

costruire il futuro

ANCE | BRESCIA

3/2024



Rivista bimestrale di ANCE Brescia

Tecnologie e cantiere edile: il quadro normativo

a cura dell'Avv. Chiara Micera

© riproduzione riservata



Avvocata Chiara Micera
Studio legale Micera

L'art. 5 del Gdpr, cioè il Regolamento europeo sulla privacy, recepito in Italia, chiarisce che per ogni trattamento dei dati è necessario avere una base giuridica valida, in assenza della quale ogni trattamento è illegittimo. Tale principio solleva diverse questioni e tra esse portiamo preliminarmente all'attenzione la questione di fondo: se è giuridicamente corretto "alimentare" gli algoritmi mediante l'acquisizione dei dati presenti "on line", immessi in rete con uno scopo diverso (si pensi alla Pa che pubblica graduatorie di concorsi pubblici, per finalità di ricerca, o anche di contenuti di natura creativa) rispetto a quello di sviluppare le attività imprenditoriale di privati.

Sul punto attendiamo il pronunciamento della giustizia statunitense per vertenza sul tema della violazione del diritto d'autore e per la concorrenza sleale promossa dalla testata giornalistica del NY Times contro OpenAi per avere "alimentato" il sistema di Ai con gli articoli on line, per poi produrre contenuti immessi in rete, di fatto, concorrenziali rispetto al giornale stesso, e comunque al mondo, un tempo avremmo detto, della "carta stampata".

La seconda questione è che quando l'algoritmo è "addestrato", cioè l'AI generativa, si pone il tema delle "allucinazioni", cioè riprodurre contenuti non veri, ma verosimili, perché non sono progettati per questo, quindi c'è un tema di affidabilità delle informazioni. Se l'utente non è adeguatamente consapevole di tale circostanza, o in alternativa, se nonostante ciò intende utilizzare detti contenuti, in quanto facilitatore di processi decisionali, ottimizzante dei costi (e quindi ritorna il tema del profitto), ne discende che un'intera catena di valore sarà vulnerabile,





Le criticità dell'applicazione dell'AI sono concorrenti con le potenzialità e gli impatti favorevoli dell'utilizzo, e il Legislatore si trova a fare i conti con un elemento dirimente per la gestione del fenomeno: i tempi dell'evoluzione tecnologica sono di gran lunga più veloci rispetto a quelli della normazione di un processo, che solitamente si basa sull'osservazione dello stesso

con comprensibili conseguenze (basti pensare al tema della sicurezza sul lavoro citato poc'anzi). A ciò aggiungasi il tema dei cosiddetti "rigurgiti", fenomeno per il quale il meccanismo di AI sottoposto a uno *stress* per l'inoltro di *prompt* (la sollecitazione per ottenere una risposta dall'AI), può immettere dati in suo possesso che ha raccolto *on line*, in contesti in cui non possono essere condivisi (ad esempio un ambiente di condivisione dei dati, o *Acdat*, nell'ambito della quale si attua la gestione informativa digitale), con probabile violazione della privacy, perché nel caso di specie, mancherebbe completamente il fondamento della base giuridica per il trattamento del dato.

Le criticità dell'applicazione dell'AI sono concorrenti con le potenzialità e gli impatti favorevoli dell'utilizzo, e il Legislatore si trova a fare i conti con un elemento dirimente per la gestione del fenomeno: i tempi dell'evoluzione tecnologica sono di gran lunga più veloci rispetto a quelli della normazione di un processo, che solitamente si basa sull'osservazione dello stesso.

Che cosa fare quindi *medio tempore* per mitigare gli effetti negativi?

I tentativi che stiamo osservando hanno un comune denominatore: affidarsi ai principi generali. Ora sappiamo che il legislatore deve poter valutare e bilanciare, esprimendo prevalenza dei diritti secondo un gradiente.

Il dibattito culturale in corso, come è noto, ha spesso invocato l'etica, quale "regolatore" primario dell'utilizzo dell'intelligenza artificiale; trattasi di un richiamo ai principi fondanti del diritto, ove i nostri "padri" del diritto romano, esprimono il presidio con il broccardo *boni mores*.

Ma la questione parrebbe più complessa, atteso che il fenomeno della digitalizzazione è ontologicamente transnazio-

nale, intercettando sensibilità di culture giuridiche molto diverse, sebbene la condizione di oligopolio dei detentori di queste tecnologie la riconduca, in realtà, a poche aeree del mondo, non solo geografiche, ma anche culturali.

Non a caso la legislazione internazionale registra la pubblicazione nel marzo 2023 da parte del Nist (National Institute of Standards and Technology – Agenzia del Governo degli Stati Uniti), un documento denominato "AI Risk Management Framework" e il 30 ottobre 2023, il Presidente Biden ha emanato l'Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. Inoltre, lo scorso 18 dicembre 2023 la Iso (*International Organization for Standardization*) ha emanato la Iso/Iec 42001 – Information Technology – Artificial Intelligence – Management System. Tali strumenti cogenti o volontari hanno un obiettivo: fornire strategie e misure per supportare lo sfruttamento dell'AI ai fini di ricerca, servizi alla persona e profitto, gestendo i rischi associati con l'obiettivo di garantire sicurezza e diritti fondamentali.

