Intelligenza Artificiale generativa: alcune questioni problematiche*

Marco Bassini

Sommario

1. Introduzione

L'avvento su larga scala dei sistemi di Intelligenza Artificiale c.d. "generativa", attestatosi in tempi rapidissimi su un livello di capillarità e crescita senza precedenti, ha dato nuova linfa un dibattito già assai partecipato sulla necessità di una regolamentazione a prova di futuro. Invero, proprio i facili entusiasmi che taluni avevano coltivato salutando la scelta delle istituzioni dell'Unione europea di avviare un processo volto a coniare un quadro normativo *ad hoc* (l'AI Act) sembrano ora aver subito una tappa d'arresto a fronte delle difficoltà di tenere il passo dello sviluppo tecnologico. Queste carenze trovano una manifestazione evidente, del resto, nell'iter legislativo dell'AI Act, che ha visto il Consiglio e il Parlamento europeo tentare non senza fatica di rimediare "in corso d'opera" all'assenza di regole che potessero cogliere e affrontare le peculiarità dell'Intelligenza Artificiale generativa nel testo originale proposto dalla Commissione.
Questo intervento si diffonderà anzitutto sui profili di carattere generale inerenti all'ipotesi di una disciplina dell'Intelligenza Artificiale generativa, per poi concentrarsi, senza alcuna pretesa di esaustività, su alcuni punti nevralgici particolari che allo stato caratterizzano, nel settore dei media, il posizionamento di questa tecnologia.

* Il testo riproduce il contenuto della relazione svolta al convegno "Pluralismo e diritto d'autore al tempo dell'intelligenza artificiale" organizzato dall'Italian Chapter dell'International Institute of Communications in collaborazione con l'Autorità per le garanzie nelle comunicazioni, in Roma, 21 settembre 2023.

2. Profilo generale: la difficile costruzione di un quadro giuridico

La volontà delle istituzioni dell'Unione europea di restituire, con l'AI Act, un assetto giuridico adeguato alla complessità e poliedricità della tecnologia merita sicuro apprezzamento e in questo quadro l'intervento di natura "adeguatrice" che tanto Consiglio quanto Parlamento hanno proposto si segnala come uno sforzo encomiabile. Tale valutazione riesce peraltro corroborata dalla considerazione del fattore temporale che caratterizzerà la messa a regime prima e l'attuazione poi del nuovo quadro normativo, non destinato a una traduzione in pratica immediata (un tema su cui forse l'Unione europea dovrebbe interrogarsi, alla luce dell'estensione del suo intervento nell'ambito digitale negli ultimi anni). Se il disegno di aggiornamento merita condivisione, si deve tuttavia notare come la garanzia di certezza giuridica non possa passare per il tramite di una sostanziale giustapposizione di norme, come quella che il testo approvato dal Consiglio e quello licenziato dal Parlamento sembrerebbero proporre. La missione delle istituzioni non è certamente, del resto, quella di *filling the gap*; ma semmai quella di tracciare un delicato equilibrio tra le diverse istanze che ruotano intorno all'avvento e alla diffusione su larga scala dei sistemi di Intelligenza Artificiale. In questo senso, le norme di cui i testi di Parlamento e Consiglio propongono l'adozione con riferimento ai modelli generativi paiono non del tutto convincenti, in quanto traducono un approccio incentrato non tanto sulla disciplina dell'utilizzo della tecnologia in questione quanto sulla tecnologia *tour court*. Riaffiora, in questo frangente, traccia dell'ansia regolatoria che contraddistingue molti legislatori a fronte dell'innovazione tecnologica. Un intervento regolamentare così esclusivamente calibrato sulla tecnologia "in quanto tale", insensibile e indifferente invece agli utilizzi particolari, potrebbe del resto trovare giustificazione soltanto sull'assunto di una intrinseca quanto indimostrata sua "pericolosità". Questo approccio si rivelerebbe oltremodo inesatto se applicato all'Intelligenza Artificiale, specialmente *general purpose*, e ai c.d. modelli fondazionali, dove la possibilità di definire il livello di rischio e correlarlo alla tecnologia è *in re ipsa* sconfessata dalla pluralità e varietà di contesti di utilizzo *downstream*. Questa considerazione è corroborata, peraltro, dalle riflessioni già presenti in letteratura sulla difficoltà di costringere i sistemi di Intelligenza Artificiale generativa entro il rigido schema precostituito dall'AI Act e fondato su livello di rischio. Tali criticità hanno fatto ipotizzare, con riflessioni che parrebbero condivisibili, l'opportunità di ideare una categoria di rischio *ad hoc*, congegnata alla luce delle caratteristiche peculiari dei modelli fondazionali e dell'Intelligenza Artificiale generativa, e così slegata dalla preconcetta elaborazione racchiusa nelle categorie delineate dall'AI Act. Tale soluzione assicurerebbe maggiore flessibilità e promette di cogliere in modo più accurato il rischio insito in questa categoria tecnologica meritevole di una considerazione autonoma. L'argomento del superamento delle categorie di rischio individuate dall'AI Act avendo senz'altro a mente perlopiù l'Intelligenza Artificiale *special purpose* non può essere peraltro trascurato, a fronte delle significative implicazioni concorrenziali che si ricollegano all'apparato di obblighi derivante dell'AI Act. Allo stato, sebbene sembri scongiurato il pericolo di una pedissequa equiparazione dell'Intelligenza Artificiale generativa ai sistemi a rischio elevato (come invece nel te-

