Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano

Gianluca Boleto
Head of Artificial Intelligence & Co-Founder @ Hodlie

September 19, 2023

Abstract

Il presente documento si pone come una veloce valutazione su quali possano essere le opportunità, ma soprattutto i rischi concreti da vigilare, di una diffusione massiva dell'utilizzo di strumenti basati su Intelligenza Artificiale all'interno del tessuto produttivo italiano. La visione proposta rappresenta la prospettiva di un sistematico utilizzatore di queste tecnologie, sia da un punto di vista personale, che soprattutto professionale, nella realizzazione di sistemi innovativi che possano creare valore all'interno di nuove imprese. A tal riguardo, il mio approccio con l'intelligenza artificiale è iniziato circa otto anni fa, quando iniziai a studiarne i fondamenti in ambito universitario. Successivamente, la applicai in lavori di ricerca pubblicati su importanti riviste di settore. Da allora, ho continuato a utilizzarla personalmente e lavorativamente, ponendola al centro del progetto dell'attuale Start-up di cui sono fondatore. Lo scopo finale del presente documento è quello di fornire un parere, da esperto del settore, sulle possibili modalità di regolamentazione di questa tecnologia rivoluzionaria, al fine di non impedirne l'utilizzo, la diffusione o lo sviluppo.

1 Svolgimento

L'intelligenza artificiale rappresenta uno degli strumenti più innovativi, potenti ed efficaci presenti sul panorama tecnologico mondiale. Sebbene il concetto di intelligenza simulata da automi sia diffuso da parecchi decenni nell'immaginario collettivo, a livello pubblico e mediatico se ne è sempre parlato scarsamente, lasciando a film con scenari distopici la narrazione di tale argomento. Con l'avvento di strumenti diffusi massivamente, quali Chat-GPT ma non solo, nell'ultimo anno si è finalmente portato il tema al centro dell'attenzione, e con esso la necessità di restare al passo con l'innovazione tecnologica a livello normativo. A tal riguardo, mentre il resto del mondo spinge fortemente sul perfezionamento e sullo sviluppo modellistico dell'AI, l'Europa si è mossa in anticipo sulla relativa regolamentazione. Invero, a due anni di distanza dalla prima proposta, il 14 giugno 2023 il Parlamento europeo ha approvato l'AI Act, la prima legislazione sull'Intelligenza Artificiale.

Con l'AI Act, l'Unione Europea ha voluto, in particolare, evidenziare la necessità di rimuovere il velo di opacità che spesso giace sopra all'AI Generativa. La priorità per il Parlamento è stata quella di assicurarsi che i sistemi di intelligenza artificiale europei siano sicuri, ma soprattutto trasparenti e tracciabili. Si è reso pertanto obbligatorio, per i creatori di strumenti basati su AI generativa, di adempiere ad alcuni obblighi di trasparenza, quali:

- la pubblicazione dei dati (con tanto di relativo Diritto d'autore) utilizzati per l'addestramento dei modelli;
- l'impossibilità di generare contenuti illegali da parte dei modelli stessi;
- l'obbligo nel rivelare che il contenuto è stato prodotto da AI.

In tal senso l'AI Act, volutamente o meno, ha posto l'accento su uno dei possibili limiti, o rischi, che una normativa sull'AI poco "pratica" possa incontrare: la distinzione tra contenuti realizzati da AI, o meno. Sebbene infatti la normativa abbia reso obbligatoria la rivelazione del creatore di contenuti prodotti da AI, evidenziando così la differenza tra contenuti generati dall'uomo rispetto a quelli generati da sistemi intelligenti, un'ulteriore distinzione da tenere in considerazione, non sempre evidente, è quella tra contenuti realizzati da AI, e quelli generati da sistemi "non intelligenti".

Concretamente, facendo riferimento a strumenti meno complessi della Generative-AI (quali Machine Learning, o Reti Neurali poco "profonde"), il confine tra Intelligenza Artificiale e sistemi informatici adeguatamente predisposti per uno specifico scopo è spesso nebuloso e poco apprezzabile, soprattutto dal punto di vista di un osservatore esterno, che non può accedere al codice sorgente di tale servizio. Pertanto, il rischio in tal senso sarebbe quello di confondere le due tipologie di servizio, o ancor peggio non riuscire a dimostrare efficacemente le differenze tra le stesse, imponendo una regolamentazione troppo limitante, o al contrario per nulla restrittiva.

Di fatto però, volendo porre l'accento solamente sui contenuti creati tramite l'AI Generativa, il rischio è quello di lasciare non regolamentate alcune tecnologie che si basano anch'esse su AI, ma che sono rivolte alla fruizione di servizi o prodotti i cui contenuti non sono direttamente generati da AI.

