Nexa Center for Internet & Society
Politecnico di Torino

L'Open Source rapportato all'Intelligenza Artificiale

Autore:

Dott. Giacomo Conti

Supervisione scientifica:

Prof. Antonio Vetrò

Ing. Manuela Bargis (TIM)

Ing. Gabriele Elia (TIM)

"Attività di ricerca svolta in collaborazione con TIM nell'ambito dell'iniziativa IPCEI – CIS – Progetto TIMECC – CUP B19J24000940005"

Finanziato dall'Unione europea
NextGenerationEU

June 2025

Studying the Internet, exploring its potential & experimenting new ideas

Via Pier Carlo Boggio 65/A, 10129 Torino, Italia

(http://nexa.polito.it/contacts-en)

+39 011 090 7217 (Telephone)

+39 011 090 7216 (Fax)

info@nexa.polito.it

Mailing address:

Nexa Center for Internet & Society

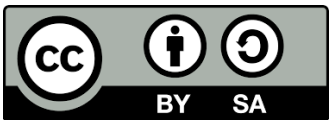
Politecnico di Torino - DAUIN

Corso Duca degli Abruzzi, 24

10129 TORINO

ITALY

The Nexa Center for Internet & Society is a research center affiliated to the Department of Control and Computer Engineering of Politecnico di Torino (http://dauin.polito.it)



Sommario

1. Introduzione

Negli ultimi anni, l'avvento dell'Intelligenza Artificiale ha iniziato una radicale trasformazione del panorama tecnologico, influenzando profondamente il modo in cui il software viene concepito, sviluppato e distribuito. Il concetto di open source, nato con l'obiettivo di democratizzare l'accesso al software, garantire trasparenza e promuovere l'innovazione collaborativa, deve oggi confrontarsi con le peculiarità dell'IA, ed in particolare con la cosiddetta IA generativa.

In origine, il concetto di software "aperto" si riferiva infatti alla possibilità di accedere e modificare liberamente il codice sorgente del programma, ovvero l'insieme di istruzioni scritte dai programmatori che ne determinano in ultima istanza il funzionamento. Questo approccio garantiva che chiunque potesse esaminare, migliorare, distribuire ed adattare il software alle proprie esigenze, seppure, a volte, con qualche vincolo (come nel caso delle licenze *copyleft*).

La disponibilità del codice sorgente permetteva anche di evitare il rischio di dipendere da una singola azienda o sviluppatore, poiché chiunque poteva intervenire per correggere errori, aggiungere nuove funzionalità o adattare il software a contesti differenti. A fronte di questo, si ponevano e si pongono ancora oggi questioni di responsabilità: più è alto (anche solo potenzialmente) il numero di sviluppatori, più è difficile costituire una catena di responsabilità precisa nel caso in cui, in breve, qualcosa vada storto: il software malfunzioni o funzioni in modo malevolo e da ciò derivino dei danni.

Tuttavia, nell'IA moderna, gli elementi chiave per il funzionamento dei modelli – come i dati di addestramento, i pesi del modello e le informazioni sui processi di ottimizzazione – sono spesso opachi o proprietari, anche quando le licenze del software si dichiarano aperte. Ciò genera nuove problematiche di trasparenza e accessibilità, che rischiano di vanificare i benefici tradizionali dell'open source. Parallelamente, il concetto stesso di open source si sta evolvendo per adattarsi alla complessità di questi sistemi, ma le definizioni e le pratiche consolidate in una realtà tecnologica molto diversa spesso faticano oggi a tenere il passo con i cambiamenti in atto. Questa transizione, unita a una crescente pressione normativa, richiede una riflessione critica sul futuro del modello open source, non solo come principio filosofico, ma come strumento pratico per governare le tecnologie avanzate dell'IA, cercando di vedere al di là delle mere dichiarazioni di principio formalistiche, spesso tendenti a configurare come "open" strumenti di IA che, in realtà, non lo sono affatto.

Il settore delle telecomunicazioni è uno dei principali beneficiari e promotori dell'innovazione nell'ambito dell'Intelligenza Artificiale. Con lo sviluppo di nuove tecnologie come il 5G e l'imminente 6G, l'IA sta diventando fondamentale per gestire automaticamente reti sempre più complesse, ottimizzare le infrastrutture e offrire servizi avanzati agli utenti, sia nel segmento B2C (business-to-consumer) che B2B (business-to-business). L'utilizzo di soluzioni IA consente infatti, almeno in teoria, alle aziende di telecomunicazioni di migliorare le prestazioni delle reti, prevedere e prevenire guasti, ottimizzare l'allocazione delle risorse e personalizzare maggiormente i servizi in base alle esigenze degli utenti.

Al contempo, il settore delle telecomunicazioni sta affrontando nuove sfide proprio legate alla dubbiosità delle nature “open” o “closed” di tali sistemi. Poiché la creazione di un modello completamente nuovo di IA richiederebbe sforzi abbordabili solo da una ristrettissima cerchia di realtà, nella maggior parte dei casi le imprese si servono di modelli di IA di terze parti, spesso proprietari, che per definizione riducono la trasparenza e la possibilità di personalizzazione. In questo senso, l’adozione di componenti open source può rappresentare una via d’uscita, ma richiede una riflessione critica sulle modalità di implementazione, le licenze da adottare e la conformità alle normative vigenti, nonché la reale “apertura” di tali modelli, per evitare il rischio di dipendenza da soluzioni proprietarie che sono “open” soltanto sulla carta.

Questo documento ha l’obiettivo di analizzare le evoluzioni e le problematiche legate all’applicazione del modello open source nel contesto dell’Intelligenza Artificiale (IA), con particolare riferimento al settore delle telecomunicazioni. In un panorama tecnologico in rapido cambiamento, l’approccio tradizionale alla dicotomia tra software "open" e "closed" risulta sempre più inadeguato per affrontare le sfide poste dall'IA, specialmente per quanto riguarda la trasparenza, il riuso e la responsabilità. Questo studio si propone di esaminare le criticità esistenti, identificare le obsolescenze del modello tradizionale e investigare soluzioni teoriche e pratiche per superarle già proposte in letteratura. Inoltre, sarà considerato il quadro normativo europeo in evoluzione, con un focus sulle recenti iniziative legislative come l'AI Act, per valutarne l'efficacia e le implicazioni. Un'attenzione particolare sarà riservata all'analisi dell'impatto di questi temi sul settore delle telecomunicazioni, dove l’IA sta assumendo un ruolo sempre più rilevante.

2. Evoluzione del concetto di Open Source nel contesto dell'Intelligenza Artificiale

2.1. Definizioni tradizionali di open e closed source + tradizionali licenze open source

La diffusione del software open source è strettamente legata al concetto di licenza, che regola come il software può essere utilizzato, modificato e distribuito. La licenza open source più diffusa è la General Public License (GPL), introdotta nel 1989 e basata sul concetto di copyleft[1].
Per "licenza" in questo caso si intende il contratto con cui il proprietario o il titolare dei diritti sul *software* abbia deciso di regolare e limitare la diffusione e l'utilizzo della sua opera. A seconda della licenza che si sceglie quando si commercializza o in altro modo si diffonde il prodotto, esso verrà categorizzato tra i *software* chiusi o quelli aperti[2].
Nel sistema del "copyleft", evidente gioco linguistico sul termine "copyright", al posto della parola "right", che in inglese è sia "diritto" che "destra", gli autori del software libero sostituirono la parola "left", che è sia "lasciato, abbandonato", sia "sinistra". A orpello grafico di questa concezione, la "c" cerchiata, simbolo del copyright, ©, viene invertita a specchio, nella licenza GPL, verso sinistra.
E' opportuno notare come non sia per forza un *software* il destinatario di una licenza Copyleft: documenti, forme d'arte e perfino scoperte scientifiche possono legittimamente essere rilasciate in tale modo[3].

A differenza del copyright, il copyleft permette agli utenti di modificare e redistribuire il software, a patto che qualsiasi derivato mantenga la stessa licenza. Questo assicura che il software e le sue varianti rimangano aperti e disponibili a tutti. E' questa la peculiairtà fondamentale delle licenze di *copyleft*: il fatto che tutto ciò che viene tratto a partire da una licenza Copyleft deve essere anch'esso Copyleft. Se uno sviluppatore trae a piene mani da un *software open source* la cui licenza esplichi la natura di Copyleft, e crea qualcosa di nuovo a partire da esso, allora quel qualcosa di nuovo dovrà obbligatoriamente avere la stessa licenza libera del programma dal quale fu tratto: "[the GPL] requires any source code linked to it to be provided to the end user, if used in a distributed product"[4].
Biblicamente, se Adamo fu licenziato in *Open Source* con Copyleft, allora anche Eva dovrà esserlo. Copyleft e Open Source, però, non sono per forza sinonimi. Parafrasando una famosa frase, si potrebbe dire che non tutte le licenze *open source* sono anche copyleft, mentre tutte le licenze copyleft sono anche *open source*.

---

[1]Daavid Bahn, Dan Dressel, *Libaility and Control Risks with Open Source Software*, Metropolitan State University, Minneapolis, MN, Novembre 2006
[2]GNU.org, *Licenze Varie e commenti relativi*, Il sistema operativo GNU, da GNU.org, versione italiana, 2017
[3]John C. Newman, *Copyright and Open Access at the Bedside,* The New England Journal of Medicine, 2011.
[4]Jeff Luszcz, *Artifex v. Hancom: Open Source is now an enforceable Contract*, Linux.com, 31 agosto 2017

Nella GPL ma non solo, è oggi sancita una clausola generale di limitazione della responsabilità, sia per ciò che riguarda quella contrattuale, sia quella extracontrattuale. I termini utilizzati per indicare l'una e l'altra sono, ovviamente, "contract" e "tort", e la formula che ne limita la rilevanza è da ritrovarsi nella formula "as is" presente in quasi tutti i tipi di licenza libera.
"As is" significa "così com'è", ed è riferito al modo attraverso il quale il *software* libero è fornito. Dire che esso è dato all'utente "così com'è" significa aprirsi la strada, immediatamente dopo, per negare qualsiasi tipo di garanzia. Si suole infatti leggere che il *software* è dato "without warranties or conditions of any kind", con una frase che suona un po' come un mantra, da quanto è onnipresente[5].
Secondo le principali licenze *open source*, il software fornito non può essere motivo di citazione in giudizio da parte dell'utente a seguito di danni prodotti, diretti o indiretti, derivanti dal suo utilizzo. Che questo tema sia sentito, in chiave negativa, è indubbio. Addirittura l'Open Source Initiative, organizzazione statunitense che dal 1998 si fa un po' da portavoce per tutto il mare magnum del software libero[6], evita accuratamente nelle sue "domande più frequenti" di menzionare quelli che di fatto sono notevoli rischi per gli utenti, che non possono far valere, stando così le cose, le loro posizioni qualora subissero danni dall'utilizzo del programma.

Oltre alle importanti licenze "Copyleft" di cui si è detto, è possibile in massima sintesi ritenere che queste si accompagnino alle licenze "Permissive" a formare il macro insieme del software open. Le licenze "Permissive" (che, nonostante sia una parola omografa in italiano, è inglese) permettono l'utilizzo, la modifica e la distribuzione del software con restrizioni minime o assenti. Si tratta pertanto delle licenze meno vincolanti in assoluto, dal momento che le richieste sono spesso limitate all'attribuzione delle note di licenza originali all'atto della distribuzione di nuovo software, lasciando quindi libero lo sviluppatore anche di monetizzare il proprio progetto al di là dei suoi materiali di origine[7]. Tra le più importanti licenze "Permissive" si segnalano la MIT License e l'Apache License 2.0.

Non è sempre agevole comparare, per così dire, il grado di libertà che le varie licenze assicurano ai loro utilizzatori. Per questa ragione, è opportuno partire invididuando alcune caratteristiche fondamentali, comuni a tutte le licenze, ed osservare di volta in volta come ciascuna di esse giunga a diverse conclusioni:

1) **La possibilità di "Linking"**: alcune licenze, come la LGPL (una versione più "permissive" della già citata GPL), permettono di collegare il codice open source a codice proprietario senza estendere le restrizioni dell'open source all'intero progetto. Questo è l'opposto di

[5] James Dixon, *What license does your software have?* Quora.com, 7 Agosto 2015
[6] Da opensource.org, *Open Source Initiative, History of the OSI,* Dicembre 2017
[7] Ad esempio la MIT License, una delle più famose licenze permissive, concede agli sviluppatori piena libertà di monetizzare i loro progetti, anche se basati su codice open source. In particolare, la licenza permette a chiunque di:
1) Usare il software per qualsiasi scopo, compreso l'uso commerciale.
2) Modificare e distribuire il software, anche come parte di un progetto proprietario.
3) Non rilasciare il codice sorgente modificato.
Quindi, uno sviluppatore può vendere prodotti o servizi basati su software sotto licenza MIT senza restrizioni, mantenendo il codice sorgente privato, se così desidera.

quanto venga sancito tramite meccanismi di copyleft: la GPL tradizionale, si ricorderà, impone infatti la ridistribuzione sempre e solo sotto GPL.

2) **La libertà di distribuzione**: con ciò si intende i vincoli dati agli utilizzatori di determinate licenze per il rilascio del codice sorgente. Non tutte le licenze open source, infatti, impongono la distribuzione del codice sorgente assieme al programma di riferimento. Licenze come la Apache License 2.0 permettono una distribuzione flessibile, mentre la GPL richiede la distribuzione intera del codice sorgente.
3) **I vincoli sulla modifica del materiale originale**: Molte licenze open source consentono di modificare il codice del programma per i propri usi, ma differiscono su come le modifiche possono essere distribuite. Di nuovo, la GPL e le licenze più propriamente "copyleft" impongono che anche le modifiche siano rilasciate sotto GPL, mentre licenze permissive come la MIT non pongono vincoli.
4) **La creazione di brevetti**: la maggior parte delle licenze open source includono clausole sui brevetti che proteggono gli utenti da rivendicazioni legali riguardanti l'uso del codice, di fatto rendendo impossibile relegare a un insieme limitato di individui la possibilità di sfruttare quegli stessi brevetti.

License	Author	Latest version	Publication date	Linking	Distribution	Modification	Patent grant	Private use	Sublicensing	TM grant
Apache License	Apache Software Foundation	2.0	2004	Permissive[13]	Permissive[13]	Permissive[13]	Yes[13]	Yes[13]	Permissive[13]	No[13]
CC BY	Creative Commons	4.0	2002	Permissive[17]	Permissive	Permissive	No	Yes	Permissive	No
CC BY-SA	Creative Commons	4.0	2002	Copylefted[17]	Copylefted	Copylefted	No	Yes	Copylefted[18]	No
GNU General Public License	Free Software Foundation	3.0	June 2007	GPLv3 compatible only[28][29]	Copylefted[26]	Copylefted[26]	Yes[30]	Yes[30]	Copylefted[26]	Yes[30]
GNU Lesser General Public License	Free Software Foundation	3.0	June 2007	With restrictions[31]	Copylefted[26]	Copylefted[26]	Yes[32]	Yes	Copylefted[26]	Yes[32]

Figura 1 Estratto di alcune delle più famose licenze e delle loro regole per ciò che concerne alcuni elementi primari del software. Da https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses

E' chiaro dunque che le licenze open source variano notevolmente per quanto riguarda la libertà che concedono agli utenti e agli sviluppatori. Se da una parte le licenze più permissive come MIT e BSD forniscono massima flessibilità, dall'altra licenze altrettanto open source, ma più propriamente copyleft, come la GPL, impongono condizioni decisamente più rigorose per ciò che concerne la distribuzione e la modifica del software. La scelta della licenza giusta deve dunque dipendere dagli obiettivi specifici del progetto, dalla natura del software, dalle ambizioni di ispirazione (o copia diretta) più o meno spinte nei confronti del materiale di partenza, e dall'intenzione, in ultima istanza personale dello sviluppatore, di mantenere il codice libero o di permetterne l'uso in applicazioni proprietarie.
Come si vedrà nel successivo capitolo, questo sistema, già notevolmente complesso, è messo in discussione dalla nuova natura dei software di Intelligenza Artificiale, dei quali il codice sorgente, tratto primariamente in esame da questo genere di licenze, è soltanto una parte (e neppure forse la più importante) dei nuovi progetti.

2.2. La crisi della dicotomia open/closed

Le licenze open source tradizionali, come la GPL (General Public License) o la Apache License, sono state sviluppate principalmente per gestire la condivisione e la modifica del codice sorgente di un software. Tuttavia, quando si vuole applicarle al contesto dell'intelligenza artificiale, esse pagano il fio di non coprire adeguatamente i nuovi elementi centrali per lo sviluppo e l'utilizzo di sistemi IA, tra i quali figurano primariamente i dataset e i modelli di addestramento.

Nel software tradizionale, il codice sorgente è l'elemento principale protetto dalla licenza, che regola la sua modifica ed eventuale successiva distribuzione. Nell'IA invece il codice rappresenta solo una parte del totale – e neppure, forse, la più importante.

Oltre al codice, figurano primariamente le enorme quantità di dati utilizzati per addestrare i modelli e, successivamente, i modelli addestrati stessi. Questi ultimi non sono semplici programmi, ma rappresentano il risultato di processi complessi di apprendimento su grandi quantità di dati, spesso proprietari, che non sono quasi mai realmente condivisi o aperti come il codice stesso[8].