sto votato dal Consiglio), il reticolato normativo costruito intorno a questa tecnologia sembrerebbe farne *sostanzialmente* dei sistemi di tale natura. Trattare l'Intelligenza Artificiale generativa come la tecnologia più rischiosa, oltre probabilmente a non rifletterne accuratamente le caratteristiche, è operazione che – come accennato – non è immune da conseguenze sul piano concorrenziale: elevato è, infatti, il pericolo che a poter rispondere dei gravosi obblighi imposti agli operatori di questo segmento di mercato, e in particolare a fornitori e sviluppatori, siano nei fatti soltanto gli attori imprenditoriali più strutturati e dotati di copertura finanziaria, con inevitabili ripercussioni sul piano dello sviluppo dell'innovazione e del possibile ingresso di nuovi *player* nel mercato, che riuscirebbe con ogni probabilità scoraggiato.

3. La qualità dei dati come premessa per la generazione legale di contenuti (*passim*)

Passando ai profili particolari, un tema occupa una posizione nevralgica rispetto a tutte le questioni che, tanto nella prospettiva dei dati quanto in quella dei contenuti, emergono dallo sviluppo dell'Intelligenza Artificiale generativa: la qualità dei dati. Non è un caso che le problematiche principali, già denunciate da diversi commentatori, derivino vuoi dalla generazione di output contenutisticamente errati, che risalgono a informazioni inesatte magari perché non più attuali (le c.d. "allucinazioni"), vuoi dalla memorizzazione di informazioni a carattere personale che vengono "randomicamente" riproposte, talvolta senza alcun legame con l'oggetto dell'attività generativa. In termini di trattamento di dati e di elaborazione di contenuti si pone un comune problema di qualità dei dati, funzionale a evitare l'automatismo *garbage in, garbage out*. Si tratta di un nodo che non riguarda soltanto l'ambito del trattamento di dati personali (al quale è comunque affrancato dal principio di esattezza dei dati racchiuso nel GDPR, tra gli altri) ma che è foriero di significative implicazioni anche sul piano dei contenuti. Non è casuale che in letteratura si sia già sollevata, opportunamente, una riflessione in ordine all'opportunità di dettare specifiche garanzie a tutela dalla qualità dei dati, prescindendo dai rimedi già esistenti (ritenuti insufficienti) nella normativa sulla protezione dei dati.

4. L'applicabilità delle esenzioni di responsabilità per i fornitori di servizi digitali alle creazioni dell'Intelligenza Artificiale generativa

Svolta la doverosa premessa affidata al paragrafo che precede, è doveroso domandarsi quale sia l'impatto dell'Intelligenza Artificiale generativa sul quadro normativo inerente ai servizi digitali che di recente è stato confezionato dalle istituzioni dell'Unione europea, con l'adozione in particolare del Digital Services Act ("DSA", regolamento (UE) 2022/2065) e del Digital Markets Act ("DMA", regolamento (UE) 2022/1925). Prescindendo in questa sede dall'esame dei profili concorrenziali (senza tacere però la loro rilevanza e anticipando che criticità emergono anche rispetto all'applicazione del DMA