In previsione dovrà essere pubblicata la Iso 42005 "Information technology – Artificial Intelligence – AI system impact assessment", lo scopo è proteggere, nel corso di tutto "il ciclo di vita" di un sistema di intelligenza artificiale, aspetti quali: sicurezza, tutela, equità, trasparenza, qualità dei dati e qualità dei sistemi, al fine di creare un sistema di gestione dell'intelligenza artificiale (Aims).

Lo standard è stato redatto in maniera da facilitare l'integrazione con altri sistemi di gestione, il primo rappresentato da Iso/Iec 27001:2022 "Sistemi di gestione per la sicurezza delle informazioni", nonché la Iso/Iec 27701 del 2019 "Privacy Information Management", nonché la Iso 9001 del 2015



“Sistema della qualità”, ed altri ancora.

Il criterio con il quale si è approcciato il tema è il *risk management*: bisognerà individuare il livello di utilizzo dell’Ai nei diversi ambiti, e per ciascuno di essi, approntare misure di mitigazione del rischio, giungendo sino alla proibizione dell’utilizzo in alcuni casi, particolarmente sensibili (si pensi ad esempio all’industria bellica).

In Europa invece di recente è stato approvato un Regolamento denominato Ai Act, che dovrà completare il proprio iter circa entro due anni per l’entrata in vigore.

Trattasi di un più strutturato strumento legislativo, ispirato ai medesimi criteri del Gdpr in tema di privacy: la cosiddetta “accountability” e l’utilizzo dell’Ai cosiddetto “by default e by design”; in buona sostanza porre in capo ai soggetti la responsabilità non solo meramente giuridica, ma anche una dimensione amministrativa ed etica che promuove un decisionismo responsabile ispirato alla trasparenza. In sintesi: il documento mette al centro la tutela dei diritti e

la libertà dell’individuo e obbliga le aziende che sviluppano Ai a dimostrare che i loro prodotti non li violino e che sin dalla loro progettazione sono state poste in essere misure idonee in tale senso.

Si rende quindi necessaria una fase preliminare d’identificazione dei rischi noti, possibili e prevedibili con conseguenze sulla salute, sulla sicurezza e sui diritti fondamentali per la redazione di una valutazione d’impatto e per la conseguente redazione di stringenti protocolli per l’integrazione responsabile di sistemi e di un piano di mitigazione. Analogamente a quanto prevede l’art.35 del Gdpr e cioè la necessità in capo al Titolare del trattamento, quando lo stesso può presentare un rischio elevato per i diritti e le libertà individuali.

Gli ambiti esaminati sono molteplici, ma il Legislatore europeo si è molto soffermato sulle limitazioni ai sistemi di identificazione biometrica e l’obbligo di trasparenza per i sistemi tecnologici.

Tali documenti elaborati a livello internazionale, allo stato, sono sprovvisti di cogenza normativa, come dicevo, rappre-

Gli ambiti esaminati sono molteplici, ma il Legislatore europeo si è molto soffermato sulle limitazioni ai sistemi di identificazione biometrica e l’obbligo di trasparenza per i sistemi tecnologici

sentando meramente linee d’indirizzo ad esecuzione volontaria, nell’attesa che siano emanate dai rispettivi Stati o Organismi deputati. Sul punto, dobbiamo segnalare che, nel nostro ordinamento, lo scorso 23 aprile, il Consiglio dei Ministri ha approvato il disegno di legge sull’intelligenza artificiale, che ora dovrà essere sottoposto al vaglio del Parlamento. Nel frattempo, per gestire questa *vacatio legis*, si è proposto alle società produttrici di Ai di redigere un documento negoziale, un Codice di Condotta,

in cui le stesse si “autoregolino” per lo sviluppo e la diffusione di detta tecnologia.

Il tentativo è di evitare che le *industry* utilizzino il mercato come laboratorio, per la messa a punto via via dei loro prodotti, in una logica di profitto, ma senza la vigenza di un sistema di prevenzione prima e di sanzione poi, delle conseguenze dell’utilizzo.

I documenti “d’ispirazione” dovrebbero essere per l’appunto le fonti normative sopracitate, ed attraverso la redazione del Codice di Condotta, di fatto si chiede una preattuazione di detti principi su base volontaria.

Concludendo possiamo evidenziare che il quadro regolatorio attuale ha correttamente posto l’attenzione sulla tutela dei diritti fondamentali, cercando di disciplinare il contenimento dei diritti, ma esprime senza alcun dubbio, l’intento di non ostacolare lo sviluppo della tecnologia, anzi di favorirlo, attraverso l’introduzione di regole chiare e trasparenti. Perché il brocardo latino recita: “*In claris non fit interpretatio*”. Allora benvenuta Ai, anche in cantiere.