

Chat GPT e la sfida della regolamentazione normativa

di Giovanna Pistorio

Aprile 2021. Per la prima volta nella storia, il Parlamento finlandese chiama in audizione un'applicazione di intelligenza artificiale: chat GPT. Dopo una serie di domande simula una possibile scelta di spesa pubblica: finanziare una pillola per curare il cancro o una pillola che fa vivere i gatti fino a cento anni. La domanda è paradossale, ma la risposta inquietante. Chat GPT suggerisce di sostenere i gatti. Quando viene interrogata sul perché, la motivazione è lapalissiana, inquietante, ma razionale nell'universo logico in cui si muove Chat GPT: i gatti sono più numerosi dei malati di cancro. È il confine, non troppo labile, tra razionalità e ragionevolezza che separa le forme di intelligenza umana dalle intelligenze artificiali. Almeno fino ad ora....

Chat GPT nasce nel maggio 2020. È una piattaforma *Generative Pre-trained Transformer*, come indica la sigla nel nome. Sviluppata dalla società statunitense OpenAI, rappresenta la forma tecnologica più avanzata per la conversazione con una macchina.

In soli due mesi raggiunge cento milioni di utenti. Utenti che ad essa si rivolgono per le più svariate esigenze: dalla digitazione predittiva alle traduzioni automatiche passando per sintesi o analisi del contenuto di testi. L'efficienza e la rapidità affascinano a tal punto, da sacrificare finanche verità e ragionevolezza.

In Italia il 31 marzo 2023 l'Autorità garante per la Protezione dei dati personali rileva alcune violazioni del Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea. Pare infatti che tale piattaforma sia priva di un'informativa agli utenti i cui dati vengono raccolti; non abbia una base giuridica che legittimi l'immissione e la conservazione massiccia dei dati; non predisponga meccanismi di protezione a tutela dei minori.

Il Garante dispone, quindi, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI. Blocco, peraltro, facilmente aggirabile con una semplice VPN che ti fa sembrare non connesso dall'Italia.

Comunque, almeno nella forma, il nostro Paese, insieme a Cina, Corea del Nord, Russia e Iran, rimane privo del servizio.

Una misura proibitiva o protezionistica?

Un dubbio sul quale si interrogano anche oltralpe e oltreoceano.

Francia, Germania e Irlanda sono pronti a seguire l'Italia se necessario per garantire maggiore sicurezza nella protezione dei dati, a fronte dei rischi che Chat GPT pare provocare.

Contestualmente, negli Stati Uniti si discute sull'opportunità di bannare TikTok, nell'ambito di un'attività più ampia volta a inibire tutte le operazioni considerate una minaccia alla sicurezza. È dei giorni scorsi la notizia relativa all'intenzione del Parlamento europeo di proibire l'uso dell'app ai propri dipendenti.

In Italia, la sospensione è stata comunque temporanea perché il 28 aprile 2023, dopo che OpenAI ha affermato di conformarsi alle indicazioni del Garante, apportando alcune modifiche, Chat GPT torna ad essere operativa.

Molte le questioni che il caso suscita: dai dubbi sull'effettività, in termini di sicurezza, delle misure apportate da OpenAI, alle difficoltà di più ampio respiro in merito alla garanzia dei diritti nell'era delle nuove tecnologie, fino al più complicato problema della regolamentazione, con il diritto, delle forme di intelligenza artificiale.

Lo sviluppo del digitale riaccende i riflettori sul delicato rapporto tra sicurezza e privacy.

Sono due bisogni, entrambi ancestrali, che, legati da un comune fondamento, vale a dire il timore dell'aggressione, conducono l'uomo verso due strade originariamente antitetiche: la *socialità*, ovvero la naturale «inclinazione ad associarsi» che induce l'uomo all'aggregazione, a fronte della forza che solo il gruppo è in grado di fornire, e la *asocialità*, ovvero quella «forte tendenza a dissociarsi» che spinge l'uomo a nascondersi per meglio salvaguardare la propria incolumità, intimità, integrità (Kant).

Quando lo sviluppo delle nuove tecnologie irrompe sulla scena, il sistema si scardina. La rivoluzione digitale consente agli algoritmi di forgiare la realtà fisica e intellettuale dell'uomo, incidendo sul modo in cui questi, come organismo informazionale (*infor*g), si relaziona con gli altri e con sé stesso in un ambiente *onlife* del tutto nuovo e in costante evoluzione (Floridi).