Le licenze open source, nella loro forma tradizionale, non sono progettate per affrontare le complessità associate alla proprietà e alla distribuzione dei dati, pagando il dazio di essere state formulate in un tempo precedente.
Ad esempio, un dataset usato per addestrare un modello IA può essere protetto da diritti di proprietà intellettuale o può contenere informazioni sensibili o personali, rendendolo non idoneo alla distribuzione con licenze aperte. Di conseguenza, anche quando un modello IA è distribuito, come spesso accade, con una licenza open source, il dataset originale utilizzato per il suo addestramento potrebbe non essere incluso, limitando la replicabilità e la trasparenza del modello.

Il sistema di licenze open source, peraltro, può creare notevoli grovigli giuridici tra il codice sorgente, i dataset ed i modelli di addestramento. È infatti del tutto usuale considerare il modello addestrato come un elemento diverso rispetto al codice sorgente del software di IA che ha portato a quello stesso addestramento, così come i dati utilizzati per addestrarlo sono un insieme totalmente a sé stante. In altre parole, modelli, codici e dataset possono avere ciascuno una licenza diversa, sia in termini di derivazione (es. il modello opensource è stato addestrato su un dataset privato) sia in termini di vincoli o permessi circa il loro utilizzo (es. il modello addestrato è venduto a pagamento e licenziato come closed source malgrado sia stato nutrito da dati open source).

Anche gli stessi dati utilizzati per l'addestramento dei modelli possono poi essere ulteriormente divisi al loro interno tra dati liberamente accessibili a chiunque e non: molti dataset utilizzati per addestrare modelli IA contengono dati personali o sensibili, che non possono essere liberamente condivisi senza violare normative come il GDPR in Europa al di fuori dei soggetti cui è stato esplicitamente dato il consenso per l'utilizzo dei dati stessi. In questo caso, un modello di IA

[8] Nicola Lucchi, *ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems*, European Journal of Risk Regulation, 2023, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/chatgpt-a-case-study-on-copyright-challenges-for-generative-artificial-intelligence-systems/CEDCE34DED599CC4EB201289BB161965#article

disponibile al pubblico ma che facesse leva su dati personali sarebbe, in teoria, disponibile solo a quanti avessero avuto l'esplicito consenso, da parte dei *data subjects*, circa l'utilizzo di quei dati specifici per quelle precise ragioni. Non solo: il *training* dei sistemi di IA si esplica anche attraverso dati non per forza personali ma lo stesso protetti da copyright, non disponibili liberamente o gratuitamente, o acceduti da *dataset* dotati di licenze closed source. L'utilizzo di questi dati per tali scopi, malgrado appaia piuttosto diffuso[9], sembra essere spesso illecito.

Anche il discorso del *copyleft* sembra scricchiolare pesantemente di fronte a questa nuova natura, che nella migliore delle ipotesi è tripartita (codice, dataset, modello addestrato), del software IA. Se infatti si considera, com'è usuale considerare, ciascuno di tali elementi come separato, allora ognuno di essi potrà avere una licenza diversa che ne governa la distribuzione, col risultato inevitabile di rischi di incompatibilità ad ogni pié sospinto, nonché numerose problemi di trasparenza e soprattutto replicabilità presso qualsiasi altro soggetto[10].

In realtà, la complessità dei problemi è ancora maggiore, dal momento che esistono ulteriori passaggi intermedi, o generali funzionalità, suscettibili di una "valutazione di apertura": oltre a codice, dataset e modello addestrato, concorrono alla creazione di un sistema di IA i pesi che vengono dati ai singoli dati del modello per la generazione dell'output, le API per interfacciare il sistema con software terzi, e le documentazioni, più o meno complete, che permettono agli utenti e agli sviluppatori di utilizzare il sistema nel modo più adeguato, anche se, realisticamente, tanto più un'analisi approfondisce in questo senso, tanti più elementi individua, giungendo alla conclusione che <<nonostante ci sia una lista sempre crescente di progetti che si autodefiniscono "open source", molti ereditano dati di dubbia liceità, e pochi condividono le importantissime istruzioni di perfezionamento, e la documentazione scientifica è estremamente rara>>[11].

Per procedere nell'analisi, occorre ora interrogarsi su due questioni fondamentali: l'una è se effettivamente sia necessaria questa percepita rincorsa all'open source o se sia una declinazione moderna della lotta contro i mulini a vento attuata da brontolosi teorici, magari anche dannosa per l'innovazione; l'altra, se possano darsi soluzioni legali realmente efficaci per mantenere un buon grado di apertura e progresso, sia dal punto di vista normativo (tema cui verrà dato spazio più avanti nel documento), sia dal punto di vista delle licenze che regolamentano poi la diffusione e l'uso degli elementi costituenti i modelli di IA.

---

[9] Il New York Times, ad esempio, ha già alla fine dell'anno scorso intentato una causa contro OpenAI per aver utilizzato suoi contenuti, senza il suo consenso, nell'addestramento di modelli: https://nytco-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf .
Si veda anche A. Pope, *NYT v. OpenAI: The Time's About-Face*, Harvard Law Review, 10 aprile 2024, https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/

[10] Si veda ad esempio il caso di Google, che ha almeno sulla carta reso open source il codice dei modelli di machine learning utilizzati per classificare i video su Youtube. Tuttavia, per addestrare tali modelli è stato usato il dataset Youtube-8M, anch'esso disponibile al pubblico, ma solo dietro specifiche condizioni, che rendono perciò impossibile per chiunque che non sia Google ricreare scientificamente lo stesso modello, facendo derivare da esso gli stessi output a partire da input eguali.

[11] A. Liesenfeld, A. Lopez, M. Dingemanse, *Opening up ChatGPT: Tracking openness, transparency, and accountability in instruction-tuned text generators,* CUI '23, Luglio 19–21, 2023, Eindhoven, https://pure.mpg.de/rest/items/item_3526897_1/component/file_3526898/content

Circa la prima, si è visto precedentemente nel documento di come il software *closed source* possa essere ritenuto essenzialmente preferibile perchè più facile e comodo da usare, perchè usualmente meglio aggiornato e meglio manutenuto grazie ai profitti derivanti dalla sua commercializzazione, e soprattutto maggiormente sicuro dal punto di vista della responsabilità, laddove se qualcosa va storto è tendenzialmente lineare risalire alle cause, ed ottenere quindi potenzialmente soddisfazione in giudizio.

Ma se ciò era vero per il software tradizionale, l'ecosistema generale dello sviluppo e della distribuzione del software è oggi molto diverso di quanto fosse in passato, e grazie a piattaforme come GitHub, che facilitano la gestione, lo sviluppo e la distribuzione del software, e a strumenti moderni come framework e librerie ben documentate (come TensorFlow), non vi è ragione per cui un sistema di IA open source possa essere più difficoltoso da usare e dotato di meno appeal di un sistema closed source.

Anche il tema della manutenzione e dell'aggiornamento sul lungo periodo può essere risolto: progetti come Apache o Mozilla Firefox ricevono aggiornamenti regolari e tempestivi grazie alla partecipazione di sviluppatori di tutto il mondo, a causa dell'alto interesse diffuso nello sviluppo di software di quel genere, dimostrando che la qualità della manutenzione e degli aggiornamenti non dipende esclusivamente da fattori economici. Peraltro, si osservano anche partnership o generiche sponsorizzazioni di soggetti importanti nell'ambito informatico circa il software libero[12]

Il tema forse più spinoso è legato alla responsabilità legale, nonché alla sicurezza in generale: punti in effetti deboli del software open source, poiché spesso manca una precisa catena di responsabilità alla quale risalire.

In generale, il consenso scientifico sembra spostarsi verso la preferenza nei confronti dei software aperti anche per questioni di etica[13]: un tema che sembra destinato ad essere sempre più importante a mano a mano che le intelligenze artificiali entrano nel quotidiano, specie in ambiti critici come la sanità o la giustizia. Ma non solo: perché si possa operare in modo propriamente scientifico su questi sistemi, è necessario che essi siano anzitutto riproducibili[14]: è questo, del resto, il primo requisito della scienza. Peraltro, a partire da questo, può ben sostenersi che sia proprio la mancanza di trasparenza e l'imprevedibilità degli output ad esporre a problematiche di responsabilità i sistemi di IA particolarmente chiusi, in modo probabilmente ancora più acuto di quanto accada per i sistemi open source spesso criticati per questo.

Come si è potuto intendere, l'open source è spesso celebrato per le qualità intrinseche di trasparenza, apertura e almeno parziale disinteresse nei confronti del profitto che lo rendono estremamente attraente dal punto di vista del marketing per qualsiasi impresa attiva nel digitale. In massima sintesi, questo ha portato numerose imprese di sistemi closed source a sfruttare

[12] Soggetti come Meta, Google, Intel e Microsoft sono ad esempio a vario titolo citati come enti di supporto per la Open Source Foundation: https://opensource.org/sponsors
[13] A. Birhane, V. U. Prabhu, E. Kahembwe, *Multimodal datasets: misogyny, pornography and malignant stereotypes,* arXiv, 5 Ottobre 2021, https://arxiv.org/abs/2110.01963
[14] E. C. McKiernan et al., *How open science helps researchers succeed,* eLife 5, luglio 2016, https://elifesciences.org/articles/16800

l'etichetta "open" per migliorare la loro immagine, senza aderire veramente ai principi fondamentali dell'open source, o aderendone soltanto in parte – posto che non esista una precisa definizione di “open source” né una serie di requisiti che vanno seguiti per potersi fregiare di tale nome.

Questo fenomeno è spesso noto come "open washing", ed avviene in massima parte quando un progetto viene dichiarato "open" per motivi di marketing, pur rimanendo nelle mani del creatore il controllo del codice, il suo mascheramento, e le decisioni di sviluppo o di accesso ai dati[15]. La mancanza di requisiti chiari e vincolanti per definire cosa significhi veramente essere open consente a queste aziende di appropriarsi di un'immagine positiva senza offrire i reali benefici della trasparenza e della partecipazione comunitaria, creando così un inganno almeno parziale, e distorcendo il significato originale, seppur impreciso, del termine.

2.3. Le nuove necessità concettuali in materia di open source

In un quadro così delineato, nell’assenza di definizione precise circa la definizione di *open* e l’inarrestabile progresso tecnologico delle IA, unito alla loro voracità in termini di dati, il cui controllo di legittimità sembra estremamente complesso, appare chiaro come siano necessari cambiamenti concettuali e legislativi in grado di adeguare i vecchi concetti a questo mutato scenario, e, se necessario, crearne di nuovi che fungano da base per la creazione di modelli di IA realmente aperti, compatibili con le norme in tema di privacy e sicurezza, e generalmente favorevoli per il pubblico e gli autori dei materiali sui quali essi sono addestrati. Delle questioni legislative si parlerà in seguito; per iniziare, è qui necessario concentrarsi su un discorso più astratto e concettuale.

Le licenze open source tradizionali, come la GPL e la Apache License, non sono state progettate per coprire la complessità delle odierne tecnologie di Intelligenza Artificiale. Del resto, al tempo della loro formulazione, l’IA non era che un concetto fantascientifico.

L’Open Source Initiative è attualmente al lavoro su una sorta di manifesto per l’Intelligenza Artificiale Open che viene periodicamente aggiornato, ed al momento della scrittura di questo documento si trova alla versione 1.0, nel quale pone quattro requisiti fondamentali perché un sistema di IA possa effettivamente definirsi “open”[16]. La reputazione e l’importanza dell’Open Source Initiative, nonché la natura discorsiva e per nulla tecnica di tali requisiti rendono questo un buon punto di partenza per interrogarsi del tema.

La definizione di Open Source AI nella versione 1.0 della è stata aspramente criticata da una parte della comunità open source, che l’ha ritenuta concentrarsi troppo poco su nuovi trend come il cloud computing, e l’importanza dei dati, specialmente definendo il suo ambito di applicazione come “ogni software che deriva, da input, metodi per generare output”[17]. Sono state messe sotto accusa le metodologie con le quali si è giunti a quest’ultimo aggiornamento di versione, portando il

[15] D. Gray Widder, M. Whittaker, S. Myers West, *Why “open” AI systems are actually closed and why this matters,* Nature, 635, 827-833, 2024, https://www.nature.com/articles/s41586-024-08141-1
[16] https://opensource.org/ai/open-source-ai-definition
[17] *A community statement supporting the Open Source Definition*, https://osd.fyi/

documento alla 1.0, ritenendo che ciò sia stato fatto attraverso processi a porte chiuse in conflitto con i principi dell'apertura e della trasparenza tipici dell'etica open source.

Al netto delle attuali tensioni interne della comunità open source, l'Open Source Foundation rimane un punto di riferimento importante sull'argomento. Secondo la definizione di Open Source AI, dunque, perché un sistema di IA possa definirsi open deve consentire agli utilizzatori le libertà di:
- **Usare** il sistema come meglio intendono senza dover sottostare ad alcun permesso
- **Studiare** come il sistema funziona ed ispezionarne i singoli componenti
- **Modificare** tale sistema per ogni scopo ritengano opportuno, causandone anche un cambiamento negli output
- Condividere il sistema con altri con o senza modifiche apportate, per qualsiasi scopo.

A partire da questi concetti, che in effetti sono un riassunto di quanto è solitamente inteso come la base dell'open source, vengono individuate alcune caratteristiche tipiche dei sistemi di IA che debbono passare al vaglio di trasparenza perché il sistema nel suo complesso possa definirsi open: **i dati, il codice sorgente** ed **i pesi**.
Queste carattersitiche sono ciò che primariamente differenzia i moderni sistemi di IA da un qualsiasi software: si tratta infatti di elementi che vanno al di là del mero codice sorgente, che costituiva l'elemento protagonista preso in rassegna dall'open source pre-IA. Seppur in qualche misura accessori al codice sorgente, essi mantengono una loro identità, importanza e soprattutto necessarietà che li rendono fondamentali per ogni sistema di IA, e pertanto per ogni vaglio di apertura che su di esso viene fatto.

I dati sono gli elementi sui quali viene addestrato il sistema: oltre alle informazioni propriamente dette, ne è importante la provenienza e pertanto la loro liceità. Se per l'addestramento di un modello di IA viene utilizzato un dataset con una licenza closed source, o se i dati all'interno dello stesso sono protetti da copyright o in altro modo viziati dal punto di vista legale, è impensabile che il sistema di IA possa definirsi open.
Oltre a questo, la Open Source Initiative fa leva sull'importanza di dichiarare il modo con cui questi dati sono stati ottenuti e selezionati, e i procedimenti con i quali si sono etichettati, modificati ed in generale resi disponibili al sistema di IA perché ne traesse addestramento. Nella criticata ultima definizione dell'Open Source Initiative sull'IA, si è voluto ridurre di importanza questo aspetto, richiedendo semplicemente che venga data una "informazione dettagliata" sui dati ma non "i dati stessi" nel loro complesso perché si possa considerare un sistema di IA open source.
Contenutisticamente, è forse questa l'obiezione maggiore che la comunità dell'open source ha rivolto alla nuova definizione dell'OSI[18].

Il **codice sorgente**, come da tradizione del software libero, dev'essere messo a disposizione tramite licenze open-source, rispettandone i parametri e coprendo tutte le fasi del ciclo di vita del modello di IA. Nella fase iniziale, cosiddetta di "pre-processing", questo significa che il codice sorgente open deve comprendere anche l'accesso e le informazioni sul formato nel quale i modelli sono stati

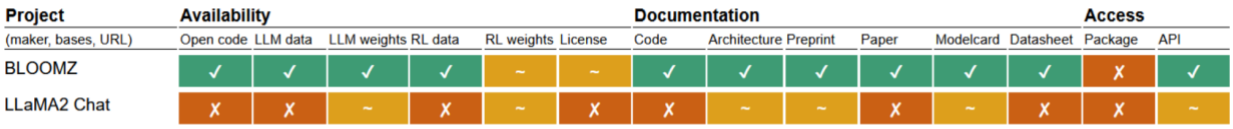
[18] J. Brockmeiner, *OSI readies confroversial Open AI definition*, LWN.net, https://lwn.net/SubscriberLink/995159/a37fb9817a00ebcb/

modificati per l'addestramento e i suoi *script* (funzionalità automatizzate che servono a replicare le caratteristiche di un dato presso altri: una volta reso comprensibile per il sistema di IA un certo dato, si replica in maniera automatizzata il modo con cui ciò è stato attuato presso altri dati).
Nella fase intermedia, di pre-rilascio, dev'essere comunicato in modo trasparente il sistema di addestramento, gli algoritmi di machine learning utilizzati, ed i test prestazionali e generali che sono stati compiuti per accertarsi della bontà del sistema.
Nella fase di distribuzione, devono essere rilasciate librerie di supporto per ausiliare gli utenti finali nella comprensione e nell'eventuale modifica del modello, nonché il sistema di inferenza (cioè il metodo tramite il quale il modello, già funzionante, apprende ancora), nonché ovviamente l'architettura del sistema, intendendo con ciò il codice propriamente detto che permette la fruizione ed il funzionamento dello stesso.