ai sistemi di Intelligenza Artificiale generativa), l'esigenza di considerare le norme contenute nel DSA trae origine dalla temuta capacità della tecnologia in discorso di produrre e disseminare non soltanto contenuti illeciti ma anche (e soprattutto) contenuti falsi (tra cui, per esempio, i c.d. *deepfakes*). Proprio la capacità dell'Intelligenza Artificiale generativa a prestarsi per questi scopi è all'origine delle preoccupazioni inerenti a un suo possibile uso per alimentare campagne d'odio o disinformative che potrebbero tradursi in effetti distorsivi sul piano democratico. Proprio il DSA è stato celebrato, forse con enfasi talvolta eccessiva, come il risultato di un profondo ammodernamento del quadro giuridico applicabile ai servizi digitali reso ormai necessario dalla conclamata obsolescenza della Direttiva sul commercio elettronico (direttiva 2000/31/CE). Come noto, quest'atto fa propria una matrice regolamentare già comune ad altre normative presenti (come il GDPR) e future (come l'AI Act), ossia l'approccio basato sul rischio. Addiviene a una differenziazione e specificazione a lungo attesa degli obblighi e delle misure di contrasto dei rischi che è calibrata sul tipo di servizio erogato e sul livello di rischio inerente. Proprio per questo, la riforma è stata salutata come un momento di svolta che impone alle piattaforme online di dimensioni elevate (c.d. VLOP, *very large online platforms*), tra cui i social network, obblighi più stringenti, anche in tema di trasparenza, rispetto alla moderazione di contenuti di terzi. Questo importante traguardo sembrerebbe però frustrato dall'avvento di un *novum* in grado di bypassare, almeno all'apparenza, le maglie delle prescrizioni esistenti.

È del tutto evidente che i modelli di Intelligenza Artificiale generativa non erano presenti alla mente del legislatore del DSA: non lo erano, del resto, nemmeno a quella del legislatore dell'AI Act che ha confezionato la proposta della Commissione. Parrebbe dunque inevitabile riconoscere che l'articolata trama normativa ora racchiusa nel regolamento non possa trovare applicazione rispetto alla creazione di contenuti derivanti dall'Intelligenza Artificiale generativa. Si badi: il DSA sarebbe comunque applicabile a tali contenuti quanto pubblicati da terzi su piattaforme online di grandi dimensioni, come un social network, o attraverso altri servizi che ricadono nell'ambito di applicazione del regolamento. Ciò che resterebbe esclusa è, invece, l'applicazione delle norme in questione agli sviluppatori o utilizzatori di Intelligenza Artificiale generativa. Per fare un esempio immediato: ChatGPT non potrebbe invocare alcuna esenzione di responsabilità rispetto ai contenuti generati.

Nonostante questa opinione dominante sia suffragata dalle intenzioni del legislatore, vi è in dottrina una tesi finora minoritaria che, pur riconoscendo che il DSA non è stato pensato perché trovasse applicazione ai sistemi di Intelligenza Artificiale generativa e ai soggetti della relativa *value chain*, ha evidenziato come sussisterebbero delle "pieghe" nel testo del regolamento che potrebbero giustificare una sua estensione anche oltre il perimetro dei servizi digitali come tradizionalmente identificati. Questo spazio interpretativo è stato ricavato dalla nozione dei motori di ricerca online fatta propria dal DSA. Si tratta, come noto agli addetti ai lavori, di una categoria "in cerca d'autore", che nel silenzio serbato dalla Direttiva sul commercio elettronico ha conosciuto declinazioni normative diverse tra gli Stati membri. Il DSA racchiude una definizione analoga a quella precedente, secondo cui è motore di ricerca online «un servizio intermediario che consente all'utente di formulare domande al fine di effettuare

ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto» (così l'art. 3, par. 1, lett. j) del DSA). Per effetto dell'adesione a questa definizione sarebbe possibile riscontrare alcuni punti di contatto tra la categoria dei motori di ricerca online e perlomeno alcuni sistemi di Intelligenza Artificiale generativa. Entrambi (motori di ricerca e sistemi di Intelligenza Artificiale generativa), infatti, fonderebbero il proprio funzionamento sull'input inziale (*prompt*) dei propri utenti, teso alla ricerca di informazioni sul web sulla base della parola chiave utilizzata. Entrambi, poi, sarebbero in grado di restituire i risultati *in qualsiasi formato* in cui possono essere trovate le informazioni relative al contenuto richiesto. E proprio su questo carattere di indifferenza rispetto alle modalità con cui il sistema restituirebbe il risultato desiderato dagli utenti fa perno l'interpretazione che vuole come possibile la riconduzione di alcuni sistemi di Intelligenza Artificiale generativa alla categoria dei motori di ricerca online, con conseguente possibilità di sottoporli alle regole previste per i VLOSE, ossia i *very large online search engines*.
La tesi che si è esposta poggia su un fragile elemento di ambiguità letterale e può essere avversata semplicemente richiamando la volontà del legislatore di dedicare il quadro normativo a una tipologia ben determinata di servizi digitali. Nondimeno, proprio la lettura audacemente proposta che è stata ora richiamata stimola la riflessione su un punto di auspicabile avanzamento del dibattito: l'applicazione del DSA agli sviluppatori di sistemi di Intelligenza Artificiale generativa sarebbe auspicabile?
A ben vedere, questa operazione, se perfezionata tramite un apposito disegno di riforma, potrebbe condurre a due risultati pratici non trascurabili.
Da un lato, dall'applicazione del DSA discenderebbe l'operatività dell'esenzione di responsabilità prevista per i fornitori di servizi allo stato assoggettati al regolamento. Un simile esito potrebbe apparire paradossale a chi ritenga che la creazione di output come testi, video o immagini sia equiparabile e indicativa di una attività editoriale e così dubitare delle ragioni per un regime giuridico che diverga dalle ordinarie regole in tema di allocazione di responsabilità per contenuti illeciti. Nondimeno, proprio nel contesto di un'attività generativa che abbisogna di continuo addestramento a fronte della possibilità di errori (allucinazioni?) pare che il sistema di *notice and action* che il DSA ha ereditato e rimodellato dalla Direttiva sul commercio elettronico ben si presti ad assolvere questa missione. Segnalando un contenuto illecito (o comunque inappropriato) agli sviluppatori di sistemi di Intelligenza Artificiale generativa, infatti, si potrebbe favorire un intervento sul processo che ha determinato la restituzione di un risultato non conforme all'ordinamento giuridico, al contempo delimitando il margine di applicazione dell'esenzione di responsabilità, che non potrebbe estendersi "oltre" il momento in cui sia stata portata a conoscenza l'illiceità del risultato generato. Ne gioverebbe, forse, anche la certezza del diritto.
Dall'altro lato, l'estensione delle regole contenute nel DSA, come è stato notato da chi ha proposto la tesi sopra richiamata, potrebbe favorire l'applicazione, perlomeno ai soggetti maggiormente strutturati (onde evitare conseguenze anticoncorrenziali) di più elaborati meccanismi di valutazione del rischio come quelli indicati all'art. 34 DSA. In

questo modo, peraltro, l'estensione del DSA risolverebbe forse un problema al legislatore dell'AI Act, impegnato nella faticosa ricerca di un punto di equilibrio.
Lo stesso problema potrebbe porsi, poi, negli Stati Uniti, laddove hanno peraltro sede numerosi attori imprenditoriali operativi anche in Europa. In questo senso, l'attuale schema della Section 230 del Communications Decency Act parrebbe non lasciare spazio ad alternative tra la qualificazione degli sviluppatori e fornitori di sistemi di Intelligenza Artificiale generativa come *information service provider* e *information content provider,* con quest'ultima opzione qualificatoria verosimilmente candidata – in assenza di interventi legislativi – a trovare supporto in eventuali contenziosi avanti alle corti statunitensi. L'*impasse* sull'opportunità di una riforma della Section 230 CDA si prolunga ormai da tempo e il dibattito potrebbe essere forse l'occasione per un suo superamento. Del resto, anche aderendo all'impostazione che ravvisa – non senza ragioni – negli attori in questione *information content provider*, vi sarebbe spazio per discutere l'opportunità delle conseguenze giuridiche (in termini di esclusione dell'esenzione di responsabilità in bianco accordata per contenuti diffamatori).

