

Cose europee?*

Salvatore Amato

Professore in quiescenza di Filosofia del diritto - Dipartimento di Giurisprudenza, Università di Catania.

Mail: samato@lex.unict.it

Come potrebbe non alimentare l'insofferenza trumpiana per le "European things" l'AI Act con i suoi 180 "considerando", 113 articoli, 144 pagine, svariati allegati, infiniti richiami a precedenti regolamenti? L'AI Act non nasconde l'ambizione di assumere un ruolo centrale nel processo di governo delle nuove tecnologie e lo fa con una pretesa di esaustività e onnicomprensività alla cui effettiva applicazione gli stessi estensori sembrano non credere, se ricorrono sistematicamente all'espressione "should be": ho contato almeno 90 di questi "dovrebbero" nei diversi "considerando". Sembra impossibile sfuggire al dubbio che, alla realtà senza regole a cui si vuole porre rimedio, si stia contrapponendo un futuro di regole lontane dalla realtà. Tuttavia, credo ci siano validi motivi per mettere da parte l'accusa a questa regolamentazione di voler svuotare l'oceano con un bicchiere, riconducendo entro un quadro normativo definito l'orizzonte indecifrabile, variegato e complesso di un'intelligenza artificiale in continua trasformazione. Malgrado la perplessità sulla funzionalità normativa dell'impianto complessivo, le farraginosità burocratiche, gli ostacoli attuativi, l'indecifrabile impatto economico, vi sono due elementi che assumono un enorme valore etico e costituiscono un rilevante vincolo politico. Il primo è un dato meta-normativo: l'affermazione, con la coraggiosa presa di posizione sui

livelli di rischio, del primato della regolamentazione sulla pretesa autosufficienza della tecnica. Il secondo è una svolta ermeneutica: incentrare l'attenzione sull'identificazione e definizione del *loop*, del complesso circuito tecnico, industriale, economico e finanziario che incrocia e condiziona i valori umani. La premessa per comprendere la rilevanza del primo punto è l'attuale predominio del modello dell'*Effective Accelerationism*, sostenuto dalla maggior parte delle *big tech* e dalle pressioni del mercato. Si fonda sulla convinzione che l'unica via per risolvere i problemi e fugare i timori sia accelerare la spinta verso l'innovazione: solo la tecnica è in grado di controllare la tecnica; più investimenti, quindi, e meno regole. Non è un caso se i primi provvedimenti di Trump siano stati la cancellazione o la messa in discussione dei tentativi di Biden di seguire il modello europeo. Biden aveva emanato, nel 2023, l'*Executive Order* su *The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, per "affrontare i rischi più pressanti per la sicurezza dei sistemi di IA". Aveva istituito l'*U.S. AI Safety's Institute* per identificare, misurare e mitigare i rischi dei sistemi avanzati di IA, ma soprattutto aveva autorizzato l'adesione alla Convenzione quadro del Consiglio d'Europa su *Intelligenza artificiale, Diritti umani, Democrazia e Stato di diritto*. La linea politica perseguita da Trump vuole riaffermare l'intangibilità di uno sviluppo tecnologico, affidato a conglomerati privati, che non solo agiscono senza controlli, ma tendono a definire a loro misura le condizioni economiche e giuridiche¹. Lo Stato si dovrebbe rafforzare attraverso la tecnica (dalle innovazioni militari ai nuovi strumenti di controllo sociale) e

* Contributo redatto all'interno del progetto Prodotto PIACERI 2024/2026 Università di Catania progetto e-TIME.

¹ «...we will continue to reject radical climate dogma and bureaucratic red tape...we need to "Build, Baby, Build!"». Leggiamo nel *Winning the Race. America's AI Action Plan* emanato da Trump nel Luglio 2025

la tecnica attraverso lo Stato (dagli investimenti pubblici su enormi data center alle agevolazioni nelle forniture di energia). Se osserviamo le dimensioni, i livelli di capitalizzazione e la quantità di funzioni, ci rendiamo conto che ci troviamo di fronte a un singolare *network* di entità multiagenti che si struttura come un sistema di sistemi, a livello organizzativo, e come uno strumento di strumenti a livello operativo: un insieme di interconnessioni meccaniche, *start up*, algoritmi, rapporti finanziari, potenza economica. In questo nuovo ordine istituzionale l'effetto di confluenza, per cui disponiamo di tecnologie in grado di agire in modo regolare e normale come utenti autonomi di altre tecnologie (sistemi di sistemi), si salda all'effetto espansionistico per cui abbiamo sistemi che continuano a perfezionarsi indipendentemente dal compito per cui sono stati programmati (strumenti di strumenti). Si sta venendo a formare un "ecosistema tentacolare" rafforzato dalla monopolizzazione dei nodi di connettività delle infrastrutture critiche (satelliti e cavi sottomarini), dall'estrazione indiscriminata dei dati e dalla loro mercificazione, dall'accumulo di una potenza di calcolo inimmaginabile, dall'accesso privilegiato a processori avanzati, dallo sfruttamento di budget colossali per l'innovazione. Infocrazia? *Cloud empires*? Un mondo senza regole in cui una qualsiasi laboratorio di ricerca, come OpenAi, può prima imporre con ChatGpt svolte inattese e poi proporsi come artefice degli orizzonti di una nuova era, l'era agentica. Senza un tentativo di penetrare le diverse articolazioni di questo *loop* che si è andato determinando, l'esigenza di affermare il primato della regolazione attraverso un complesso apparato di strutture di governo, livelli di rischio, vincoli e sanzioni sarebbe meramente illusorio. L'auspicio un'intelligenza artificiale "affidabile, antropocentrica, etica, sicura" ("considerando" 1 e 8) e il rispetto degli ulteriori principi etici