I **pesi** sono i parametri che determinano in ultima istanza l'*output* del sistema di IA, intendendo con ciò il risultato che viene prodotto a partire da un *input* dell'utente. Questi devono essere distribuiti in modo che sia chiaro quali valori numerici sono stati utilizzati per il collegamento delle informazioni (o *layer*) utilizzate per addestrare il modello: valori numerici più alti faranno sì che il sistema di IA reputi più importante una certa informazione. Poiché i pesi possono non essere statici, ma cambiare di valore numerico lungo la vita del modello, ciò dovrebbe essere reso palese in un sistema realmente Open, e dovrebbero anche essere messi a disposizione dell'utenza finale i cosiddetti "checkpoint", cioè le versioni intermedie in cui il sistema di IA si è via via trovato nel corso della sua costante evoluzione.

A partire da queste considerazioni si possono pertanto individuare con maggiore precisione i requisiti concreti che i sistemi di IA devono avere perché possano essere propriamente definiti open. Alcuni autori hanno pertanto iniziato a individuare le caratteristiche dei più diffusi sistemi di IA, dando una valutazione positiva, negativa o neutra della loro apertura[19]. Ne è risultata una tabella (di cui si riporta un estratto in Figura 2) nella quale emerge che nessun sistema di IA disponibile al momento dello studio fosse completamente open in tutte le sue componenti[20].
Tristemente in fondo alla classifica figura proprio ChatGPT, che nonostante sia stato sviluppato da *Open*AI, è un progetto closed source: il modello non è disponibile pubblicamente né lo sono la documentazione, il codice, i pesi ed i dati sui quali è stato addestrato, sui quali permane il mistero[21].

[19] A. Liesenfeld, M. Dingemanse, *Rethinking open source generative AI: open-washing and the EU AI Act*, FAccT, giugno 2024, Rio De Janeiro, https://pure.mpg.de/rest/items/item_3588217_2/component/file_3588218/content
[20] https://opening-up-chatgpt.github.io/
[21] M. Nasr et al., *Scalable Extraction of Training Data from (Production) Language Models*, 28 novembre 2023, *https://arxiv.org/pdf/2311.17035*



Project	Availability						Documentation						Access	
(maker, bases, URL)	Open code	LLM data	LLM weights	RL data	RL weights	License	Code	Architecture	Preprint	Paper	Modelcard	Datasheet	Package	API
BLOOMZ	✓	✓	✓	✓	~	~	✓	✓	✓	✓	✓	✓	✗	✓
LLaMA2 Chat	✗	✗	~	✗	~	✗	✗	~	~	✗	~	✗	✗	~

Figura 2 Estratto da Liesenfeld e Dingemanse. Per consultare l'intera tabella, visitare https://opening-up-chatgpt.github.io/

Nonostante l'Open Source Initiative sia un'entità rispettata ed influente, è evidente che la convenienza commerciale abbia portato i sistemi di IA più diffusi ad una natura chiusa. Non solo: le ultime polemiche di cui si è dato conto inerenti alla pubblicazione della versione 1.0 della definizione hanno sostanzialmente creato uno scisma all'interno della comunità, tale per cui in molti ritengono ancora valere la "Open Source Definition" propriamente detta (non quindi, quella specifica per l'IA), aggiornata alla versione 1.9[22], determinando ulteriore confusione e complessità nel momento in cui si volesse utilizzare questa base teorica.

La base teorica offerta dalla stessa Initiative nella definizione di *openness* rapportata all'Intelligenza Artificiale è comunque fondamentale per stratificare le fondamenta del discorso, che dovrebbe essere portato ad un ulteriore approfondimento, e ad alcuni vincoli normativi irrinunciabili, dalla legislazione dei singoli Stati e dell'Unione Europea in particolare.

Esiste poi un approccio al software forse ancora più radicale, che viene solitamente individuato nel concetto del "Free Software". Con esso si intende un paradigma di sviluppo in qualche misura imparentato con l'Open Source Software, ma con un approccio fondamentalmente diverso. Anziché concentrarsi su ciò che gli sviluppatori possono o non possono fare, in base alla licenza e alle caratteristiche della stessa, il Free Software pone al centro della questione l'utente finale, e ne definisce quattro libertà fondamentali:
1) la libertà di utilizzare il software per ogni intento;
2) la libertà di studiare e modificare il codice;
3) la libertà di distribuirne copie;
4) la libertà di condividere versioni modificate con altri.

Tali libertà, se sancite in modo assoluto, possono secondo alcune comuni critiche del modello dare un riscontro generalmente negativo alla società: un software che possa essere utilizzato liberamente senza alcun vincolo può suscitare legittime preoccupazioni di mal utilizzo, o di utilizzo illecito o dannoso.

Questo è sempre più apparente nei sistemi di IA, sui quali tali preoccupazioni legate all'uso improprio della tecnologia sono emerse con grandissima forza. C'è, in effetti, una generale preoccupazione sociale che si esplica nel desiderio di controllare come il sistema di IA venga di volta in volta utilizzato, per prevenire danni.

[22] https://opensourcedeclaration.org/index-en-us.html

Nuove licenze, come la RAIL License (Responsible AI License)[23] cercano di combattere gli utilizzi negativi tramite una serie di limiti, per esempio proibendo l'uso di sistemi di IA, pur liberi, per discriminare o attuare sorveglianza di massa. A differenza delle licenze open source tradizionali, che permettono un utilizzo senza restrizioni, RAIL introduce limitazioni specifiche sull'uso del modello per prevenire applicazioni dannose, come la discriminazione o la disinformazione. Sebbene il codice sorgente resti aperto, i modelli devono rispettare queste restrizioni d'uso per garantire che vengano applicati in modo etico e sicuro.

Tali restrizioni, però, entrano inevitabilmente in conflitto con la filosofia alla base del free software, che vieta ogni limitazione all'uso del software (prima libertà). Limitare l'uso del software è censura: in atto, una situazione peggiore di quella, potenzialmente verificatasi solo in potenza, dell'uso del software per scopi illeciti o non etici[24]: "un mondo in cui ci sia una proliferazione contradditoria di limiti all'utilizzo del software indrodurrebbe talmente tanto attrito da minare gli enormi benefici democratici che vi sarebbero tramite lo scambio continuo del software libero". Ad esempio, la preoccupazione è che si possa abusare di queste restrizioni per reprimere critiche, come impedire che il software venga usato per criticare certi soggetti o certi temi.

Come risposta alle preoccupazioni etiche nell'IA, la Free Software Foundation, il principale ente che promuove l'utilizzo del Free Software, propone invece strumenti alternativi come programmi di certificazione etica (ad esempio il "Respects Your Freedom") e codici etici per sviluppatori, escludendo dal novero del free software quel software che dovesse, ad esempio, spiare indiscriminatamente l'utente. Questi metodi, senza imporre restrizioni legali sull'uso del software, permettono se non altro di promuovere un utilizzo etico e consapevole, rispettando al contempo i principi di libertà su cui si fonda il free software.

Ancor più nel nuovo mondo dell'IA, è evidente che trovare un equilibrio tra la libertà di sviluppo e la responsabilità etica sia una sfida aperta e probabilmente destinata a non raggiungere mai una concreta conclusione.
Le soluzioni basate su licenze restrittive, come la RAIL, rispondono alla necessità di controllare l'uso delle tecnologie potenti, ma rischiano di frammentare il movimento open source, e sono chiaramente sconvenienti o del tutto invise alle imprese affermate nel settore – che preferiscono di gran lunga legare i propri progressi tecnologici a sistemi chiusi e vincolati, comprensibili e modificabili realmente soltanto dai loro creatori. D'altro canto, l'approccio radicale del free software difende una visione in cui la libertà di utilizzare e distribuire il software non deve mai essere compromessa, rimanendo convinta che la vera etica si costruisca non tramite il controllo ma tramite l'educazione e la trasparenza: si tratta di un argomento forse altrettanto estremo ed utopistico rispetto a quello della proprietà chiusa dei software, specialmente se si considera la diffusione e l'utilizzo degli strumenti di Intelligenza Artificiale anche presso un pubblico inesperto o comunque disinteressato a questi temi, che difficilmente troverà l'opportunità su larga scala di

[23] C. Munoz Ferrandis, Danish Contractor, H. Nguyen, D. Lansky, *The BigScience RAIL License*, https://bigscience.huggingface.co/blog/the-bigscience-rail-license
[24] J. Sullivan, *Building ethical software based on the four freedoms*, Free Software Foundation, 27 novembre 2019, https://www.fsf.org/bulletin/2019/fall/building-ethical-software-based-on-the-four-freedoms

documentarsi su un tema, quello del software aperto, che storicamente riguarda innanzi tutto una schiera tutto sommato ridotta di esperti ed appassionati, ben diversa rispetto all'utente medio di un generatore di immagini o di testo basato su IA.

3. L'Open source in relazione a trasparenza e responsabilità nello sviluppo e adozione di sistemi di IA

3.1. Limiti della riusabilità e riproducibilità nei sistemi IA, e le implicazioni legali per lo sviluppo e l'adozione di sistemi di IA

Si è visto che la crescente influenza sociale e tecnologica dei moderni sistemi di I.A. solleva domande critiche riguardanti la regolamentazione, l'etica e la sicurezza, rendendo in astratto necessaria una governance internazionale che possa affrontare queste sfide in modo coordinato, nella migliore delle ipotesi tramite una collaborazione generale tra stati, imprese private e organizzazioni internazionali nell'ottica di definire una volta per tutte un sistema di governance efficace, che, nello specifico dell'argomento primario di questo documento, sia innanzi tutto in grado di discernere ciò che è realmente open source e ciò che non lo è, e quali siano gli elementi costitutivi di tale definizione.

Questo iato normativo non solo limita il progresso tecnico e scientifico (o almeno, limita il controllo cui tale progresso è sottoposto, e ne lascia forse troppo liberi i fini e le metodologie), ma hanno anche conseguenze legali significative per lo sviluppo e l'adozione dell'IA.
La riusabilità, intesa come la capacità di riutilizzare un sistema o un modello IA in diversi contesti e applicazioni, è spesso limitata a causa di fattori intrinseci ai sistemi di apprendimento automatico. Molti modelli IA sono infatti altamente specializzati e ottimizzati per un compito specifico, il che riduce la loro adattabilità a scenari differenti.
Si tratta, in primo luogo, dei cosiddetti "modelli pre-trained", o, all'italiana, "pre-addestrati"[25], che cioè si specializzano in specifici campi e sono spesso utilizzabili "in locale", intendendo con ciò la possibilità per l'utente finale di far funzionare il sistema di IA sulla propria macchina ed utilizzando la di lei potenza computazionale, non dovendo per forza passare attraverso un sistema terzo (anche solo un sito web, come del resto funziona l'interfaccia basilare di ChatGPT).
In buona parte dei casi, e nella stragrande maggioranza per ciò che riguarda un uso occasionale o domestico degli strumenti di IA, si pone infatti una necessità di passare tramite sistemi terzi per fruire delle funzionalità di questa tecnologia. Ciò è in massima parte dovuto a due principali fattori:

[25] Nvidia, probabilmente la principale impresa attiva in questo momento nel settore computazionale riguardante l'IA, definisce così un modello pre-trainato: "è un modello di apprendimento profondo addestrato su grandi insiemi di dati per svolgere un compito specifico. Può essere utilizzato così com'è o ulteriormente perfezionato per soddisfare le esigenze specifiche di un'applicazione." Da https://blogs.nvidia.com/blog/what-is-a-pretrained-ai-model/#:~:text=A%20pretrained%20AI%20model%20is%20a%20deep%20learning%20model%20%E2%80%94%20an,fit%20an%20application's%20specific%20needs.

il primo, che è essenziale dotarsi di enorme potenza computazionale per arrivare all'output richiesto[26], dalla quale consegue la necessità di procurarsi un *hardware* particolarmente prestante, che soltanto pochissimi utenti sono in grado di avere (quand'anche siano in primo luogo consapevoli della sua necessarietà). Il secondo, già esplicitato, dovuto alla reticenza da parte delle grandi imprese dell'IA di rilasciare liberamente i propri codici sorgente, modelli, dati, pesi, e così via: insomma tutta la *suite* che in definitiva costituisce un sistema di IA e che sarebbe necessaria per modificarlo, copiarlo e aggiornarlo.

Un esempio significativo in tale senso è la dipendenza dai dati di addestramento e, di conseguenza, le loro prestazioni dipendono fortemente dalla qualità e dalla rappresentatività di questi dati.
Come qualsiasi sistema informatico, anche l'Intelligenza Artificiale fornisce un *output* a partire da un *input.* Questi dati sono a tutti gli effetti una forma di *input* precedente a quello dell'utente[27], e fornire enormi quantità di dati all'IA richiede una potenza computazionale impressionante, ben al di là di quanto un utente, per quanto professionale, possa ottenere all'interno dei propri locali e della propria attività.
Tramite questi dati, e a seconda della loro natura e della loro quantità, l'algoritmo è addestrato in modo da rispondere a richieste generiche (come avviene per i sistemi di IA generativa o con i chatbot), o per rispondere a richieste specifiche.
Se le richieste sono generiche, per avere un buon risultato nell'*output* è necessario fornire al modello quantità strabilianti di dati e poter effettuare l'addestramento con un *hardware*, prestazionalmente parlando, dalla potenza computazionale impressionante.
Se le richieste sono al contrario specifiche, ed il modello di IA non vuole essere generale ma settorializzato, allora si riducono anche le esose richieste *hardware* cui è sottoposto: i dati con cui l'algoritmo è addestrato sono minori, più localizzati e anche maggiormente comprensibili e controllabili. Si pensi in tale senso ai sistemi di IA per la gestione di compiti specifici, o per l'ausilio nella compilazione di documenti, nella gestione di tabelle e database, nell'analisi e divisione di grandi quantità di informazioni[28].
Va comunque menzionato come un minimo *pre-training* generale vada comunque compiuto anche presso questi modelli, dal momento che le abilità base di interfacciamento con l'utente debbono essere garantite: il modo di esprimersi in una certa lingua, la conoscenza sintattica e lessicale, e la corretta comprensione di termini anche tecnici sono tutti elementi per i quali è necessario un addestramento, anche computazionalmente intensivo, da parte degli sviluppatori sul modello.
La necessità di notevolissime prestazioni hardware in fase di addestramento, e di dati specifici per compiti specifici, pone quindi un doppio ostacolo alla replicabilità dei sistemi IA altrove: quali altri

[26] L. Heim, M. Anderljung, E. Bluemke, R. Trager, *Computing Power and the Governance of AI,* AI Centre for the Governance of AI, 14 febbraio 2024, https://www.governance.ai/post/computing-power-and-the-governance-of-ai

[27] Si intende con ciò far notare come esistano due "input": il primo, a priori, è quello dell'inserzione di enormi quantità di dati in un modello IA a partire dai suoi sviluppatori. Il secondo, a posteriori, è quello del singolo utente che "dice" al sistema di IA che cosa questi debba compiere, per esempio tramite una stringa di testo. Per ciò che concerne il discorso sulla potenza computazionale, l'"input" rilevante è il primo: quello degli sviluppatori.

[28] Più noti, forse sono i moderni motori per l'analisi di giochi complessi, come AlphaZero per gli scacchi o AlphaGo per il go, o i sistemi IA per migliorare la qualità dell'immagine a schermo, come l'Nvidia DLSS.

soggetti, oltre ai creatori del sistema, sono infatti in grado di mettere in campo una potenza computazionale sufficiente ed una mole di dati accettabile?

Ma anche per ciò che concerne *l'output* sono necessarie prestazioni *hardware* assolutamente non secondarie. Con ciò si intende la generazione del risultato finale a partire da una richiesta dell'utente.
Anche qui, il risultato finale può esplicarsi "in locale", cioè sulla macchina dell'utente finale, oppure tramite servizi terzi (come accade per ChatGPT o numerorissimi servizi di generazione di immagini o video, disponibili tramite API e dietro pagamento).
E anche per l'output si pone la stessa questione prestazionale dell'input: più l'output è potenzialmente generico, più risorse hardware sono richieste e più dati devono essere stati forniti all'algoritmo in fase di pre-training per avere un risultato accettabile. Se al contrario l'output è specifico, allora questi requisiti sono ridotti.
Attualmente, la capacità di generare un output preciso e tempestivo dipende fortemente dall'hardware impiegato, ed in particolare dalle GPU (Graphics Processing Units)[29], chiamate usualmente in italiano "Schede Video"[30], che sono essenziali sia per l'addestramento dei modelli sia per la generazione di output in tempo reale. La natura delle GPU le rende ideali per il calcolo di quei modelli di deep learning che richiedono l'elaborazione di matrici complesse e di grandi volumi di dati in parallelo. Questo è particolarmente importante sia durante l'addestramento (la fase di *training* precedentemente descritta), sia quando l'IA genera un risultato sulla base di una richiesta specifica (l'*output* di cui si sta parlando ora).

Sia la qualità dell'output, sia la velocità con la quale esso è stato raggiunto sono infatti influenzate esclusivamente dalle variabili prestazionali di tali componenti hardware e concorrono insieme alla concreta e reale possibilità di utilizzo delle IA: qualora venisse a mancare una sufficiente potenza computazionale, l'output impiegherebbe troppo tempo per essere raggiunto (o non potrebbe essere raggiunto affatto), oppure dovrebbe essere significativamente ridotto qualitativamente, cosa che non sempre è possibile fare.

