GIUSTIZIA INSIEME

Diritto e innovazione

Il Garante della privacy sbloccherà ChatGPT? di Giuseppe Sepe

di Giuseppe Sepe

26 aprile 2023

Quando l'intelligenza artificiale incontra (e si scontra con) il diritto

Non ha generato molto entusiasmo il provvedimento[1] con il quale, lo scorso 30 marzo 2023, il Garante per la protezione dei dati personali ha - in via di urgenza - provvisoriamente limitato il trattamento dei dati personali degli utilizzatori italiani di ChatGPT, di fatto determinando il blocco dell'operatività del servizio, sotto minaccia di sanzioni amministrative e penali (art. 170 del codice per il trattamento dei dati personali).

Il Garante della privacy italiano è stato, nel panorama internazionale, pioniere nell'imporre uno stop del chat-bot, attirandosi un bel po' di critiche, talune delle quali probabilmente infondate, rispetto ad altre più sottili e pertinenti[2].

Se le principali violazioni riscontrate dal Garante giustificavano evidentemente l'apertura di un'istruttoria (ad esempio l'assenza di verifica dell'età anagrafica degli utenti, che non impediva l'accesso alla piattaforma di minori di anni tredici, la mancata predisposizione di apposita informativa sulla raccolta e le finalità del trattamento dai personali, la inesistente possibilità di incidere sul trattamento mediante richiesta di rettifica, correzione, distruzione dei dati) altre obiezioni sono invece apparse, a taluni commentatori, come frutto di un approccio di tipo conservatore o meglio, figlio di un grande fraintendimento ma, forse, o piuttosto, pieno di problematicità inespressa.

Ci si riferisce alla parte del provvedimento in cui il Garante contesta agli sviluppatori "*l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT*", e poi laddove rimarca la possibile inesattezza del trattamento, *"in quanto le informazioni fornite da ChatGPT non sempre corrispondono al dato reale*".

Sotto tale profilo, ciò che il Garante sembra valutare criticamente costituisce proprio il *cuore* dei modelli di linguaggio di grandi dimensioni (LLM). Questi ultimi, tuttavia, non hanno lo scopo di garantire la "certezza del risultato" o la "esattezza della risposta" bensì quello, ben diverso, di imitare l'utilizzo del linguaggio umano restituendo all'interlocutore una risposta plausibile, coerente, aderente al testo, espressa in linguaggio naturale.[3]

In altre parole un "aggeggio" come ChatGPT non è un'enciclopedia da cui si possa tirare fuori un risultato scientificamente esatto ma è, per ora, un insieme di codici miranti ad intuire le ricorrenze statistiche insite negli elementi testuali introdotti dall'utente e consegnare risposte coerenti sulla base di un'analisi probabilistica (una previsione) basata su un'enorme massa di dati, che il sistema già conosce, ma di cui non comprende assolutamente il significato.[4]

Si tratta dunque di modelli statistici che scompongono il testo in "token" (non assimilabili a dati personali, costituendo meri frammenti di parole, di per sé privi di senso compiuto) e sono in grado di svolgere previsioni su quali elementi testuali potrebbero ricorrere, sulla base di parametri come la *temperatura* che "regola il livello di casualità e probabilità nella scelta del prossimo token da inserire nel testo".[5]

All'aumentare della *temperatura* corrisponde un aumento dell'inaccuratezza e quindi di *creatività* del modello che sarà in grado di restituire output più stravaganti ma anche, magari, più innovativi e utili.

Mediante il dialogo con l'operatore il modello può perfezionare le risposte e dunque "auto apprendere" ma questo è esattamente un punto di forza dell'AI generativa e non, come il Garante lascerebbe credere, la sua debolezza. Paradossalmente, quindi, la prospettiva tradizionale di protezione giuridica del dato sembra confliggere con *l' in sè* dello strumento tecnologico che si nutre di input testuali, trasformati in token, lavorati e tradotti nuovamente in testo, migliorando di volta in volta il processo di apprendimento.

Non vi è dubbio che le "risposte inesatte" (inaccuratezza dell'Output) possano, sotto un diverso angolo visuale, distorcere la verità storica e produrre, se mal usate, disinformazione o anche rivelarsi lesive della onorabilità, identità personale di soggetti specifici così determinando

l'insorgere di possibili contese (sono già note, ad esempio, iniziative legali promosse a causa di informazioni inveritiere diffuse dal Chatbot, come il caso del Sindaco australiano Brian Hood[6]).