richiamati dal "considerando" 27 sarebbero l'ennesimo riecheggiamento delle tante dichiarazioni internazionali, linee guida, codici di condotta che si sono accumulati inutilmente in questi anni. Non potremmo evitare, dinanzi a questa finora inutile corsa all'enunciazioni di valori, lo stesso fastidio che, nel 1948, Carl Schmitt confidava all'intimità del suo *Glossario* dinanzi al susseguirsi di richiami al diritto naturale: "... alcune dozzine di postulati del tutto contraddittori, un mucchio di vaghe clausole formali, i cui concetti presupposti- restano indefiniti e offrono l'immagine di cento volti diversi con cento nasi di cera". Il Regolamento ha il pregio di porre l'accento non solo sui valori, ma soprattutto sulla "catena del valore" attraverso cui si sviluppa questa "famiglia di tecnologie". Per questo motivo scompone tanto la dimensione soggettiva (distributore, importatore, deployer, fabbricante del prodotto, terzi) quanto la dimensione oggettiva (dati di addestramento, dati di convalida, dati di prova, dati di input, dati biometrici, dati operativi sensibili) e pone l'accento sulle infrastrutture critiche e sui rischi sistemici. Suggerisce l'adozione di codici di buone pratiche e la creazione di ambiti controllati di sperimentazione. Tocca anche il tema del modello di IA per finalità generali e il problema dell'approccio di apprendimento automatico. Non so quanto tutto questo sia efficace a livello operativo, ma ritengo sia importante iniziare a pensare che, nell'aspirazione a uno sviluppo *human in the loop*, non sia l'*human* che dobbiamo scoprire, ma dobbiamo penetrare e dissezionare la crescente complessità del *loop*. Ce lo suggeriscono gli stessi artefici della rivoluzione digitale. "Open AI cannot be a normal company" scrive Altman sul suo Blog. Secondo Zuckerberg, Facebook è diventato più simile a un governo che a un'impresa tradizionale. Nell'annunciare Grok 3, Musk afferma che non è un modello di AI, ma è una famiglia di modelli. È



impossibile regolamentare ciò che non sappiamo individuare ed è difficile allineare ai valori umani ciò che non può essere regolamentato. L'affidabilità è strettamente collegata alla trasparenza. Per questo motivo l'AI Act dedica particolare attenzione al problema dell'opacità e ipotizza il riconoscimento di un diritto a una spiegazione chiara ed esaustiva qualora, nei sistemi ad alto rischio, la decisione produca effetti significativi sui diritti fondamentali ("considerando" 171). A sua volta l'art. 14 pone l'esigenza della "sorveglianza umana", sottolineando l'opportunità di "comprendere correttamente la capacità e i limiti di sistemi di IA ad alto rischio". La cautela che induce a parlare, nell'art. 14, di "opportunità" (*«are enabled, as appropriate and proportionate»*) e non di diritti, malgrado il "diritto di ottenere una spiegazione" del "considerando" 171, ci fa riflettere su un punto cruciale di tutto questo apparato di controlli e vincoli: il fatto che i sistemi di intelligenza artificiale, in particolare i sistemi linguistici generativi, vengono addestrati e valutati su enormi dataset non controllabili a causa della indecifrabilità dei processi interni, per cui non basterebbe aprire i codici sorgenti, comunque spesso coperti dal segreto industriale, ma bisognerebbe risalire a una serie di snodi, ciascuno dei quali è anch'esso protetto da copyright. Inoltre nei sistemi più evoluti a finalità generale gli stessi programmatori e tecnici non sono spesso in grado di spiegare come il sistema sia arrivato a determinati risultati o di prevedere i risultati. Questo effetto *black box* non è, allo stato attuale delle conoscenze, eliminabile per cui dobbiamo convivere con una strutturale limitazione dell'interpretabilità algoritmica.

L'opacità aumenta se consideriamo tutto il settore dell'impiego militare e della pubblica sicurezza esplicitamente esclusi dalla Regolamentazione. Nel 2023 l'*AI in the UK: Ready, Willing and Able?* dell'House of Lords Select Committee

afferitava chiaramente che «sulla base delle prove che abbiamo ricevuto, riteniamo che il raggiungimento di una piena trasparenza tecnica sia difficile, e forse addirittura impossibile, per alcuni tipi di sistemi di IA in uso oggi, e in ogni caso non sarebbe appropriata o utile in molti casi». Non possiamo ormai fare a meno dell'intelligenza artificiale, ma non sappiamo e/o non vogliamo controllarla. Se è vero, come sostengono i teorici dell'*Effective Accelerationism*, che ci avviamo verso un nuovo illuminismo, potrebbe essere un "illuminismo oscuro", se ascoltiamo Nick Land. La regolamentazione europea cerca di evitare questa deriva negativa e, a mio avviso, indica anche la via corretta: individuare e definire gli anelli della "catena del valore", penetrando la complessità del *loop* per rendere effettivo il principio di esplicabilità. Temo, però, che ci siano ancora troppi ostacoli tecnici, politici ed economici.