Un esempio significativo dell'uso intensivo delle GPU in fase di output è rappresentato dai sistemi di riconoscimento vocale o dai sistemi di traduzione simultanea. In questi casi, le GPU devono processare grandi quantità di dati vocali o testuali in tempo reale per generare una traduzione o una trascrizione accurata. La traduzione automatica in tempo reale, come quella utilizzata da piattaforme come Google Translate, richiede una notevole quantità di potenza di calcolo per

[29] L'utilizzo delle GPU per il funzionamento dei sistemi di IA è motivato dal fatto che tali componenti siano ottimizzati per gestire simulatenamente migliaia di operazioni di calcolo e di dati in parallelo, ciascuno dei quali calcoli è però tendenzialmente semplice e precisamente definito. Al contrario, un CPU (o "processore", in italiano), è un componente estremamente versatile sviluppato per la gestione di calcoli complessi in maniera sequenziale: è necessario per il generale funzionamento del sistema, ma non può competere con le GPU nel momento in cui si tratta di operare in parallelo su calcolazioni specifiche.
[30] Nvidia, oggi spesso agli onori delle cronache e che sta attraversando un periodo di spettacolare successo sul mercato azionario, è appunto l'impresa principale che sviluppa e produce tali componenti.

elaborare il linguaggio naturale e produrre traduzioni fluide e coerenti in un'ampia varietà di lingue e contesti.
Un altro esempio può essere osservato nei sistemi di IA per la generazione di immagini. Piattaforme come MidJourney o lo stesso ChatGPTv4, che generano immagini su richiesta a partire da una descrizione testuale, richiedono GPU potenti per processare i milioni di parametri che compongono i modelli addestrati, se non direttamente unità di processamento dati ad-hoc (NPU, neural processing unit). Infatti, non possono che essere eseguiti su piattaforme terze, e non permettono la loro fruizione in locale, escludendone pertanto qualsiasi forma di riproducibilità. Più generico e ampio è il compito richiesto (ad esempio, la creazione di un'immagine dettagliata a partire da un prompt generico), più grande sarà la quantità di risorse computazionali impiegate, e meno frequentemente il modello sarà reso realmente aperto e disponibile per il pubblico.
In questi contesti, il modello di IA deve essere in grado di produrre output altamente specifici e dettagliati. L'inferenza può avvenire in pochi secondi, ma solo grazie all'uso di molteplici GPU all'avanguardia o financo sperimentali (con conseguente enorme consumo energetico[31]), che forniscono la potenza necessaria per gestire tali calcoli intensivi.

Volendo offrire un riassunto il più chiaro possibile di quanto appena esplicitato, si può affermare che esistano dunque tre caratteristiche fondamentali che devono tutte coesistere perché un sistema di IA possa essere creato da zero, oltre ovviamente al *know-how* dell'ente che volesse raggiungere quest'obiettivo:
1) La disponibilità di enormi quantità di dati lecitamente ottenuti e legalmente impiegabili.
2) La disponibilità di ingenti sistemi informatici dalle prestazioni elevate per il *training* del sistema.
3) La disponibilità di capacità computazionale sufficiente per ottenere infine un *output* accettabile, in termini di qualità e tempo impiegato.

Circa il punto 1), le problematiche legate alla riproducibilità e riusabilità hanno ovviamente importanti implicazioni legali. Nei contesti dove è necessaria la massima trasparenza, la mancanza di replicabilità può rendere difficile rispettare le normative che richiedono la verificabilità dei modelli IA.
Inoltre, si è già avuto modo di discutere su come la proprietà dei dati giochi un ruolo centrale nel grande puzzle che porta all'esistenza di un'IA realmente riproducibile. Anche se il codice può essere open-source, i dataset utilizzati per l'addestramento spesso non lo sono, limitando la possibilità di riprodurre esattamente i risultati di un modello. Ciò solleva questioni legali legate alla proprietà intellettuale e alla conformità con normative come il GDPR. Non solo il dataset utilizzato per l'addestramento del modello può infatti contenere dati la cui raccolta presenta problematicità secondo le attuali normative, ma anche lo stesso dataset può poi essere intellettualmente protetto, e l'illecito può realizzarsi a seguito del suo utilizzo non autorizzato.

[31] N. Chukwudum Ohalete et al., *Data Science In Energy Consumption Analysis: A Review Of Ai Techniques In Identifying Patterns And Efficiency Opportunities,* Engineering Science & Technology Journal, 4(6), pp 357-380, https://fepbl.com/index.php/estj/article/view/637

Non vanno poi sottovalutate le questioni inerenti alla responsabilità legale e alla necessaria presenza di una "catena di responsabilità" cui risalire nel momento in cui l'impiego di uno strumento di IA produca conseguenze nefaste. La risoluzione di questo problema, come si è indicato all'inizio, diventa ancora più complicata nel momento in cui il sistema è effettivamente open source, laddove è per natura pressoché impossibile generare una catena di responsabilità precisa ed attendibile.
Questi temi, e specialmente le possibili soluzioni in fase di implementazione in Europa, Cina e Stati Uniti, verranno analizzati nel prossimo capitolo.
Al di là delle soluzioni legislative, ne esistono però anche di tecnologiche: sistemi che sono concettualmente diversi da quelli tradizionalmente intesi per la raccolta dei dati o che offrono soluzioni *ab origine* per eliminare alcuni dei problemi di cui si è detto. Tra queste, si segnalano:
a) I dataset sintetici[32], cioè dataset formati da elementi artificiali che scimmiottano i dati reali ma non contengono ovviamente alcuna informazione sensibile. In un futuro sempre più vicino nel quale i dati generati da un sistema di IA siano indistinguibili da quelli reali, l'utilizzo di tali dataset potrebbe permettere l'addestramento di novelli sistemi di IA in totale sicurezza e senza doversi preoccupare di vincoli legislativi o di proprietà sull'utilizzo degli stessi[33]. Nonostante la corretta ed ovvia obiezione al fatto che tali dati siano per natura "finti", possono ricalcare le proprietà statistiche di quelli reali, e rivelarsi utili nell'insegnare a nuovi modelli operazioni basilari, come la necessaria competenza linguistica e sintattica che permetta la richiesta di *output* da parte dell'utente e la loro generazione in una forma per questi comprensibile[34].
Si pone inoltre il problema dell'origine dei dati sintetici, in una sorta di rivisitazione moderna dell'antico adagio "chi controllerà i controllori?": la generazione dei dati sintetici è lecita, e da quali fonti è provenuta?
b) Il Federated Learning, un metodo distribuito di addestramento dei sistemi di IA che ricorda il peer-to-peer, e che mira a risolvere contemporaneamente i problemi legislativi inerenti alla privacy dei dati raccolti ed i problemi tecnologici legati alla latenza nel trasferimento di dati di grandi dimensioni in blocco. Con il Federated Learning l'algoritmo di apprendimento viene distribuito su molteplici dispositivi (si pensi a diversi computer, smartphone e così via), detti "nodi", ciascuno dei quali esegue l'addestramento localmente. La potenza computazionale è quindi distribuita e cresce al crescere dei dispositivi connessi. Senza un server centrale di riferimento, tutti i dispositivi inviano di volta in volta solo gli aggiornamenti del modello da loro svolte (si pensi ai pesi o a vari parametri di ottimizzazione): piccoli pacchetti di informazioni sono continuamente condivisi, invece di avere, come avviene tradizionalmente, un grande blocco che va aggiornato completamente ogni volta. Nonostante l'idea sembri promettente, permangono perplessità legate al cosiddetto fenomeno dell'*avvelenamento dei modelli*, tramite il quale è possibile sabotare la buona riuscita del training attraverso l'invio malevolo di dati volutamente errati.

[32] S. Nikolenko, *Stnthetic Data for Deep Learning,* Springer, 2021
[33] Karen L. Boyd. *Datasheets for Datasets help ML Engineers Notice and Understand Ethical Issues in Training Data*. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, 2021, https://doi.org/10.1145/3479582
[34] K. Yasar, *What is synthetic data? Examples, use cases and benefits,* Techtarget.com, https://www.techtarget.com/searchcio/definition/synthetic-data

Circa i punti 2 e 3, invece, la questione sembra più strettamente legata alla disponibilità di hardware prestazionalmente elevato a costi di produzione e di utilizzo accessibili, intendendo con ciò sia il prezzo del componente in sé, sia il suo costo di utilizzo in termini di manutenzione e soprattutto di dispendio energetico.
In questo senso, si vuole offrire una visione parzialmente ottimistica su ciò che il futuro potrà offrire, basandosi sullo storico incremento prestazionale che di anno in anno i componenti hardware ottengono[35] e sulla significativa velocità con il quale questo avviene, ulteriormente aumentata dalla recente accelerazione che l'interesse sull'IA ha comportato[36].
Già negli ultimi anni, le schede video commercialmente disponibili anche per utenti privati consentono l'esecuzione di modelli di IA sulla propria macchina locale, e potenzialmente offrono sufficiente capacità computazionale per lo sviluppo di propri, nuovi modelli, seppure nella gran parte dei casi inferiori rispetto alle alternative proprietarie.
Il problema in questo senso attiene alla fase di pre-training, che richiede ancora una potenza computazionale spesso irraggiungibile. Gli utenti finali sono pertanto spinti ad utilizzare modelli già pre-addestrati e a fornire a loro soltanto i dati specifici che servono al raggiungimento di uno scopo preciso. Si pensi in tale senso alla possibilità di realizzare immagini in locale tramite il noto modello *Stable Diffusion*. Aggiungendo al programma pre-addestrato i cosiddetti "checkpoint", cioè i dati finali di addestramento, è possibile generare immagini con stili diversi e con maggiore o minore definizione e, conseguentemente, più o meno computazionalmente intensivi[37]. L'importanza di generare e mantenere *input* e *output* in locale è fondamentale: l'utente deve poter mantenere, se lo desidera, il controllo sui suoi dati senza essere costretto a passare presso sistemi terzi, che lo limitano, ne carpiscono spesso il comportamento per fini economici, e in molti casi non sono

---

[35] Un esempio non direttamente legato all'Intelligenza Artificiale ma estremamente indicativo del futuro a venire può derivare da un famoso video Youtube chiamato "*I Remade Iron Man VFX With $20",* disponibile al link https*://www.youtube.com/watch?v=ZyChddyTrY8,* nel quale l'autore, ErikDoesVFX, replica oggi, migliorandoli, alcuni effetti speciali di un popolare film statunitense del 2008 con un budget di 20$ a fronte dell'impiego della produzione hollywoodiana, più di quindici anni prima, di oltre 400 esperti di effetti speciali.

[36] Un'accelerazione sulla quale vale la pena riflettere, dal momento che non sempre ha davvero giovato alla qualità dei componenti impiegati: la ricerca della prestazione a tutti i costi ha dato origine, negli ultimi anni, a significativi problemi hardware dovuti, in sintesi, alla volontà di ottenere il massimo della velocità sul singolo componente senza aver contestualmente portato reali migliorie alla qualità materiale e ai processi produttivi, né avendo portato innovazioni tecnologiche e metodologiche.
Da ciò sono derivati i recenti scandali Intel, i cui processori di 13° e 14° generazione hanno iniziato a mostrare malfunzionamenti o a smettere di funzionare in larghissimo numero (si veda https://www.pcworld.com/article/2415697/intels-crashing-13th-14th-gen-cpu-nightmare-explained.html#:~:text=Intel's%2013th%2D%20and%2014th%2Dgeneration,permanent%20damage%20for%20many%20users) ed un generale malcontento per le schede video Nvidia, viste come sovrapprezzate a causa dell'enorme aumento della loro domanda (https://www.mmo-champion.com/threads/2636852-Nvidia-4000-series-is-now-officially-a-waste-of-sand), e costruite in modo approssimativo: https://www.techradar.com/computing/gpu/this-graphics-card-generation-is-over-and-it-was-mostly-trash

[37] In altre parole, Stable Diffusion, pre-addestrato, consente la generazione di immagini. Il tipo e la qualità delle immagini è determinato dai dati finali di addestramento, disponibili per l'utente e condivisi tra utente, chiamati "checkpoint". Ogni checkpoint porta con sè uno stile ed una qualità diversa nell'output delle immagini. L'utente è poi in grado di determinare quale checkpoint usare e di determinarne, con ulteriori parametri, la qualità finale. A titolo di esempio, per mostrare la potenza computazionale richiesta, la realizzazione di un'immagine in HD (a risoluzione 1920x1080), con un checkpoint di media qualità, richiede un hardware di fascia alta, con una scheda grafica che possegga almeno 12GB di memoria video, e dura in media circa trenta secondi. In comparazione, servizi terzi come ChatGPTv4, Midjourney o Dall-e generano immagini qualitativamente elevate a risoluzioni anche superiori in circa dieci secondi.

disponibili gratuitamente. Inoltre, è facile ipotizzare questioni di sicurezza inerenti alla diffusione di dati e informazioni per le quali l'utilizzo di sistemi di IA terzi può non essere possibile.

La somma di questi ostacoli alla riproducibilità di sistemi IA è generalmente noto come "la crisi della riproducibilità"[38]. Questa crisi si manifesta su due fronti principali: da un lato, come si è visto, è il settore dell'IA ad essere concretamente difficile da riprodurre; dall'altro, però, riverbera questa sua difficoltà negli studi scientifici su di essa.
La complessità dei modelli di IA, l'opacità dei dati, i parametri generalmente nascosti con cui vengono dati pesi e misure per la produzione degli output, tutti contribuiscono a rendere difficile la riproducibilità degli studi e degli esperimenti nel campo dell'IA. Questa mancanza di riproducibilità non solo ostacola il progresso scientifico, ma mina anche la fiducia nei risultati ottenuti, poiché non possono essere verificati o validati da altri ricercatori.

Senza la possibilità di replicare con precisione e prevediblità gli esperimenti diventa pressochè impossibile elaborare nuove conoscenze basate su risultati pregressi. La scienza progredisce attraverso la verifica e la validazione di teorie antistanti, e la mancanza di riproducibilità interrompe questo processo fondamentale.

In generale, viene rilevata una tendenza crescente in cui studi ad alto profilo mancano di dettagli cruciali. Anche in campi come la biologia e la fisica, dove le informazioni necessarie per replicare gli esperimenti sono ancora più fondamentali, si rilevano mancanze[39]. Non esistendo, come si è già potuto osservare, linee guida universali per la documentazione e la condivisione dei risultati nel campo dell'IA, è inevitabile lo svilupparsi di pratiche non uniformi o standardizzate.
Le iniziative più generalmente proposte per risolvere questa "crisi" possono riassumersi così:

- **Promozione della trasparenza**: Incoraggiare la condivisione aperta di codici, set di dati e dettagli sperimentali attraverso piattaforme pubbliche e repository liberamente accessibili.
- **Standardizzazione delle pratiche**: Sviluppare e adottare linee guida comuni per la documentazione e la verifica dei risultati nel campo dell'IA.
- **Requisiti necessari di riproducibilità**: Le riviste scientifiche e le conferenze dovrebbero richiedere la disponibilità di materiali riproducibili come criterio per la pubblicazione.
- **Formazione e sensibilizzazione**: Educare ricercatori e sviluppatori sull'importanza della riproducibilità e sulle migliori pratiche per conseguirla.

Anche a fronte del verificarsi di queste proposte, rimane comunque un ostacolo fondamentale per la totale riproducibilità dei sistemi di IA per come sono sviluppati oggi: l'accesso limitato a hardware a prestazioni elevate impedisce di fatto di replicare senza alcuna approssimazione studi, o semplici modelli, che richiedono elevate risorse computazionali.

[38] O. E. Gundersen, *Ther Reproducibility Crisis Is Real,* Association for the Advancement of Artificial Intelligence, 2020, https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/download/5318/7246
[39] W. D. Heaven, *AI is wrestling with a replication crisis*, technologyreview.com, 12 novembre 2020, https://www.technologyreview.com/2020/11/12/1011944/artificial-intelligence-replication-crisis-science-big-tech-google-deepmind-facebook-openai/

3.2. Auditing di sistemi IA: stato legislativo in Europa, Stati Uniti e Cina

Auditing I.A. in Unione Europea

Per "auditing" si intende generalmente la metodologia e le regole che stanno alla base della verifica dei sistemi di intelligenza artificiale da parte di organi indipendenti, e nello specifico di quelli statali. Collegando quanto appena detto a ciò che è stato scritto precedentemente, un auditing completo dovrebbe prendere in esame i modelli in sé, i dati sui quali sono stati addestrati, e l'output atteso, nell'ottica di definirne il livello di trasparenza e la conformità legislativa, nonché, il loro grado di apertura, o "openness".

