni che vengono dai nostri comportamenti e spostamenti individuando le nostre tendenze politiche, religiose e sessuali, creando sorveglianza continua. Occorre, allora, riflettere sul fatto che questi stessi strumenti (*tools*) sono gli stessi che

hanno consentito agli internauti di accedere, come mai prima, all'informazione libera. Ciò significa che tutto dipende dall'uso che si fa di questi dati e da come, in base ad essi, gli algoritmi vengono strutturati. Se è così, vuol dire che all'algoritmo possono essere forniti non solo dei dati alterati dai bias, ma inattendibili, o falsi perché l'obiettivo potrebbe essere quello di creare disinformazione anche attraverso immagini e video inveritieri .

La questione della falsità di un'immagine e, in generale, quello della pervasività delle *fake news* appare tanto più dirompente quanto la loro attendibilità risulti confortata da un'immagine accompagnando la nostra progressiva lontananza dalla realtà, il bacio di Giuda è quello che riceviamo (Joan Fontcuberta) .

La questione è anche politica, perché l'uso sempre più intensivo dell'intelligenza artificiale anche attraverso la produzione di fotografie immaginarie ci allontana non solo dalla realtà, ma da un senso critico che l'occhio deve esercitare per preservare la mente dai tranelli che sono tanto più frequenti quanto più si radica in noi una certa attitudine al consumo delle immagini e ad atteggiamenti narcisisti degli internauti, più propensi a credere semplicemente a ciò che vedono.

Questa tendenza potrebbe, nel tempo, rilevarsi fatale perché capace di creare veri e propri mondi virtuali ed irreali, destinati a raggiungere ed addomesticare al consumo e al traffico digitale gli strati della popolazione meno dotati di strumenti culturali capaci di reagire a questo fenomeno di istupidimento (dumbing down), riservando ai più abbienti la fruizione diretta di esperienze reali: il fenomeno dei viaggi sulla luna di Jeff Besos e la stessa tragedia del Titan diretto al relitto del Titanic sembrano dimostrarlo, così i meno dotati per capire l'inganno esorcizzano la propria ignoranza affidandosi ai nuovi sciamani.

Così sembriamo condannati ad un esistenzialismo *on line* dove i dati ci vengono continuamente sollecitati, condannati come siamo a riempire, anche per operazioni del tutto banali, schede, scaricando sempre nuove App da aggiornare di continuo ed, ogni volta, avvertiamo il fastidio dell'assenza di un'interazione reale con un nostro simile e ci sentiamo nel pericolo costante dell'assenza di una condivisione reale. Forse è questa la genesi della ragione per cui oggi nessuna organizzazione è in grado di produrre un cambiamento o di creare quello che si chiamava un *sensemaking,* ossia la ragione di stare insieme, il suo senso mentre dietro l'angolo vi è il pericolo

costante di una omologazione selvaggia del pensiero che crea, a sua volta polarizzazione delle differenze sociali, consumismo esasperato, creazione di desideri e necessità di emulazione che prima non esistevano

Noi stessi, nel nostro rapporto quotidiano con il nostro telefono, siamo portati a pensare un po' distrattamente che i *social* hanno influenzato il nostro modo di pensare la vita in maniera subdola con il solo scopo di generare profitti in favore dei grandi *gatekeepers* che praticano l'illusionismo facendoci credere che l'iperconnessione sia dispensatrice di democrazia, ossia ci proietti in un mondo dove tutti saranno protagonisti e dove tutto può accadere, mentre ci ipnotizzano con la pubblicità e controllano i nostri spostamenti. Ricordate le biciclette quasi gratis per girare in centro storico, poi gettate da qualcuno nel Tevere o rubate? Non costavano niente perché ciò che contava, per l'azienda cinese dispensatrice della locomozione ecologica, erano i nostri spostamenti destinati a creare preziose mappe di orientamento per nuovi *business*.

Nel frattempo che cosa accade in Italia? Secondo il Garante privacy nella raccolta dei dati necessari all'addestramento dell'algoritmo mancherebbe un'informativa agli utenti e a tutti gli interessati i cui dati vengono raccolti da OpenAI, e sarebbe deficitaria "una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati personali".

Sappiamo che il nostro Garante della privacy ha disposto, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti della statunitense OpenAI, azienda cui fa capo chat GPT, ossia una tecnologia software capace di simulare una conversazione tra umani, aprendo un'istruttoria avente per oggetto l'utilizzo dei dati personali da parte di questa *chatboat*.

Da aprile di quest'anno l'applicazione, con gli adattamenti richiesti dal Garante, si è riaffacciata sul Web con cancellazione dei dati raccolti e non utilizzati intesi come paletti messi al suo uso indiscriminato ai fine del *training*.

A sua volta, in Unione europea, si discute dell'AI Act, ossia del regolamento destinato a disciplinare l'uso indiscriminato della biometria del riconoscimento facciale e fare chiarezza sull' implementazione, attraverso la raccolta dei dati, dell'intelligenza artificiale generativa. Se n'è parlato al Parlamento europeo a metà giugno attraverso l'approvazione il 14 giugno 2023 dell'Artificial Intelligence Act, secondo lo statuto dei diritti dell'UE e destinato ad entrare in vigore nel 2025.

Il testo è stato definito come una novità mondiale dove l'attivismo europeo si è distinto rispetto ad ogni altro paese, destinata a moralizzare l'imperversare delle applicazioni sopra indicate, ossia chat GPT, Open AI e Bard, vietandole laddove non sia certa la loro ascendenza generativa in AI.

Nel frattempo, Google sta sperimentando la sua chatbot sperimentale, battezzata "Bard", ma non in Europa.

Ciò che, però, ancora manca è una responsabilizzazione collettiva in tema di cultura di protezione dei dati personali, specialmente da parte delle aziende che utilizzano il software di AI affidandosi a ditte esterne le quali non sono in grado di controllare, quali committenti, il rispetto della normativa sulla raccolta di dati.

Esiste, poi, un problema immane - simile ad una statua sepolta - di cui intuiamo, per ora, solo una parte della testa, ossia che l'intelligenza artificiale divorerà intere categorie di lavoro sostituendosi ad esse. Nel tempo, la prima conseguenza sarà non solo disoccupazione e povertà, ma presto o tardi verrò meno l'esistenza stessa di uno Stato che si basa, per esistere, sulla produzione di ricchezza e la distribuzione di essa, mentre settori interi di servizi fondamentali, come sanità e istruzione, non saranno più finanziabili e saranno canalizzate verso l'imprenditoria privata che li somministrerà a costi non alla portata di tutti, meno che mai disponibili per masse indifferenziate di forza lavoro facilmente rimpiazzabili con sistemi di intelligenza artificiale a costi decisamente inferiori. Per costoro non resterà che il sostentamento universale di Stato, (finché sarà possibile) che li priverà di ogni prospettiva di miglioramento e li declasserà, definitivamente, al rango di docili consumatori di quel poco che rimane disponibile nelle città divenute circo: concentrazione sul corpo, alimentazione compulsiva e ricerca, sulla rete divenuta prigione, un'impossibile visibilità. I più anziani, come suggeriva un governo di qualche anno fa, se fa troppo caldo e non se la sentono di passare la giornata sul web o non possono permettersi né vacanze, né condizionatore, potrebbero trascorrere la giornata dentro i supermercati in compagnia delle merci refrigerate, al resto ci pensa AI.