Molteplici e indiscusse le potenzialità che l'inarrestabile sviluppo delle tecnologie dell'informazione determina: dalla velocizzazione della comunicazione, alla globalizzazione delle relazioni, all'accrescimento delle conoscenze. Le meraviglie dell'intelligenza artificiale consentono di archiviare, sistemare una quantità significativa di dati. Tuttavia, aumentano anche i rischi. Sequenze di algoritmi penetrano più o meno silenziosamente nella vita di ciascun individuo, indagando nei settori più disparati: dalla salute, alle scelte economiche, agli interessi personali, alla potenzialità criminale, realizzando una precisa profilazione del singolo e della collettività, tale da consentire peraltro di orientare scelte di natura repressiva o di incidere sulla c.d. predittività delle decisioni giudiziarie. Una profilazione che avviene grazie all'immissione di informazioni nella rete – alle volte, peraltro, in modo non del tutto consapevole – e da cui deriva quella sempre più evidente e problematica forma di «alienazione contemporanea» (Palazzani). I dati così trasferiti nel mondo

virtuale possono essere utilizzati per attività non sempre lecite, se non addirittura criminali. Riemerge, dunque, l'esigenza di invocare l'«*habeas data*», quale «sviluppo di *quell'habeas corpus*», dal quale è nata la libertà personale (Rodotà). È in tale contesto che la privacy assume una connotazione del tutto nuova, più ampia, dinamica, includendo il diritto a poter conoscere, gestire, controllare i flussi informativi connessi ai dati personali, ovvero il c.d. diritto *all'autodeterminazione informativa* (Rodotà, Colapietro). In questa nuova veste, la privacy, oltre a un bisogno individuale, diventa un'esigenza della collettività, in quanto strumentale alla garanzia dei diritti e alla democraticità dell'ordinamento.

È nella sua dimensione di esigenza collettiva che la privacy interagisce, in un rapporto di stretta complementarità, con la sicurezza. In quest'ottica, la linea di confine diventa davvero labile fino quasi a scomparire del tutto, se esaminata rispetto alla sicurezza cibernetica, vale a dire a quell'insieme di attività volte a «proteggere la rete, i sistemi informatici, gli utenti di tali servizi», ovvero lo Stato e i suoi soggetti, dai pericoli derivanti dall'uso illecito, se non criminoso delle nuove tecnologie informatiche (Regolamento UE 2019/881).

Chat GPT ne è emblematica conferma. Dimostra che il diritto alla privacy non è più tanto e solo un diritto individuale, ma, in vista della funzione sociale che ricopre, concorre alla sicurezza, alla sicurezza dei diritti, quale obiettivo di carattere generale, meta di ogni Stato di diritto.

Privacy e sicurezza sono dunque due facce della stessa medaglia.

La medaglia che rappresenta la «sicurezza umana», ovvero quel poliedrico bisogno di protezione della generalità dei diritti dell'uomo, messi a rischio da una potenziale molteplicità di pericoli (De Vergottini). La conflittualità, oggi, non riguarda infatti solo le aggressioni, gli attacchi terroristici, ma anche i rapporti economici, l'ambiente, la sanità, l'informazione e la comunicazione, le forme di intelligenza artificiale, la gestione dei dati.

Siffatta eterogeneità rende necessaria, ma complicata, la regolamentazione.

Chat GPT è solo la punta dell'iceberg.

Oggi, viviamo nella rete: in un contesto in cui le nuove tecnologie dell'informazione e della comunicazione, l'internet delle cose, i droni, gli algoritmi, le auto autonome, le stampanti 3D, i social media, il GPS dimostrano quanto inarrestabile e rapido sia lo sviluppo del progresso e soprattutto quanto il diritto fatichi a seguirne il passo.

Sempre più spesso il diritto appare tardigrado e misoneista.

Nel passaggio epocale dal nomos della Terra al nomos del Mare, il diritto è chiamato a scardinare categorie che sembravano consolidate e a misurarsi con nuove e inedite problematiche (Celotto).

Occorre una regolamentazione interna, ma capace di interagire con quella sovranazionale, che sia in grado di operare in una realtà senza confini di spazio e di tempo, «dove la volontà si esprime oltre

gli Stati e oltre il diritto degli Stati» (Schmitt). È in tale contesto che si inserisce la proposta della Commissione europea del 21 aprile 2021 di elaborare una disciplina organica e condivisa con riguardo alle forme di intelligenza artificiale.

Serve una regolamentazione “tecnica”, globale, efficace. Chi conosce il diritto, non conosce solo il diritto e, dunque, se il legislatore non è un pessimo artista, deve avvalersi di consulenze ad hoc, rese da esperti, per plasmare la norma giuridica (Carnelutti). Il che non è affatto facile in un momento in cui anche il “pioniere dell’Intelligenza artificiale”, Geoffrey Hinton, esprime grande preoccupazione per l’incidenza dirompente che le nuove tecnologie hanno sul futuro dell’umanità e il Future of Life Institute sostiene la richiesta della sospensione di almeno sei mesi nell’addestramento dei più potenti sistemi di IA, per implementare la sicurezza nella progettazione e nello sviluppo. Né la regolamentazione diventa più agevole ricorrendo, a sua volta, a decisioni automatizzate o semiautomatizzate, nel dubbio che l’algoritmo non sia programmato o addestrato assicurando il rispetto della privacy, delle diversità culturali, del principio di eguaglianza e di non discriminazione.

Insomma, la regolamentazione delle nuove tecnologie con il diritto ricorda le fatiche di Sisifo: non solo è impegnativo raggiungere quell’equilibrato bilanciamento che la sicurezza dei diritti implica, ma arrivati in cima alla vetta, il masso rotola inesorabilmente a valle e l’evoluzione dei progressi tecnologici impone nuove sfide.