L'auditing attiene qualsiasi forma di intelligenza artificiale, intendendo con ciò le funzioni fondamentali che con tale tecnologia possono essere svolte.
Si è soliti infatti distinguere, innanzi tutto, l'I.A. "Generativa", che è probabilmente la più nota e agli onori delle cronache e che è costituita da modelli progettati per generare contenuti nuovi e originali, come testi, immagini o video.
Ma oltre all'IA Generativa si segnala primariamente l'IA "Analitica", progettata per analizzare dati storici ed identificarne ripetizioni e schemi, nella speranza di prevedere eventi futuri a partire da condizioni simili.
Altre forme di IA si definiscono "Descrittive" quando semplicemente forniscono informazioni comprensibili o sintetizzate a partire da grandi quantità dati difficilmente fruibili per l'essere umano, e IA "Operative", che cioè svolgono pedissequamente compiti ripetitivi, anche complessi.
La fantascienza, ma soltanto questa, conosce infine l'IA "Generale", cioè il grande spauracchio di un unico sistema che sia in grado di fare tutto.

La fonte normativa primaria sul tema è rappresentata attualmente senz'altro dall'AI Act, entrato in vigore il 1° agosto 2024 e che sarà applicabile a partire dal 2 agosto 2026, che introduce un quadro legislativo basato su un approccio al rischio, classificando i sistemi IA in base alla loro potenziale pericolosità, e impone per essi specifiche regole a cadenze temporali differenti[40].
Seguendo lo stile legislativo di precedenti atti, come il GDPR, si applica anche "ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, laddove l'output prodotto dal sistema sia utilizzato nell'Unione". In altre parole, qualsiasi soggetto che esperisca effetti nel mercato dell'Unione tramite sistemi di IA è sottoposto alla normativa dell'AI Act.
E, si diceva, l'entrata in vigore effettiva di numerose sue regole è cadenzata. Queste, sintetizzate, sono le sue scadenze temporali principali:
1 Agosto 2024: Entrata in vigore; da questo momento iniziano a computarsi le scadenze future.

[40] H. Beverley-Smith, E. J A Evans, C. H N Perowne, *The EU Artificial Intelligence Act Comes Into Force on 1 August 2024*, https://www.faegredrinker.com/en/insights/publications/2024/7/the-eu-artificial-intelligence-act-comes-into-force-on-1-august-2024

2 Febbraio 2025[41]: I sistemi di IA il cui rischio è ritenuto inaccettabile divengono proibiti.
Si includono in questi le IA per manipolare subliminalmente o sfruttare le vulnerabilità delle persone che possono causare danni fisici o psicologici, l'uso indiscriminato di identificazione biometrica in tempo reale in spazi pubblici o l'uso di 'punteggi sociali' derivati dall'IA da parte delle autorità (uso che potrebbe svantaggiare ingiustamente individui o gruppi già vulnerabili).
2 Agosto 2025: Le norme divengono efficaci per i sistemi di IA generale, che possono cioè svolgere molteplici funzioni lungo settori differenti: l'esempio più tipico è rappresentato dalle IA generative quali ChatGPT, Copilot, Bard, e così via, ma si comprendono anche i sistemi dedicati alla generazione di immagini o video, anche se sono integrati in sistemi più onnicomprensivi.
2 Agosto 2026: L'AI Act si applicherà a tutti i sistemi determinati nell'Allegato 3 dell'Atto come ad Alto Rischio, includendo con ciò i sistemi dedicati alla gestione del personale, alle analisi biometriche e alle analisi di accesso ai servizi.
2 Agosto 2027: Vengono sottoposti alla disciplina dell'AI Act i sistemi ad alto rischio categorizzati nel primo allegato. Si tratta di sistemi di IA utilizzati in prodotti soggetti alla legislazione dell'UE sulla sicurezza dei prodotti, includendo con ciò i giocattoli, gli aeromobili, i dispositivi ad uso medico, e gli ascensori o montacarichi.
30 Dicembre 2030: l'AI Act si applicherà infine per quelle IA facenti parte di sistemi su larga scala già creati a partire da norme europee nei settori delle garanzie di libertà, di sicurezza e di giustizia, come lo Schengen Information System[42].

Da ciò discende la necessità, per le imprese che si occupino di sviluppare o di operare sui sistemi di IA, ed anche per quelle che semplicemente ne fruiscono, di controllare il rischio degli stessi e rispettare i requisiti imposti dall'AI Act. Inoltre, la legge impone alle organizzazioni creatrici dei sistemi di incorporare meccanismi di conformità sull'AI Act prima che i sistemi siano immessi sul mercato, per garantire che le loro tecnologie di IA soddisfino gli standard legali fin dall'inizio.

Ma le imprese materialmente creatrici dei sistemi di IA non sono le uniche ad essere coinvolte nell'ambito applicativo dell'AI Act: a partire dall'articolo 2, oltre ai fornitori e distributori di tali servizi si parla di "deployer", definiti poi con precisione all'articolo 3 come "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale". Da ciò discende la conseguenza che a chiunque utilizzi un sistema di IA per esigenze professionali è demandato seguire le regole dell'AI Act, ed accertarsi pertanto che le prescrizioni sull'utilizzo di tali sistemi siano rispettate dal sistema stesso utilizzato.
È importante, tuttavia, notare quanto segue: l'IA Act è un testo legislativo sterminato, con una notevolissima parte dedicata ai preamboli e numerosi allegati, ai quali è dato rimando spesso negli articoli concreti del testo. Intende essere una fonte generale sul tema dell'I.A., mirando più ad obiettivi che a prescrizioni sul come raggiungerli.
Gli audit propriamente detti di tali sistemi di IA, pur non essendo specificamente obbligatori per i fornitori e gli implementatori ai sensi dell'AI Act, possono logicamente fornire una solida base per

[41] Art. 113 AI Act, https://artificialintelligenceact.eu/article/113/
[42] Art. 111 AI Act, https://artificialintelligenceact.eu/article/111/

garantire la conformità a molte delle sue disposizioni, non dissimilmente di come avveniva in tema di privacy dopo l'introduzione del GDPR. L'AI Act a più riprese infatti pone l'accento sui principi di equità (Racc. 74, 110, 27), supervisione umana (Art. 14), accuratezza (Art. 15) e trasparenza (Art. 50)[43].

Il problema principale di un simile ragionamento è causato dall'indeterminatezza delle procedure da seguire, che, seppure in teoria commisurate al rischio e quindi ragionevolmente desumibili a seconda dell'attività svolta, possono essere diverse per gli utilizzatori finali rispetto a quelle delle autorità nazionali previste dall'AI Act all'articolo 28, incaricate di vigilarne la conformità. In altre parole, nell'assenza di precise indicazioni e di un consenso generalizzato sul tema[44] può determinarsi il problema di imprese che operino procedure di audit ritenute poi insufficienti dalle autorità nazionali, senza però che vi sia per esse un'effettiva prescrizione legislativa, a tutto svantaggio del principio di certezza del diritto.

Non solo: **le problematiche di trasparenza, irreplicabilità e generale opacità dei sistemi di intelligenza artificiale descritte nel capitolo precedente rientrano qui per complicare ulteriormente gli sforzi di quanti, ultimi utilizzatori o "deployer" di un sistema di IA, vogliano assicurarne il rispetto dei principi espressi nell'AI Act**. Questo problema si accentua ed investe altri ambiti del diritto ancora quando i dati originali sui quali il sistema è stato addestrato non sono pubblicamente disponibili per motivi di riservatezza o proprietà intellettuale.

Uno dei progetti più rilevanti che mira a risolvere questo tema è l'AI Auditing Project, proveniente dalla Commissione Europea. Questo progetto si propone di sviluppare metodologie pratiche per valutare la conformità dei sistemi IA alle normative europee, in particolare al GDPR[45]. L'auditing si concentra principalmente sulla valutazione della protezione dei dati e sulla trasparenza degli algoritmi, con l'obiettivo di fornire strumenti che aiutino le autorità a verificare se i sistemi IA rispettano le garanzie di protezione dei dati. Questo progetto prevede l'uso di checklist e strumenti di auditing per ispezionare i modelli IA, migliorare la trasparenza e garantire che i sistemi rispettino le normative sulla privacy e i diritti umani.

Nonostante sia centrato sul rispetto del GDPR, l'AI Auditing Project offre interessanti spunti "per assicurarsi che gli sviluppatori e gli implementatori di sistemi di IA abbiano rispettato tutte le misure necessarie, in ogni momento, per assicurarsi che l'impatto dei loro sistemi sia compatibile con la legislazione esistente", ma nonostante ciò, si affretta ad affermare che "le procedure utilizzate dalle autorità nazionali potrebbero essere differenti"[46], sollevando alcune legittime perplessità.

---

[43] M. Martin Zamorano Barrios, *AI Audits: How do you implement the EU AI Act?*, Trilateral Research, 24 luglio 2024, https://trilateralresearch.com/artificial-intelligence/ai-audits-how-do-you-implement-the-eu-ai-act#:~:text=The%20introduction%20of%20the%20AI,principles%2C%20and%20relevant%20societal%20values.

[44] E. Thelisson, H. Verma, *Conformity assessment under the EU AI act general approach*, AI and Ethics, Springers, 3 gennaio 2024, vol.4

[45] *AI Auditing*, https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing_en#:~:text=The%20AI%20Auditing%20project%20aims%20to%20map%2C%20develop,initiative%20of%20the%20Spanish%20Data%20Protection%20Authority%20%28DPA%29.

[46] G.Galdon Clavell, *AI Auditing, Checklist for AI Auditing*, https://www.edpb.europa.eu/system/files/2024-06/ai-auditing_checklist-for-ai-auditing-scores_edpb-spe-programme_en.pdf

Ciononostante, offre innanzi tutto un sistema di checklist, o una "model card", com'è definita, che gli sviluppatori dei sistemi di IA dovrebbero offrire a quanti usufruiscano del loro servizio, contenente informazioni sui quali a loro volta, se ne fanno un uso professionale, dovranno accertarsi di essere edotti. L'idea non è certamente nuova[47], e già da alcuni anni si sono susseguite proposte, in particolare di matrice statunitense[48]. Generalmente, i requisiti della model card teorizzata dall'AI Auditing Project si possono riassumere così:

Informazioni generali:

- Nome del sistema di IA, versione, data di distribuzione e cronologia delle versioni.
- Dati del proprietario del sistema e dei fornitori, e ruolo dei fornitori.
- Livello di rischio in base all'AI Act.
- Documentazione esistente.

Informazioni sull'utilizzo e sul trattamento dei dati

- Descrizione degli scopi previsti, utilizzi, contesto e ruolo/servizio fornito (Articoli 5.1.b, 5.2 e 24.1 GDPR)
- Contesto organizzativo nel quale se ne presuppone l'uso
- Eventuale necessità di ruoli umani

Informazioni sui dati di addestramento/validazione

- Fonti dei dati/metodologia di raccolta (Articoli 5 e 9 GDPR)
- Tipi di dati e caratteristiche (Articoli 5.1.a, b GDPR)
- Implementazione di sistemi di Privacy by Design (Articolo 25 GDPR)
- Dataset (Articoli 5.1.a, b GDPR)

Informazioni sul modello

- Metodo utilizzato nella creazione del modello
- Output semplificati
- Variabili decisionali

Informazioni su bias e impatti (in laboratorio/ambienti operativi)

- Metriche (Articoli 5.1.a e 5.1.b GDPR)
- Categorie protette (Articoli 13.1.e, 14.1.e e 35.9 GDPR)
- Tassi d'impatto per categoria e profilo (Articolo 5.1.d GDPR)

Informazioni sui meccanismi di ricorso:

---

[47] M. Arnold, R. K. E. Bellamy, M. Hind, S. Houde, S. Mehta, A. Mojsilović, R. Nair, K. Natesan Ramamurthy, A. Olteanu, D. Piorkowski, D. Reimer, J. Richards, J. Tsay, and K. R. Varshney. 2019. *FactSheets: Increasing trust in AI services through supplier's declarations of conformity*. https://doi.org/10.1147/JRD.2019.2942288

[48] Ke Yang, Julia Stoyanovich, Abolfazl Asudeh, Bill Howe, HV Jagadish, and Gerome Miklau. 2018. *A Nutritional Label for Rankings*. In Proceedings of the 2018 International Conference on Management of Data (SIGMOD '18), May 27, 2018. Association for Computing Machinery, New York

- Informazioni di trasparenza (“explainability”) dell’algoritmo (Considerando 71 GDPR)
- Meccanismi di ricorso o revisione (Articoli 13.2.f, 14.2.g e 15 GDPR)

Non solo. Nell’ambito di un *audit* più approfondito quale quello che l’AI Auditing Project assume possa essere svolto da una autorità nazionale di controllo, in particolar modo legato al trattamento dei dati personali, si individuano quattro punti chiave:

1) La necessità di uno **scopo** chiaramente identificato e documentato. Si deve assicurare che l'uso della componente di IA sia in relazione con l'obiettivo finale del trattamento e conforme alle condizioni di liceità previste dalla normativa, oltre a stabilire i requisiti per gli operatori umani che supervisionano il sistema.
2) E’ opportuno stilare **un’analisi della proporzionalità e necessità,** che comporti la valutazione dell'uso del sistema di IA paragonandolo ad altre opzioni, focalizzandosi sui diritti e le libertà degli interessati. Si devono considerare i rischi introdotti dall'IA nel trattamento dei dati e documentare le motivazioni per la sua implementazione.
3) Similmente a quanto già accade secondo il GDPR, la **limitazione della conservazione dei dati** richiede che i dati personali siano conservati solo per il tempo necessario alle finalità del trattamento, identificando le basi legali per eventuali periodi di conservazione estesi.
4) Infine, un'**analisi delle categorie di interessati** dovrebbe comportare l'identificazione delle persone coinvolte e la valutazione delle conseguenze a breve e lungo termine che l'implementazione della componente IA può avere su di loro.

L’AI Auditing Project pone peraltro una notevole attenzione nei confronti delle fonti di *bias* algoritmico possibilmente presenti nei sistemi di IA utilizzati professionalmente. In questo caso, però, si ripete un problema già precedentemente individuato: una vera e propria valutazione di questo tipo richiede l’accesso completo ai *dataset* utilizzati in fase di addestramento. Questo, come si è visto, non è quasi mai possibile, a causa dell’opacità tipica di tali informazioni, e sarebbe irragionevole richiedere che un privato intraprenda una lunga e complicata analisi di un tema estremamente tecnico e specifico che potrebbe essere perfino completamente al di fuori del suo controllo.
E’ probabilmente per questi motivi che l’AI Auditing Project concentra questa parte riguardante il bias come prerogativa delle investigazioni svolte dalle autorità di supervisione, come a comprendere la concreta impraticabilità di simili requisiti per il pubblico finale che acquisisce ed utilizza sistemi di IA.

Riguardo proprio questo tema della possibile discrepanza nella valutazione algoritmica tra autorità nazionali e imprese private, è da segnalarsi l'*European Centre for Algorithmic Transparency*[49], istituito dalla Commissione Europea già nel 2023 per fornire competenze scientifiche e tecniche per l'applicazione del Digital Services Act (DSA), in particolare riguardo alla trasparenza e alla responsabilità dei sistemi algoritmici utilizzati dalle piattaforme online. Tra questi, spicca l’analisi e

[49] *European Centre for Algorithmic Transparency,* https://algorithmic-transparency.ec.europa.eu/index_en

la valutazione di quegli algoritmi che sono utilizzati dalle piattaforme online di grandi dimensioni (le VLOPS, *very large online platforms)*[50].
Sviluppando metodologie e strumenti per l'audit algoritmico, l'ECAT può aiutare contestualmente a standardizzare il modo in cui i sistemi di IA sono valutati in tutta l'Unione Europea, fungendo da hub centrale di competenza sul quale i regolatori nazionali potranno fare affidamento.
È prevedibile che nei prossimi mesi o anni il centro diventerà più attivo e visibile nel suo ruolo di monitoraggio e analisi dei sistemi algoritmici.

La necessità per i soggetti finali che utilizzano sistemi di IA di poter acquisire una consapevolezza completa dello strumento, e di conseguenza anche dei dati da esso utilizzati, mette in ulteriore risalto l'importanza di fare chiarezza sul tema degli standard open source, e di come il termine sia attualmente spesso svuotato di significato. Di questo argomento si offrirà maggiore approfondimento nel prossimo capitolo.

Auditing I.A. negli Stati Uniti

Oltreoceano, la regolamentazione dell'intelligenza artificiale si trova ancora ad uno stadio embrionale, complice anche la natura volutamente frammentaria del diritto degli Stati Uniti, già resa evidente in materia di privacy[51].
Tuttavia, esistono progetti messi in campo da agenzie federali e statali che mirano a sviluppare metodologie per far fronte ai rischi inerenti allo sviluppo dell'IA, nonché a fornire linee guida su come poter effettuare analisi su di esse, *auditing* propriamente detti in modo non dissimile a quanto descritto per l'Unione Europea.
Il primo di questi progetti, o *framework*, come spesso vengono definiti in lingua originale, appartiene al **NIST,** l'Istituto Nazionale per gli Standard e la Tecnologia. Il NIST è un'agenzia federale che opera sotto il dipartimento del Commercio incaricata di sviluppare "standard, linee guida e strumenti di misuramento" in diversi settori, principalmente tecnologici. Negli anni recenti, il NIST si è concentrato molto sulla cybersicurezza, e per ultimo sull'IA[52].
Nel 2023, il NIST ha pubblicato un *AI Risk Management Framework*, che offre un approccio preciso per le imprese che vogliano effettuare analisi del rischio su sistemi di IA[53]. Ovviamente, l'approccio è più volte definito "volontario", mancando una fonte legislativa cogente che obblighi le imprese a svolgere tali compiti.