Oltretutto, la logica del "self-proof" è notoriamente poco efficace su larga scala, rispetto a un organo di vigilanza autorizzato e competente nel normare, e ancor di più vigilare, l'utilizzo di tecnologie innovative. Relativamente a ciò, si pone come assolutamente necessaria la consulenza (se non direttamente la presenza) di personale esperto della tecnologia all'interno del suddetto organo. Questo poiché è di fondamentale importanza che, a predisporre una normativa nazionale, ci siano anche esperti e utilizzatori dell'Intelligenza Artificiale, per poterne tutelare le potenzialità, senza limitarne gli utilizzi.

In una logica di semplificazione della normativa da proporre, si potrebbe mettere in luce l'origine e le caratteristiche dei dati che vengono utilizzati per l'addestramento dei modelli. Infatti, tutti i modelli di Machine Learning o Deep Learning, anche quelli soggetti a "human-feedback" come quello proposto in Chat-GPT, basano interamente la loro efficacia sulla quantità, la qualità e la rilevanza dei dati in input.

In concreto, qualsiasi società che agisce legalmente durante il processo di raccolta e trattamento dei dati, ha la possibilità di dimostrare in qualsiasi momento l'origine degli stessi, e il trattamento a cui sono sottoposti. Se questo processo fosse reso obbligatorio, nel momento in cui si fosse chiamati a rispondere dell'origine dei dati presso un preposto organo competente, in qualità di creatori di servizi o contenuti basati su AI, si potrebbe dimostrare la natura dei dati stessi, mostrandone la fonte di origine, senza dover scomodare la tutela della privacy delle informazioni coinvolte, poiché non si è chiamati a mostrarle qualitativamente. Così facendo, si porrebbe al centro dell'attenzione ciò che realmente determina le caratteristiche dei servizi basati su AI (n.d.r.: ovvero i dati coinvolti durante la fase di addestramento), senza rischiare di pubblicare informazioni confidenziali circa la natura della tecnologia adottata, il tutto regolato da un ente il cui scopo sia quello di normare i dati, e il loro utilizzo.

Infatti, le macchine e i sistemi informatici sono indubbiamente molto precisi e veloci, ma sebbene siano chiamati "intelligenti", rappresentano degli strumenti di per sé "stupidi". Concretamente, questi possono generare output circoscritti unicamente alla semantica del proprio processo di addestramento. Nonostante ciò, pubblicamente l'AI è spesso erroneamente percepita come uno strumento in grado di ribellarsi al volere del proprio creatore, ma attualmente ciò è ancora molto distante dalla realtà dei fatti. Tuttalpiù, può iniziare a generare output sconnessi, a causa di dati in input gestiti malamente, o non filtrati alla radice. Sarebbe sbagliato pensare che questa tecnologia possa, al giorno d'oggi, sviluppare un ragionamento proprio, o ancor più generare emozioni e agire seguendo i propri istinti.

Pertanto, il panorama attuale, per quanto si stia sviluppando con una velocità impressionante che obbliga qualsiasi Stato ad adoperarsi per cercare di restare al passo, è ancora ben lontano dal creare un'intelligenza senziente e sensibile.

Al tempo stesso, l'incredibile velocità di diffusione di questa tecnologia rende inevitabile monitorarne l'utilizzo, poiché un suo errato e inconsapevole impiego può comportare gravi problematiche a coloro che ne usufruiscono.

Da un punto di vista dell'utilizzatore finale invece, come discusso durante l'incontro avvenuto nel Senato Statunitense il 13 settembre 2023 sul tema dell'AI (o almeno secondo quanto trapelato), sarebbe importante che l'utente, usufruendo di determinati servizi o contenuti prodotti da AI, ne diventasse anch'esso responsabile in prima persona, potendone dimostrarne l'origine. Una normativa del genere, che in un certo senso prosegue il percorso introdotto dall'AI Act, non si limita a garantire i "Diritti d'autore" del contenuto generato da AI, ma punta a responsabilizzare chiunque voglia utilizzare tale tecnologia per finalità sociali, lavorative o educative. Seguendo questa logica, la direzione da adottare è quella di monitorare l'utilizzo e la diffusione di questa tecnologia, ma non limitarne il relativo sviluppo.

In conclusione, il rischio più concreto al quale ci si affaccia oggi è relativo alla velocità esponenziale di sviluppo dell'Intelligenza Artificiale, in particolare di quella Generativa. Dunque, il problema da affrontare è legato alla diffusione di massa di una nuova tecnologia facilmente accessibile, ma la cui fruizione consapevole è ridotta ancora a un ristretto numero di individui. Personalmente ritengo fondamentale evitare di rallentare il processo di sviluppo e di ricerca in questo ambito, ma altresì favorire la spinta imprenditoriale del nostro Paese tramite l'utilizzo di questa tecnologia.