Ciò che potrebbe derubricarsi ad “effetto collaterale” dell’impiego della intelligenza artificiale, è esattamente il motivo per cui diversi studiosi, filosofi e giuristi, lungi dal voler impedire lo sviluppo di simili tecnologie, affermano la necessità di un’appropriata disciplina normativa in grado di accompagnare il processo di “design”, cioè la fase progettuale, lo sviluppo (development) e l’utilizzo degli applicativi anziché limitarsi a concepire tardivamente rimedi e correttivi all’uso improprio della tecnologia.[7]

E' chiaro, insomma, che tra una visione problematica, prudente e un approccio innovatore e “fuori dalle regole” si coglie una certa distanza che deve in qualche modo essere colmata anche grazie all’indagine giuridica che suggerisce di inserire le nuove tecnologie e segnatamente quelle che fanno uso della intelligenza artificiale in una nuova cornice normativa che superi i confini nazionali, allo scopo di garantire il rispetto dei principi fondamentali di tutela della persona umana non solo con riferimento al trattamento dei dati.[8]

Cos’è allora che sorprende in positivo dell’intervento del Garante? Che in breve tempo gli opposti quanto (apparentemente) inconciliabili punti di partenza si sono riavvicinati ciascuna delle parti facendo dei passi verso l’altra. La sviluppatrice Open AI impegnandosi a prendere in considerazione ed elaborare soluzioni per risolvere i punti critici segnalati e il Garante preannunciando la sospensione dell’efficacia del provvedimento di limitazione provvisoria qualora le prescrizioni, dettate lo scorso 11 aprile, trovino attuazione.

Ma quali sono le prescrizioni dettate dal Garante?[9] In estrema sintesi, pubblicare sul sito un Informativa che spieghi le modalità di trattamento, la logica del trattamento, i diritti spettanti agli interessati, nonché la previsione di uno strumento di "opposizione" e correzione o cancellazione dei dati eventualmente "inesatti" trattati (tanto sulla base del Regolamento generale sulla protezione dei dati, Reg UE 2016/679); modificare la base giuridica del trattamento dei dati eliminando il riferimento al "contratto" e assumendo viceversa il "consenso" o il "legittimo interesse"; nonché implementando uno strumento per il "diritto di opposizione al trattamento dei dati"; implementare strumenti di "age verification" che servano a bloccare l'accesso ad infra-tredicenni in assenza del consenso dei genitori. In ultimo promuovere una "campagna di informazione" presso la popolazione allo scopo di informare "le persone" sul fatto che i loro dati personali possono essere stati "raccolti" e "trattati" per l'addestramento "degli algoritmi", ecc.

Se questi punti saranno, come sembra, accettati e messi in opera dalla società sviluppatrice del software, il divieto dovrebbe, entro la fine di aprile 2023, venir meno e consentire la ripresa del servizio. Ma la difficile convivenza tra essere umano ed AI è soltanto all'inizio.

[1] **https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870832**

[2] Nelle settimane successive al 30/3/23 anche altri paesi europei, come Francia, Spagna e Germania, hanno avviato istruttorie finalizzate a chiarire i punti di frizione tra il GDPR e il trattamento operato da OpenAi. Il Comitato europeo per la protezione dei dati (EDPB), ha poi deciso di lanciare una task force su ChatGpt: **https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en**

3 Su natura, funzionamento e limiti dei LLM v., su questa rivista, l'articolo di F. Pilla: **Quali impatti avranno su di noi i Large Language Models e CHAT GPT** ; vi sono molti articoli di divulgazione scientifica, tra questi, ad esempio: https://www.mlq.ai/what-is-a-large-language-model-llm/

[4] Le contestazioni del Garante sotto questo aspetto denoterebbero una "*una limitata comprensione della natura e del funzionamento dei modelli di intelligenza artificiale*", cfr. **Giuseppe Vaciago e Gianluca Gilardi, Stop a ChatGPT, il Garante contesta "inaccuratezza" dell'output e trattamento dei dati personali**; **R. Pareschi, ChatGPT e il paradosso del censore.**

[5] https://ilariopanico.it/intelligenza-artificiale/temperatura-gpt-3-cos-e/

[6] https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/

[7] **Giuseppe D'Acquisto, Chatgpt e AI, regolamentare la responsabilità o l'efficienza è la prossima sfida** ; **Franco Pizzetti, ChatGpt: senza diritti siamo nudi davanti all'intelligenza artificiale**-artificiale/ ; **https://ilbolive.unipd.it/it/news/perche-chatgpt-ha-bisogno-regole**; Federico Cabitza, Deus in machina? L'uso umano delle nuove macchine, tra dipendenza e responsabilità, Bompiani, 2021.

[8] **https://www.agendadigitale.eu/sicurezza/privacy/pizzetti-chatgpt-senza-diritti-siamo-nudi-davanti-allintelligenza-artificiale/** ; cfr la proposta di regolamento del Parlamento europeo in tema di intelligenza artificiale (Artificial Intelligence Act), **https://eur-lex.europa.eu/legal-**

content/EN/TXT/?uri=celex:52021PC0206

[9] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702