[50] Qui una lista di queste piattaforme: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413. Figurano, tra gli altri, Amazon, Google, Facebook, Instagram, Wikipedia, Youtube, Twitter.
[51] Si veda in questo senso il California Consumer Privacy Act, una legislazione con numerose somiglianze al GDPR europeo, ma valevole soltanto per lo stato della California: https://oag.ca.gov/privacy/ccpa.
[52] Da https://www.nist.gov/itl/ai-risk-management-framework/roadmap-nist-artificial-intelligence-risk-management-framework-ai
[53] NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

L'obiettivo dichiarato del framework è quello di migliorare la *trustworthiness* dei sistemi di IA, intendendo con ciò l'affidabilità sia reale che percepita da parte del pubblico e dell'impresa: quanto, in altre parole, è possibile "affidarsi" all'IA, e fidarsi dei suoi output.
Per fare ciò, il NIST suggerisce un approccio quadripartito:

1) Governare ("Govern")
   Nella prima fase, vengono istituite politiche, procedure, definizioni e strutture organizzative che supportino una gestione efficace dei rischi dell'IA. Oltre all'istituzione di una catena di responsabilità, si suggerisce di stabilire linee guide interne che guidino l'utilizzo e l'eventuale sviluppo di sistemi di IA, e di assicurarsi che le attività relative agli strumenti di IA siano in linea con le leggi e i regolamenti applicabili.
2) Mappare ("Map") il sistema di IA.
   Si intende con ciò comprendere approfonditamente il contesto in cui il sistema di IA si troverà ad operare. Non si intende qui comprendere il funzionamento del sistema, ma semplicemente individuare gli obiettivi perseguiti, le parti interessate (i cosiddetti "stakeholder") e i potenziali impatti, specialmente qualora esistano normative locali applicabili ai casi di utilizzo.
3) Misurare ("Measure") il sistema di IA.
   Questo significa valutare e analizzare i rischi che l'utilizzo del sistema di IA comporta. In primo luogo, si tratta di valutare l'accuratezza, la precisione e l'efficacia del sistema, individuando al contempo eventuali pregiudizi nei dati o vizi negli algoritmi che potrebbero portare a *bias* o malfunzionamenti. Il NIST sembra osservare la questione più che altro dalla parte degli utilizzatori finali, che devono misurare il sistema sulla base degli output in una fase di test prima di impiegarli realmente. Non si tratta dunque di suggerimenti o requisiti per gli sviluppatori di sistemi di IA, quanto piuttosto di metodologie che gli utilizzatori finali possono adoperare per capire, nei limiti delle loro possibilità, se l'IA impiegata sia sufficientemente affidabile.
4) Gestire ("Manage")
   Nella fase di "gestione", vengono implementate strategie e controlli per mitigare i rischi precedentemente identificati. Si tratta di pianificare azioni specifiche che riducano l'impatto dei rischi e ne controllino periodicamente lo stato.

Il NIST ha poi esteso il suo framework originale, basato sull'IA in generale, con un Generative AI Profile[54]. Questo "profilo" fornisce linee guida specifiche per la gestione dei rischi associati ai sistemi di intelligenza artificiale generativa, che com'è noto sono modelli di IA capaci di creare, a partire da un input utente, nuovi contenuti come testo, immagini, audio o video.
Secondo il *Profile*, esistono i seguenti rischi unici associati all'IA generativa, dei quali gli utilizzatori devono tenere conto ulteriormente nel momento in cui vogliano seguire il precedente *Framework.*

[54] NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf,

A conferma della provenienza statunitense del documento, tra questi rischi ne figurano anche alcuni di quasi fantascientifici, come un aumentato rischio di accesso ad armi nucleari o biologiche. Si offre qui una sintesi di quelli più rilevanti:

- **Allucinazioni**: La generazione di contenuti plausibili ma errati o privi di senso.
- **Misinformazione e Disinformazione**: La possibilità di creare e diffondere informazioni false, intenzionalmente o meno.
- **Deepfake e Media Sintetici**: La creazione di immagini, audio o video realistici ma falsi che possono ingannare e manipolare.
- **Rischio dipendenza**: Possibili rischi derivanti dall'interazione tra umani e sistemi IA, tra cui eccessiva dipendenza, bias di automazione o confusione tra IA e umano.
- **Bias e Questioni Etiche**: La potenziale generazione di contenuti che riflettono o amplificano bias presenti nei dati di addestramento.
- **Violazione della Proprietà Intellettuale**: Rischi di produrre contenuti che violano diritti d'autore o altri diritti di proprietà intellettuale.
- **Violazioni della Privacy**: Possibile esposizione di informazioni sensibili o personali attraverso i contenuti generati.

Sforzi per offrire una regolamentazione comune dell'AI e sancire regole precise sui suoi requisiti provengono anche dal potere esecutivo degli Stati Uniti. Già alla fine del 2023, la Casa Bianca ha ritenuto di promulgare un Executive Order per chiamare all'azione le compagnie più attive nel settore dell'IA (su base volontaria), per offrire aiuto sul tema[55].

Da questa iniziativa può ritenersi iniziato l'iter che ha portato all *Validation and Evaluation for Trustworthy AI Act,* o *VET AI Act*, iniziativa legislativa bipartisan del Senato degli Stati Uniti che mira a dare una base normativa, quindi obbligatoria, ai sistemi di auditing e di gestione del rischio per i sistem di intelligenza artificiale[56].

Il VET AI Act mira a sviluppare dettagliate linee guida prendendo in esame sia audit esterni che audit interni, intendendo quindi dare regole sia agli enti di controllo, sia agli stessi utilizzatori dei sistemi di IA, uniformando la disciplina.

La legge, attualmente allo stadio di semplice proposta, consentirebbe di effettuare valutazioni indipendenti da parte di terzi per verificare le affermazioni che le aziende di IA fanno sui loro sistemi. Queste valutazioni coprirebbero aree come la funzionalità del sistema, la mitigazione degli errori e la privacy dei dati, avendo come modello i revisori indipendenti nel settore finanziario. Il NIST, inoltre, già precedentemente citato, dovrà agire in coordinamento con altre agenzie federali, per la creazione di linee guida e simulazioni per identificare le vulnerabilità nei sistemi di IA. Questi

[55] The White House, *FACT SHEET: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitment on AI*, 26 luglio 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announces-new-ai-actions-and-receives-additional-major-voluntary-commitment-on-ai/

[56] S.4769 *VET Artificial Intelligence Act*, Congress.gov, https://www.congress.gov/bill/118th-congress/senate-bill/4769/text/is

protocolli di gestione del rischio diventerebbero dunque standardizzati, e, in massima sintesi, valuterebbero i danni potenziali, la qualità dei dati e la sicurezza del sistema.

All'interno della tipica frammentazione normativa che si rinviene usualmente negli Stati Uniti, si rilevano anche varie linee guida e standard per settori specifici[57]. Ad esempio, il Dipartimento dell'Energia ha lanciato un programma pilota per valutare l'uso energetico dell'IA[58] e potenziali ottimizzazioni dello stesso, e il Dipartimento per la Sicurezza Nazionale ha creato ampie linee guida per utilizzare l'IA nei settori della sorveglianza e della gestione delle emergenze[59]. In tutte queste iniziative si notano gli stessi obiettivi descritti lungo tutto il documento: la necessità di stabilire linee guida e criteri precisi per determinare l'affidabilità di un sistema di IA; gestire e comprendere i rischi nel miglior modo possibile; proteggere i dati personali.

Auditing I.A. in Cina

L'attenzione della politica cinese sul tema dell'intelligenza artificiale è evidente da molti anni. A partire dal 2017, con il *New Generation AI Development Plan*, sono state promulgate numerose leggi e regolamenti che influenzano lo sviluppo dell'IA e definiscono i requisiti che prodotti e servizi derivati devono soddisfare per essere immessi sul mercato.[60]

Si nota in Cina un interesse particolarmente sentito nell'assicurarsi che si possa risalire ad una catena di responsabilità, peraltro sancendo a più riprese il principio secondo il quale gli esseri umani debbono mantenere il controllo sui sistemi di IA ed essere infine responsabili delle conseguenze del loro utilizzo[61].

Già in altri documenti si rendeva conto di come la Cina abbia anche particolarmente sentito il tema dell'I.A. generativa, prima forse ancora di quanto sia accaduto in occidente: ha inteso regolare le applicazioni IA utilizzate per generare testo, video e audio, dopo un diffuso utilizzo illecito per la creazione di notizie false online. E' già da tempo che il contenuto generato artificialmente in Cina deve essere obbligatoriamente indicato come tale, apponendo una "indicazione apposita" in un "luogo ragionevolmente posizionato" all'interno del contenuto generato[62].

---

[57] M. Fazlioglu, *US federal AI governance: Laws, policies and strategies,* Iapp.org, Novembre 2023, https://iapp.org/resources/article/us-federal-ai-governance/

[58] Energy.gov, *Innovation, Safety and Security: DOE Leads on AI,* 31 ottobre 2023, https://www.energy.gov/articles/innovation-safety-and-security-doe-leads-ai

[59] U.S. Department of Homeland Security, *Artificial Intelligence Roadmap 2024,* https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf

[60] *China's New Generation Artificial Intelligence Development Plan (2017),* https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/, traduzione del documento a cura dell'Università di Stanford.

[61] *Ethical Norms for New Generation AI*, https://cset.georgetown.edu/publication/ethical-norms-for-new-generation-artificial-intelligence-released/ traduzione a cura del CSET – Center for Security and Emerging Technology

[62] *Provisions on the Administration of Deep Synthesis Internet Information Services*, *https://www.chinalawtranslate.com/en/deep-synthesis/*

Ma l'innovazione normativa forse più peculiare ed interessante è rappresentata dall'istituzione del "registro degli algoritmi"[63], Il registro è un database online di algoritmi che hanno "proprietà di opinione pubblica o capacità di mobilitazione sociale". Gli sviluppatori di questi algoritmi sono tenuti a dichiarare come i loro algoritmi sono stati addestrati e distribuiti, **compresi i set di dati su cui l'algoritmo è stato addestrato**. Devono inoltre compilare un rapporto di autovalutazione sulla sicurezza dei loro algoritmi. Una volta che un algoritmo è stato registrato con successo, una versione limitata del file viene resa pubblica[64]. Normative successive hanno esteso l'obbligo di registrare gli algoritmi anche ad altri sviluppatori, in settori diversi.

Fonte normativa di importanza primaria per il settore dell'I.A. in Cina sono le "Disposizioni sulla gestione dei servizi di raccomandazione algoritmica"[65], che stabiliscono un quadro normativo dettagliato per l'uso delle tecnologie di raccomandazione algoritmica nei servizi di informazione su Internet. Queste disposizioni mirano a promuovere i Valori Fondamentali del Socialismo, proteggere la sicurezza nazionale e l'interesse pubblico, oltre a salvaguardare i diritti legali di cittadini e organizzazioni.

Si riscontra qui un meccanismo di controllo continuo, demandato ai fornitori dei sistemi di IA, per evitare modelli che violino leggi o etica, come l'induzione alla dipendenza o a spese eccessive. Inoltre, devono gestire efficacemente la sicurezza delle informazioni, prevenire la diffusione di contenuti illegali o negativi e assicurarsi che le informazioni generate dagli algoritmi siano chiaramente etichettate.

Viene istituita una sorta di graduatoria basata sulle caratteristiche dei servizi di IA, come le già citate in precedenza "influenza sull'opinione pubblica" e "capacità di mobilitazione sociale", e sono istituiti appositi registri nei quali tali servizi sono registrati. I fornitori di tali servizi, lì iscritti, saranno poi periodicamente ispezionati.

Il 9 settembre 2024, la Cina ha rilasciato il suo primo *AI safety governance framework*[66]. Il *framework* è progettato attorno a un approccio centrato sul dichiarato principio di sviluppare l'IA per il bene comune. Anche in questo testo ritornano le usuali preoccupazioni di sicurezza, trasparenza, responsabilità e *bias*.

Il Quadro classifica i rischi di sicurezza dell'IA in due categorie principali: quelli inerenti alla tecnologia stessa e quelli derivanti dalla sua applicazione. Propone misure tecnologiche per mitigare questi rischi, come il miglioramento delle pratiche di sviluppo, la qualità dei dati e valutazioni rigorose per garantire affidabilità e sicurezza nei sistemi IA.

---

[63] M. Sheehan, *China's AI Regulations and How They Get Made*, Carnegie Endowment for International Peace, 10 luglio 2023, https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en

[64] M. Sheehan, S. Du, *What China's Algorithm Registry Reveals about AI Governance,* Carnegie Endowment for International Peace*,* 9 dicembre 2022, https://carnegieendowment.org/posts/2022/12/what-chinas-algorithm-registry-reveals-about-ai-governance?lang=en

[65] *Provisions on the Management of Algorithmic Recommendations in Internet Information Services*, tradotto da China Law Translate, 4 gennaio 2022, https://www.chinalawtranslate.com/en/algorithms/

[66] D. Tobey, A. Carr, C. Bigg, S. Fulton, A. Ge, K. Hoffner, *China releases AI safety governance framework,* DLA Piper, 12 settembre 2024, https://www.dlapiper.com/en/insights/publications/2024/09/china-releases-ai-safety-governance-framework

La parte probabilmente più concreta ed interessante del *framework* è rappresentata da una lunga lista di rischi potenziali dei sistemi di IA, che offre per essi una panoramica completa e soprattutto concreta, ed è riportata in questa tabella:

Categoria Principale	Sottocategoria	Rischi Specifici
Rischi intrinseci per la sicurezza	**Rischi da modelli e algoritmi**	- Rischi di mancata spiegabilità - Rischi di pregiudizi e discriminazione - Rischi di robustezza - Rischi di furto e manomissione - Rischi di output inaffidabili - Rischi di attacchi malevoli
	Rischi dai dati	- Rischi di raccolta e uso illegale dei dati - Rischi di contenuti impropri e avvelenamento nei dati di addestramento - Rischi di annotazione non regolamentata dei dati di addestramento - Rischi di perdita di dati
	Rischi dai sistemi di IA	- Rischi di sfruttamento attraverso difetti e backdoor - Rischi per la sicurezza dell'infrastruttura informatica - Rischi per la sicurezza della catena di approvvigionamento
Rischi per la sicurezza nelle applicazioni di IA	**Rischi nel cyberspazio**	- Rischi per la sicurezza delle informazioni e dei contenuti - Rischi di confusione dei fatti, inganno degli utenti e bypass dell'autenticazione - Rischi di perdita di informazioni dovuti a uso improprio - Rischi di abuso per attacchi informatici - Rischi di trasmissione di falle di sicurezza causate dal riutilizzo di modelli
	Rischi nel mondo reale	- Induzione di rischi tradizionali per la sicurezza economica e sociale

		- Rischi dell'uso dell'IA in attività illegali e criminali - Rischi di uso improprio di tecnologie e oggetti a duplice uso
	Rischi cognitivi	- Rischi di amplificazione degli effetti delle "bolle informative" - Rischi di utilizzo per avviare guerre cognitive
	Rischi etici	- Rischi di discriminazione e di pregiudizi sociali, e di ampliamento del divario di intelligenza - Rischi di sfida all'ordine sociale tradizionale - Rischi che l'IA diventi incontrollabile in futuro

3.3 Open source e auditing: scenari futuri

L'auditing dei sistemi di Intelligenza Artificiale ed il tema dell'open source sono due facce di una stessa medaglia. Da un certo punto di vista, l'open source sembra essere l'unico possibile sistema con cui gli utilizzatori finali dei servizi di IA sono in grado di procedere ad un auditing preciso e ben fatto, in grado di dare risposta ai quesiti imposti dal legislatore e fatti applicare dalle autorità nazionali, secondo sistemi che, come si è visto, non risultano ancora sufficientemente precisi né chiari. Ma al di là delle obbligazioni provenienti da norme vere e proprie, l'auditing introduce un livello di responsabilità e controllo che sembra essere particolarmente necessario per affrontare i rischi e le complessità legati all'IA anche al di là di un obbligo di legge. Questi due ambiti, pur operando con principi differenti, possono convergere per favorire da una parte uno sviluppo più etico, responsabile e comprensibile dei sistemi di IA, ma dall'altro può anche venire in favore degli utilizzatori finali, specie di natura professionale, che poi saranno portati ad assicurare la loro conformità legislativa.

Immaginando dunque una strada riassuntiva per il futuro, è del tutto plausibile che agenzie come il **National Institute of Standards and Technology (NIST)** negli Stati Uniti od il **Centro Europeo per la Trasparenza Algoritmica (ECAT)** nell'Unione Europea acquisiranno sempre maggiore importanza in futuro, contribuendo a stabilire linee guida e soprattutto standard internazionali per l'auditing dei sistemi IA. Si è visto come l'AI Risk Management Framework del NIST, ad esempio, includa funzioni specifiche come la governance, la mappatura dei rischi, la misurazione e la gestione per affrontare ogni aspetto critico della gestione del rischio IA. Immaginare un connubio di questi ragionamenti con una maggiore consapevolezza (ed eventualmente una vera e propria definizione) dell' "openness" dei sistemi di IA sembra essere una possibilità favorevole di futuro legislativo.