5. La riconducibilità dei prodotti di Intelligenza Artificiale generativa a tutela costituzionale

Vi è poi un convitato di pietra nel dibattito sulle questioni relative all'esatto inquadramento dei sistemi di Intelligenza Artificiale generativa entro la cornice normativa esistente: il tema della riconducibilità all'ambito di tutela della libertà di manifestazione del pensiero dei contenuti prodotti mediante Intelligenza Artificiale generativa. È un dilemma che si intreccia con l'ulteriore nodo, ben più dibattuto in tempi recenti, legato all'estensione ai contenuti prodotti da Intelligenza Artificiale generativa della tutela autoriale.
La domanda potrebbe apparire peregrina e forse mal posta, sol che si pensi che le maggiori preoccupazioni sono emerse, allo stato, rispetto alla produzione di contenuti falsi per supportare campagne disinformative o per danneggiare l'altrui reputazione (con ricorso, per esempio, alla tecnica dei *deepfakes*). Ulteriori dubbi potrebbero manifestarsi ponendo mente al fatto che le costituzioni, come quella italiana all'art. 21, sembrerebbero presupporre che le manifestazioni di pensiero tutelate siano ascrivibili a individui, peraltro esigendone l'identificabilità (l'art. 21 allude, infatti, alle manifestazioni del "proprio pensiero"). Parrebbe così eccentrico domandarsi se le creazioni dell'Intelligenza Artificiale generativa godano di tutela costituzionale come esercizio della libertà di espressione (ponendosi peraltro il problema, in parte analogo all'ambito del diritto d'autore, di discernere tra le ipotesi di utilizzo della tecnica come strumento da parte di persone fisiche "parlanti" e "autori" e quelle di "autonoma" creazione, non servente, dell'Intelligenza Artificiale generativa). La difficoltà di individuare un "parlante" (*speaker*) e di ricollegarvi *free speech rights* potrebbero così risultare argomenti decisivi.
Adottando una diversa prospettiva, tuttavia, si comprende come il tema si sia posto, seppure timidamente, in alcune riflessioni di autori statunitensi. È la prospettiva non del parlante, bensì dell'uditore, del cittadino che ha cioè diritto a informarsi e ricercare con-

tenuti, anche generati dall'Intelligenza Artificiale generativa. Ci si colloca in quello che la giurisprudenza della nostra Corte costituzionale ha indicato come il profilo passivo della libertà di informazione. In questo senso, riorientando la decodificazione del problema, ci si domanda se eventuali limitazioni previste dall'ordinamento alla creazione di contenuti mediante Intelligenza Artificiale generativa risulterebbero rispettose del dettato costituzionale. Il punto è naturalmente molto sentito nell'ordinamento statunitense, dove la libertà di espressione è ancora fermamente modellata sul paradigma del libero mercato delle idee ispirato dalla celeberrima *dissenting opinion* di Justice Holmes del 1919, fedele a una visione pluralistica e diffidente di ogni interferenza di matrice pubblicistica. Proprio il libero fluire e confrontarsi delle idee sarebbe ostacolato da previsioni che, in ipotesi, dovessero prevedere delle limitazioni *content-based,* ossia contenutisticamente sensibili, all'utilizzo dell'Intelligenza Artificiale generativa. Estendere la tutela del Primo emendamento, nella prospettiva del diritto a ricevere informazioni, al prodotto creato artificialmente segnerebbe un limite al potere di contrasto della disinformazione. Al contempo, però, come è stato notato, fungerebbe da salvaguardia rispetto a limitazioni di stampo meno liberale, quali eventuali repressioni del dissenso che i poteri pubblici intendessero perseguire anche nell'utilizzo dell'Intelligenza Artificiale generativa.
Confrontata con l'approccio europeo, questa prospettiva di inquadramento sembrerebbe difficilmente conciliabile con la lotta senza quartiere alla disinformazione che le istituzioni dell'Unione europea hanno inaugurato ormai da tempo. Tuttavia, un "assist" forse involontario nella direzione opposta, di un incontro con la sensibilità statunitense, sembrerebbe potersi cogliere nel disposto dell'art. 28b, par. 4, lett. b), del testo votato dal Parlamento europeo, laddove si prevede che i fornitori di modelli fondazionali utilizzati in sistemi di Intelligenza Artificiale generativa hanno l'obbligo di allenare e sviluppare tali modelli in modo da assicurare tutele adeguate contro la generazione di contenuti in *violazione del diritto dell'Unione europea* e senza pregiudizio ai diritti fondamentali, tra cui la *libertà di espressione* (enfasi aggiunte). Una lettura "in controluce" di questa disposizione, focalizzata sulla natura della disinformazione come contenuto non necessariamente in violazione di legge, sembrerebbe gettare insperatamente un "ponte" tra le sensibilità di Stati Uniti ed Europa.

6. Conclusioni

Le riflessioni esposte senza alcuna pretesa di esaustività rivelano la difficoltà di tracciare uno statuto giuridico adeguato a cogliere e riflettere la complessità intrinseca dell'Intelligenza Artificiale generativa. Difficile da collocare in uno scenario di rischio preciso, sfuggente a norme pensate in tempi recenti per servizi e mercati digitali, di incerta riconducibilità al perimetro di libertà costituzionalmente tutelate, l'Intelligenza Artificiale generativa lancia la sfida ai legislatori delle potenze tecnologiche. Una sfida importante, che si auspica non venga affrontata con l'ansia regolamentare altrove evidenziata da diversi commentatori e senza che la lotta per la sovranità tecnologica finisca per sacrificare diritti e innovazione.