Il recente sviluppo del **VET AI Act** negli Stati Uniti comprova peraltro la necessità, sentita anche oltreoceano, di ottenere regole quanto più possibili formali per l'auditing per i sistemi IA, e specie di quelli ad alto rischio. Con il supporto di queste normative e della crescente pressione sociale per una regolamentazione etica, si prevede che gli Stati Uniti potrebbero evolvere verso un sistema di certificazioni obbligatorie per i sistemi IA ad alto rischio, sia per garantire la sicurezza degli utenti sia per facilitare la conformità delle aziende con standard nazionali e internazionali. I programmi di

auditing saranno probabilmente integrati con pratiche di valutazione continua del rischio, promuovendo verifiche periodiche sui modelli IA e una maggiore collaborazione con enti indipendenti, anche in assenza di una normazione univoca a livello federale. Si tratta di una somiglianza di approccio a quella già tenuta dall'AI Act, che, attraverso la sua categorizzazione basata sul rischio, punta a stabilire una gerarchia di controlli e verifiche demandata anche ad enti indipendenti. Per i sistemi ad alto rischio, l'UE richiede infatti audit obbligatori eseguiti da terze parti. L'obiettivo a lungo termine è dichiaratamente quello di creare un sistema in cui i modelli IA possano essere certificati per il loro uso in tutta l'Unione Europea, con una standardizzazione che possa fungere poi da riferimento a livello globale, in modo non dissimile a quanto già tentato con il GDPR.

Questa della predisposizione di standard a livello internazionale emerge come una questione centrale per il futuro, specialmente se si considera come la maggior parte dei soggetti attivi nello sviluppo dei sistemi di IA siano fondamentalmente statunitensi. Il rischio in questo senso è lo stesso già esposto in altre analisi a proposito del GDPR: che taluni soggetti, perlopiù per valutazioni economiche, decidano che sia meglio non fornire i propri servizi sul mercato europeo anziché adeguarsi alle sue stringenti normative e a standard differenti rispetto a quelli in vigore nel paese in cui concretamente avviene lo sviluppo del software. In questo contesto, iniziative come *il Trade and Technology Council*[67] tra Stati Uniti e UE[68] stanno esplorando opportunità di cooperazione per stabilire un terreno comune sulla regolamentazione tecnologica. E' anche qui del tutto possibile che tali inziative siano poi foriere di predisposizioni, non per forza obbligatorie e di fonte normativa, maggiormente precise e condivise in tema di auditing per l'IA. Questa sinergia tra paesi potrebbe poi favorire la nascita di framework di auditing IA che siano riconosciuti e accettati a livello globale, semplificando la conformità per le aziende internazionali e riducendo le barriere di ingresso nei mercati regolamentati.

Infine, stando alla disciplina costituita dall'AI Act, futuri atti dovranno affrontare più specificamente ed in maniera più rigorosa il problema dell'"openness".

Con ciò si intende il fatto che, **l'AI Act, secondo il suo stesso articolo 2, "non si applica ai sistemi di IA rilasciati con licenza libera e open source**, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o come sistema di IA rientrante nell'ambito di applicazione dell'articolo 5 o 50", cioè quelli o del tutto vietati (per esempio perché attuano profiling o identificazione biometrica) o che sono tenuti a obblighi maggiori di trasparenza, perchè interagiscono costantemente col pubblico e/o creano contenuto che deve essere segnalato come artificiale (per esempio le IA generative di testo o immagini).

Segue dunque che nasca un forte interesse da parte delle imprese affinché i loro sistemi di IA non vietati nè generativi siano definiti come open source, così da non essere sottoposti alla disciplina dell'AI Act. Da ciò nascono possibili rischi di elusione definitoria già citati in precedenza, primo fra tutti il tentativo di influenzare la definizione di "open source" da parte delle grandi realtà private, che potrebbero cercare di indebolire o confondere gli standard per aggirare le restrizioni

[67] Si veda https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

[68] Commissione Europea, *EU and US continue strong trade and technology cooperation at a time of global challenges*, comunicato stampa del 5 aprile 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1827

normative. Si noti che questo, secondo alcuni, è già avvenuto: si tratta della recente polemica che ha investito il mondo open source e di cui si è dato conto precedentemente nel documento. La nuova *Open Source AI Definition* si pone infatti in questo solco, semplificando le richieste di trasparenza specie per i dataset senza che venga intaccata la definizione di open source.

I modelli rilasciati con licenze open source, peraltro, non dovranno fornire dettagli approfonditi sui dati utilizzati per l'addestramento e sulle metodologie di training, trasferendo questa responsabilità al futuro EU AI Office[69]. Questa esenzione pone un problema significativo: senza una definizione chiara e precisa di open source, i rischi di manipolazione aumentano, rendendo urgente una maggiore trasparenza e coerenza normativa. Per ciò che concerne l'EU AI Office nello specifico, è anch'esso da considerarsi come un potenziale ente di estrema rilevanza per il futuro per ciò che riguarda il tema del *risk management* e della standardizzazione normativa; tuttavia, si rileva come non abbia ancora reso pubblica alcuna sua attività sul tema dell'open source[70].

Si segnala infine il *Model Openness Framework* (MOF)[71], un sistema di classificazione sviluppato dalla comunità dell'iniziativa *Generative AI Commons*[72], per valutare e classificare la completezza e l'apertura dei modelli di machine learning[73]. Questo framework mira ad esaminare quali componenti del ciclo di sviluppo del modello sono rese pubbliche e sotto quali licenze, cercando di offrire una valutazione il più possibile oggettiva. Il MOF si basa su principi di scienza aperta, open source, open data e accesso aperto, richiedendo che specifici componenti del ciclo di sviluppo del modello siano inclusi e rilasciati sotto licenze appropriate. L'obiettivo è prevenire la falsa rappresentazione di modelli che si dichiarano aperti (l'*open washing* di cui si è parlato più volte), guidare ricercatori e sviluppatori nel fornire tutti i componenti del modello sotto licenze permissive e aiutare individui e organizzazioni a identificare modelli che possono essere adottati senza restrizioni. Nell'ottica dei suoi autori, l'adozione diffusa del MOF favorirà un ecosistema IA più aperto, beneficiando la ricerca, l'innovazione e l'adozione di modelli all'avanguardia.

Per facilitare l'implementazione del MOF, è stato sviluppato il Model Openness Tool (MOT), uno strumento progettato per facilitare la valutazione e la classificazione dei modelli di machine learning in base al MOF[74]. Questo strumento fornisce una piattaforma per valutare i modelli di IA ivi presenti rispetto ai 16 componenti del MOF, garantendo trasparenza, riproducibilità e usabilità.

In conclusione, nonostante non si riesca ad individuare con certezza una via primaria da percorrere, è ragionevole presumere come dovranno nascere nuovi standard non per forza legati

---

[69] Liesenfeld, A., & Dingemanse, M. (2024*). Rethinking open source generative AI: open washing and the EU AI Act*. 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 1774–1787). FAccT '24: The 2024 ACM Conference on Fairness, Accountability, and Transparency.
Si veda anche, in proposito dell'European AI Office nello specifico, https://digital-strategy.ec.europa.eu/en/policies/ai-office

[70] Il primo ed unico sinora documento rilasciato al pubblico è un *Risk management logic of the AI Act and related standards* del 30 maggio 2024, https://ec.europa.eu/newsroom/dae/redirection/document/105898, che si occupa di analisi del rischio ed offre un panorama generale della (ancora embrionale) standardizzazine che dovrebbe seguire all'entrata in vigore dell'AI Act. Non c'è, però, nessuna informazione specifica sul tema dell'open source.

[71] M. White & al, *The Model Openness Framework: Promoting Completeness and openness for reproducibility, Transparency, and usability in artificial intelligence, https://arxiv.org/abs/2403.13784*

[72] *Building a Responsible and OpenCommunity for Generative AI*, https://genaicommons.org/

[73] *Model Openness Framework (MOF),* https://isitopen.ai/?utm_source=chatgpt.com

[74] Disponibile al link https://mot.isitopen.ai/

ad una definizione di “open source” data da terze parti, come l’Open Source Initiative, o che, per lo meno, questa possibile definizione venga poi trasferita ufficialmente in una fonte legislativa. Al contempo, utilizzare lo strumento normativo per definire in modo troppo robusto e preciso un concetto cangiante potrebbe non rivelarsi la strada migliore da percorrere per l’innovazione e l’appetibilità del mercato europeo per simili progetti.

4. Proposte legislative europee sull'Open Source e l'Intelligenza Artificiale

4.1. Panoramica del quadro normativo europeo

Nel corso della trattazione si è più volte avuto modo di trattare il quadro normativo europeo in tema di Intelligenza Artificiale in diversi punti, laddove emergeva la sua rilevanza. Scopo di questo capitolo è di riassumerlo nel modo più chiaro possibile, in una trattazione uniforme, e di mostrarne gli ineludibili collegamenti con il concetto di open source, più volte preso in considerazione da fonti normative ma non formalizzato realmente in alcuna norma.

Innanzi tutto, è opportuno spendere qualche parola sul **Digital Services Act (DSA)** e sul **Digital Markets Act (DMA)**: questi, com'è noto, sono regolamenti di notevole importanza dell'Unione Europea che stabiliscono regole specifiche per migliorare la trasparenza e la responsabilità delle piattaforme digitali, incluse quelle che utilizzano sistemi di IA. Pur non concentrandosi direttamente sull'IA, il quadro di norme che delineano indirettamente può impattarne l'uso, specialmente per quanto riguarda le *Very Large Online Platforms* **(VLOPs)**[75], ovvero le piattaforme digitali, e i motori di ricerca, con un impatto significativo sulla società e sul mercato.

Iniziando dal Digital Services Act, esso stabilisce una serie di obblighi per le piattaforme digitali, ed emergono in particolare quelli legati alla **trasparenza algoritmica** e alla **gestione dei contenuti**[76].
Le piattaforme sono obbligate a fornire informazioni chiare e trasparenti sui meccanismi algoritmici utilizzati per classificare, raccomandare o moderare i contenuti. Da ciò deriva un possibile collegamento con i sistemi di IA nel momento in cui tali meccanismi algoritmici sono effettivamente potenziati o affiancati da essi. Lo stesso vale per la valutazione dei rischi, demandata anch'essa alle VLOPs con cadenza annuale, ed includendo perciò anche i potenziali impatti dei sistemi IA su disinformazione, manipolazione politica, hate speech e altri contenuti dannosi.

Il Digital Markets Act si concentra invece principalmente sulla regolamentazione delle pratiche monopolistiche e anticoncorrenziali, mirando a garantire equità tra i partecipanti del mercato digitale, indipendentemente dalla loro dimensione e forza. Il DMA tocca diversi aspetti che impattano l'uso e lo sviluppo dell'IA, imponendo ai cosiddetti "gatekeepers", cioè le piattaforme di grandi dimensioni, l'obbligo di consentire l'interoperabilità delle loro piattaforme con servizi di terze parti. Solitamente a livello tecnico questo avviene attraverso la predisposizione, da parte dei gatekeepers, delle cosidette API: interfacce software che permettono a diverse applicazioni di comunicare tra loro, facilitando lo scambio di dati e l'accesso a funzionalità specifiche della piattaforma[77].
Secondo gli obblighi imposti dal DMA, i terzi che utilizzano servizi della piattaforma gatekeeper

[75] Si tratta di quelle piattaforme con oltre 45 milioni di utenti nell'UE: https://digital-strategy.ec.europa.eu/it/policies/dsa-vlops
[76] Commissione Europea, *Un'Europa pronta per l'era digitale: nuove norme online per le piattaforme*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-platforms_it
[77] Si veda per esempio questa pagina dedicata al tema di Google: *Consentire ad applicazioni di terze parti di accedere ai dati della directory* https://support.google.com/a/answer/6343701?hl=it

possono richiederle l'accesso ai dati dei loro utenti, di quelli cioè che hanno utilizzato tali servizi[78]. Questo requisito può, puramente in astratto, favorire lo sviluppo di soluzioni IA open source, poiché garantisce che i dati possano essere condivisi maggiormente e con più soggetti.

Vietando poi ai gatekeeper di utilizzare i loro algoritmi per favorire i propri servizi rispetto a quelli di concorrenti, i sistemi IA che classificano o raccomandano contenuti o prodotti concorrenziali rispetto ai gatekeeper possono procedere alla loro commercializzazione in un campo da gioco più equo: le piattaforme devono infatti garantire che i loro non siano costruiti per privilegiare i servizi della stessa impresa.

Tuttavia, nella pratica, molte grandi piattaforme forniscono accesso alle loro API per permettere a sviluppatori e servizi di terze parti di interagire con i loro sistemi. Potrebbe quindi accadere che tale accesso sia **parziale**, limitato solo a determinate funzioni o a dati non particolarmente utili, impedendo una reale interoperabilità e limitando le capacità delle aziende concorrenti di sviluppare applicazioni o servizi pienamente competitivi. Per esempio, un motore di ricerca potrebbe offrire ad aziende terze l'accesso ai dati relativi al posizionamento dei risultati, ma senza rivelare i criteri completi utilizzati per determinare il ranking. Questo renderebbe di fatto impossibile per le aziende competere o ottimizzare la propria visibilità (posto che il raggiungimento di questo obiettivo avrebbe già elementi di criticità notevoli), poiché le informazioni chiave sull'algoritmo sottostante resterebbero riservate. Nonostante gli sforzi di equlibrare il mercato presenti nel DMA, questa tipologia di accesso alle API e ai dati non è spesso realmente completo, e può, nel concreto, tradursi in un'**interoperabilità limitata**, che di fatto non consente una concorrenza equa o un'innovazione completa da parte delle terze parti.

Sicuramente l'atto normativo più significativo in tema di regolamentazione dell'IA è l'**Artificial Intelligence Act, o AI Act**, di cui si è già dato ampio spazio nel documento.

Secondo l'articolo 2, paragrafo 3 del Regolamento, esso "*non si applica ai sistemi di IA forniti sotto forma di componenti di software open source resi disponibili gratuitamente tramite licenze open source*".

Questa esclusione **non** si applica se i sistemi di IA open source sono **classificati come ad alto rischio**, o rientrano nell'ambito di applicazione degli **Articoli 5 o 52**, cioè sono vietati o costituiscono IA generative.

Tali eccezioni, pur rilevanti, non costituiscono la maggioranza dei sistemi di IA generalmente diffusi e fruiti da utenti finali per ragioni professionali (quindi soggetti all'AI Act). Di conseguenza, le imprese potrebbero essere incentivate a classificare i loro sistemi di IA come open source per evitare di essere soggette ai requisiti stringenti dell'AI Act.
Si è a tal proposito avuto modo di inquisire in altre parti del documento come da ciò derivino possibili tentativi di influenzare o alterare la definizione di "open source". L'elusione della regolamentazione tramite un uso sbarazzino del termine "open source" può peraltro dare anche un indebito vantaggio competitivo sul mercato.

[78] Usercentrics.com, *In che modo il Digital Markets Act (DMA) europeo influisce sulla privacy degli utenti e sulla gestione del consenso,* https://usercentrics.com/it/knowledge-hub/digital-markets-act-dma-impatto-privacy-utenti-e-gestione-consenso/#:~:text=Portabilit%C3%A0%20e%20accesso%20ai%20dati&text=In%20questo%20modo%20gli%20utenti,sulla%20loro%20piattaforma%2C%20su%20richiesta.

Possibili soluzioni a questo complicato problema saranno postulate nel prossimo capitolo.

Si è poi citato l'*European Center for Algorithmic Transparency* **(ECAT)**, istituito nell'ambito del DSA, gioca un ruolo chiave nel controllo dei sistemi algoritmici, in particolare per quanto riguarda le piattaforme online di grandi dimensioni. In potenza, attraverso la collaborazione con enti di ricerca e regolatori nazionali, l'ECAT dovrebbe portare alla predisposizione di norme migliori, più chiare e concrete, e promuovendo pratiche di auditing standardizzate per tutti i sistemi IA, indipendentemente dalla loro natura open o closed source, diffusi nel mercato europeo.

4.2. Possibili cambiamenti normativi per favorire trasparenza e innovazione

Come si è visto, nonostante i passi in avanti normativi e dottrinali che stanno progressivamente venendo realizzati nell'Unione Europea, permangono alcune **criticità**, che si possono riassumere in due punti principali, entrambi collegati tra loro:

- L'assenza di regole realmente precise sulla definizione di open source, e sui requisiti perché ci si possa fregiare del termine.
- Lo stile a volte eccessivamente generico delle norme, che può far emergere dubbi applicativi e di controllo sia da parte degli utilizzatori finali che dalle autorità di controllo.

Una prima soluzione potrebbe essere quella di legare la definizione di open source delle istituzioni europea quelle maggiormente accettate dalle organizzazioni e comunità online più attive sul tema, e maggiormente diffuse nella prassi. Nonostante la più famosa e potenzialmente rilevante definizione di "open source" provenga dalla Open Source Initiative, ve ne sono comunque altre: enti come la Free Software Foundation, o l'Apache Software Foundation, hanno le proprie linee guida e i propri criteri per determinare cosa costituisce software open source[79]. Anche l'Unione Europea ha provato ad elaborare una sua propria licenza "free & open source", chiamata l'European Union Public Licence (EUPL)[80], che tuttavia non ha preso nel concreto particolarmente piede e non è aggiornata rispetto agli ultimi importanti cambiamenti del mercato, essendo stata costituita nel 2007 ed aggiornata, nella sua versione più recente, a maggio 2017. L' AI Act in questo senso, o un altra fonte legislativa ad esso collegata, potrebbe avrebbe quindi un rimando extra-normativo che darebbe in astratto maggiore certezza e precisione, e, nella migliore delle ipotesi, impedirebbe alle imprese di dichiarare erroneamente come open source sistemi che non soddisfano i requisiti di trasparenza e accessibilità.

Ma questa soluzione, evidentemente, offre il fianco a numerose critiche e problematicità già emerse in corso di trattazione. Ancorare elementi normativi ad una definizione esterna rischia di creare problematiche di interpretabilità, e soprattutto di dipendenza nei confronti di enti che nulla hanno a che fare con le istituzioni europee propriamente dette e legislativamente accettate, compromettendo l'autonomia normativa dell'UE e delegando a privati di dubbia fiducia un potere definitorio di rilevanza pubblica.

[79] Wikipedia offre una tabella che misura le compatibilità tra organizzazioni open source e licenze alla pagina https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses , sezione "Approvals".
[80]Commissione Europea, *The EUPL, Guidelines, FAQ, Infographics,* https://interoperable-europe.ec.europa.eu/collection/eupl/eupl-guidelines-faq-infographics

Si è visto come affidarsi a una definizione come quella dell'OSI (o ad un'altra) potrebbe rendere l'Unione Europea vulnerabile a cambiamenti normativi decisi da terze parti, che potrebbero non riflettere sempre gli interessi o i valori europei ed essere determinati da interessi privati: gli stessi interessi che tramite la normativizzazione della definizione si vorrebbero eliminare. In parole più semplici, l'OSI, per esempio, potrebbe aggiornare la propria definizione per ragioni di mercato o per decisioni interne, generando confusione e incertezza normativa: malgrado non sia chiaro se e in quale modo vi siano state influenze, è la situazione che si sta verificando proprio in questo periodo, con la formalizzazione della nuova Open Source Definition, dalla quale è nata una notevole discussione e perfino uno scisma.

Considerando quanto appena detto, si potrebbe porre una soluzione in qualche misura più oppressiva e burocratica, per cui si dovrebbe richiedere *anche* al software open source, ed ancor più ai sistemi di AI definibili come open source, una serie di requisiti minimi, come ad esempio standard di trasparenza, comprensibilità e documentazione. Questo è maggiormente importante laddove tali sistemi sono diffusi in istituzioni pubbliche, come del resto l'UE si auspica da molto tempo.

Già negli anni passati, infatti, la **Open Source Software Strategy**[81] dell'Unione Europea si è posta come propositi quelli di promuovere e migliorare l'uso del software open source nelle istituzioni e nelle politiche dell'Unione. Vi sono state due grandi "tornate" di questa strategia: una impiegata tra gli anni 2014-2017, l'altra dal 2020 al 2023[82]. Al momento della scrittura del documento non si rileva un'attività simile portata avanti per il 2024 e gli anni seguenti: la Commissione Europea ha infatti inteso tagliare notevolmente i fondi per le iniziative sul software libero e open source nell'ambito dei programmi Horizon nei prossimi anni[83]. Iniziative quali la *Next Generation Internet*[84] sono state peraltro soppresse del tutto nel nuovo budget dell'Unione Europea, che si concentrerà invece massimamente sul concetto di intelligenza artificiale in senso lato[85].

La Open Source Software Strategy ha comunque portato alcune interessanti novità: intanto, ha portato la Commissione Europea a distribuire il suo software in open source[86] tramite una piattaforma dedicata non dissimile come stile a Github: code.europa.eu[87]. La stessa Commissione è attiva su Github dietro lo user ec-europa. Poi, ha portato alla nascita di strutture quali *Open Source Programme Office(OSPO)* della Commissione Europea[88], che dovrebbe agire di concerto con gli altri Uffici dedicati all'Open Source dei vari Stati Membri, tramite il **network degli Open Source**

---

[81] Commissione Europea, *Open Source Software Strategy,* https://commission.europa.eu/document/download/97e59978-42c0-4b4a-9406-8f1a86837530_en?filename=en_ec_open_source_strategy_2020-2023.pdf, 21 ottobre 2020

[82] Come si vede dal sito ufficiale della Commissione dedicato alla strategia: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/digital-services/open-source-software-strategy_en

[83] B. Vigliarolo, *FOSS funding vanishes from EU's 2025 Horizon program plans,* theregister.com, 17 luglio 2024, https://www.theregister.com/2024/07/17/foss_funding_vanishes_from_eus/

[84] La NGI è un'iniziativa in seno alla Commissione Europea che mira (o forse mirava) a guidare la regolamentazione di internet per assicurarne una maggiore fiducia presso i cittadini europei. https://ngi.eu/about/

[85] Free Software Foundation Europe, *EC cuts funding support for Free Software projects,* 19 luglio 2024, https://fsfe.org/news/2024/news-20240719-01.en.html

[86] EU Commission makes software publicly available through open source, https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/eu-commission-makes-software-available-through-open-source-2021-12-09_en

[87] P.E. Schmitz, The new platform launched by Director General for Informatics, 3 ottobre 2022, https://interoperable-europe.ec.europa.eu/collection/eupl/news/codeeuropaeu

[88] Si veda https://interoperable-europe.ec.europa.eu/collection/ec-ospo

Programme Offices[89]**.** Questo *network* promuove la collaborazione tra le organizzazioni del settore pubblico sull'adozione e la gestione del software open source. L'iniziativa, avviata a maggio 2022, riunisce 13 organizzazioni provenienti da 8 Stati membri, tra cui amministrazioni cittadine, ministeri, dipartimenti governativi e istituti di ricerca. Attraverso incontri regolari, facilitati dall'OSPO della Commissione Europea, il network favorisce lo scambio di conoscenze e migliori pratiche per implementare e sviluppare soluzioni open source nei servizi pubblici.

Il tema è strettamente legato a quello della sovranità digitale e tecnologica spesso al centro dei dibattiti pubblici sulle tecnologie all'avanguardia, e alla percepita mancanza delle stesse, in Europa[90]. Creare un ecosistema digitale indipendente, a prescindere dal livello raggiunto, rappresenta di sicuro una strada importante per il consolidamento di settori strategici che difficilmente sarebbe auspicabile vedere delegati ad altri, in dipendenza di tecnologie proprietarie di paesi di terze parti.

Questi cambiamenti concreti nell'approccio delle istituzioni europee, con l'intenzione di coinvolgere i regolatori nazionali, sembra aver portato a buoni risultati, nonostante l'Open Source Software Strategy non sia stata ufficialmente rinnovata per gli anni 2024 e seguenti[91], e nonostante certi proclami del passato, che si possono leggere nei vecchi documenti della stessa OSSS, non abbiano portato a granché[92]. Peraltro, l'Unione Europea sta promuovendo i principi FAIR[93] nell'ambito dell'Open Science per migliorare la gestione e la condivisione dei dati e del codice scientifico, attraverso programmi come Horizon Europe e iniziative come l'European Open Science Cloud[94]. In breve, l'UE incoraggia i ricercatori a rendere i loro dati e software facilmente rintracciabili, accessibili tramite protocolli aperti, interoperabili attraverso standard comuni e riutilizzabili grazie a licenze aperte.

Nonostante sia lodevole l'impegno della Commissione verso la diffusione del software open source, rimane alla base il grande tema della mancanza di una definizione univoca dello stesso, peggiorata oggi a sua volta dalla multi-sfaccettatura tipica dei sistemi di IA.

Ultimamente, il c.d. "Report Draghi"[95], che si occupa di delineare una strategia competitiva in molteplici settori per il futuro dell'Unione Europea, tralascia in modo piuttosto evidente il tema dell'Open Source e del suo legame con l'IA, fondamentalmente dedicandogli un rigo in tutto il

---

[89] G. Hillenius, *Gradually align on open source practices: Networking OSPOs in the EU,* Commissione Europea, 5 giugno 2024, https://interoperable-europe.ec.europa.eu/collection/ec-ospo/news/gradually-align-open-source-practices

[90] L. Dibiaggio, L. Nesta, S. Vannuccini, *European Sovereignigy in Artificial Intelligence,* LUISS, 17 dicembre 2024, https://leap.luiss.it/wp-content/uploads/2024/12/WP20.24-European-Sovereignty-in-Artificial-Intelligence.pdf

[91] Si rilevano tuttavia alcune iniziative simili o assimilabili, come ad esempio l'*EU Open Source Policy Summit 2025,* evento programmato per il 31 gennaio 2025 a Bruxelles che offrirà una piattaforma di dialogo tra la nuova amministrazione dell'UE e la comunità open source europea. Da https://summit.openforumeurope.org/.

[92] Per esempio, nel documento del 2020-2023 si leggono obiettivi quali "la creazione di una Commissione digitalmente trasformata, *user focused and data driven*: una vera Commissione Digitale", oppure ci si propone di "diventare, come UE, un modello cui ispirarsi per una società potenziata dai dati", e di "ottenere sovranità tecnologica in alcune aree critiche".

[93] Un insieme di linee guida pensate per migliorare la gestione e condivisione dei dati scientifici. L'acronimo sta per Findable, Accessible, Interoperable, Reusable.

[94] Commissione Europea, *European Open Science Cloud (EOSC): What the European Open Science Cloud is,* https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en

[95] The future of European competitiveness, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

documento, e limitandosi ad auspicare che “i modelli siano addestrati con dati liberamente contribuiti da molteplici paesi dell’UE; supportato da un framework open-source”.
Oltre a questo auspicio, il tema non viene preso concretamente in esame, e non si offrono, almeno per ora, soluzioni precise ad argomenti precisi.

Oltre al problema definitorio ormai citato in modo quasi ossessivo, c’è anche un dilemma pratico nella misura in cui la mancanza di norme concrete sulle metodologie di auditing e sui requisiti precisi dei sistemi di IA rende a volte confusa l’applicazione delle norme e i possibili controlli che possono nascere in seno ad autorità pubbliche. Senza linee guida chiare e precise, le autorità potrebbero trovarsi a fronteggiare numerose difficoltà nell'esaminare il funzionamento dei sistemi di intelligenza artificiale. L'assenza di criteri standardizzati per la valutazione di algoritmi, dati di addestramento, processi decisionali e impatti potenziali rende complesso per le autorità identificare possibili rischi e bias che potrebbero influenzare il comportamento dei sistemi di IA. Ciò si traduce in una maggiore incertezza durante le procedure di auditing, che potrebbero risultare inefficaci o incoerenti tra diverse applicazioni o settori.

Si potrebbe sostenere la creazione di **norme aggiuntive** che specificassero ulteriormente, nel concreto, quali requisiti e quali metodologie debbano essere seguite per garantire un’adeguata trasparenza ed il rispetto reale – e non solo formale – dello spirito della legge. Si pensi ad esempio al tema delle API citato in precedenza a proposito del Digital Markets Act: sarebbe opportuno che venga legislativamente imposto per le API di includere tutte le **funzionalità principali** del sistema di IA, in modo che eventuali terze parti abbiano un accesso sostanziale, e non limitato o parziale, favorendo un'effettiva interoperabilità tra le piattaforme.

In un mercato così mutevole e in rapida evoluzione, nel quale perfino la stessa definizione di partenza di open source non è fissa ma cangiante, starebbe alle autorità competenti di vigilare sull'uso della classificazione open source per assicurarsi che non venga utilizzata per eludere gli obblighi normativi. Gli obblighi dichiarativi, insieme alla previsione di sanzioni per imprese che aggirino la legge tramite false dichiarazioni, dovrebbero essere certamente migliorati e resi più concreti, anche a tutela di quanti, come si è già detto, saranno poi inevitabilmente sottoposti a controlli.

Nel momento in cui il software open source, o sistemi di IA open source, fossero usati dalle istituzioni pubbliche, potrebbe essere utile richiedere che le licenze utilizzate rispettino criteri specifici. In questo senso si intende agire non tramite una definizione scolpita nella pietra di open source, ma tramite una serie di licenze “permesse” e dichiarate conformi dall’Unione Europea, lasciando in questo modo maggiore flessibilità nella scelta delle stesse, imbrigliando meno il mercato e riducendo il rischio di rimanere in qualche misura indietro rispetto al progresso tecnologico: una definizione univoca sancita per via legislativa è infatti molto più difficile e lunga da cambiare rispetto a quella di una Open Source Initiative che ragiona su tempi privatistici.

Alcune iniziative sembrano parzialmente andare in questa direzione,
“Public Money, Public Code"[96] è una campagna promossa dalla Free Software Foundation Europe che sostiene l'idea che il software finanziato con fondi pubblici debba essere reso disponibile come software libero e open source. Se i soldi sono pubblici, allora anche l’accesso al codice deve esserlo. La campagna, che ha riscosso il sostegno di numerose organizzazioni e imprese[97], desidera l’adozione di software libero nelle amministrazioni pubbliche, puntando ad un miglioramento di sicurezza e qualità dei servizi offerti, ma soprattutto di trasparenza. In teoria, secondo gli aderenti

[96] Public Code Public Money, *Lettera Aperta*, https://publiccode.eu/it/openletter/
[97] https://publiccode.eu/it/, *Organizzazioni Aderenti*.

all'iniziativa, un approccio "*public money, public code*" riduce il rischio di vulnerabilità nascoste e aumenta la fiducia dei cittadini nei servizi digitali. Inoltre, l'uso di software open source evita il "vendor lock-in", ossia la dipendenza da un unico fornitore, permettendo alle istituzioni di risparmiare sui costi a lungo termine e di avere maggiore controllo sui propri strumenti digitali.

Non c'è, in questo caso, una preferenza verso uno specifico tipo di licenza: l'importante è che "il software finanziato pubblicamente e sviluppato per il settore pubblico sia reso pubblicamente disponibile sotto una licenza Software Libero/Open Source", non essendo specificato esplicitamente quale licenza utilizzare. Come si è visto, però, le licenze specialmente open source possono essere anche molto diverse tra loro, prevedendo clausole di copyleft o limiti alla possibilità di guadagno a partire dal software utilizzato o ridistribuito. Anche in questo caso si dovrebbe comunque porre un problema di definire una o più licenze privilegiate e generalmente preferibili per il software nell'Unione Europea.

Ad aprile di quest'anno, peraltro, è entrato in vigore l'*Interoperable Europe Act*[98], regolamento europeo proposto già nel 2022[99], che mira a creare una rete di amministrazioni pubbliche digitali sovrane e interconnesse, accelerando la trasformazione digitale del settore pubblico europeo. Uno degli elementi centrali per tale progetto è la promozione dell'uso di soluzioni open source nelle pubbliche amministrazioni. Riconoscendo i benefici del software libero in termini di flessibilità, sicurezza e costi ridotti, l'atto incoraggia le istituzioni a condividere e riutilizzare componenti software, evitando duplicazioni e favorendo, almeno sulla carta, l'innovazione. Tale quadro di cooperazione sarà guidato dall'Interoperable Europe Board, composto da rappresentanti degli Stati membri, della Commissione, del Comitato delle Regioni e del Comitato Economico e Sociale Europeo, e sarà finanziato tramite il programma Digital Europe. Il regolamento è obbligatorio a tre mesi dalla sua pubblicazione, e lo è quindi diventato a luglio 2024. Tuttavia, i primi obblighi per le istituzioni e le agenzie europee iniziano a scattare solo da gennaio 2025, quando dovranno svolgere i loro primi, obbligatori, studi di interoperabilità. Allo stesso modo, gli Stati Membri dell'UE saranno tenuti a designare autorità nazionali competenti sul tema entro la stessa data: gennaio 2025. È quindi troppo presto per avere dati più precisi sulle ripercussioni e la generale efficacia dell'*Interoperable Europe Act.*

Come ultimo punto, è opportuno segnalare la presenza di iniziative provenienti da singole municipalità ed enti territoriali, che mirano a migliorare, per quanto sia loro possibile e limitatamente ai loro confini di competenza, la trasparenza, l'affidabilità e con esse la percezione pubblica che i sistemi di IA possono avere, dando regole e sviluppando prassi in parallelo rispetto all'Unione Europea. Il Registro degli Algoritmi di Amsterdam, ad esempio, è una piattaforma che offre una panoramica dei sistemi di intelligenza artificiale e degli algoritmi utilizzati dalla città[100]. Questo registro consente ai cittadini di comprendere quali algoritmi sono impiegati nei servizi municipali, il loro funzionamento e le finalità per cui sono stati sviluppati. Attraverso il registro, è possibile accedere a descrizioni dettagliate dei vari algoritmi, avendo quindi maggiore trasparenza

[98] Commissione Europea, *New Interoperable Europe Act to deliver more efficient public services through improved cooperation between national administrations on data exchanges and IT solutions*, 21 novembre 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6907

[99] Commissione Europea, *Interoperable Europe Act Proposal*, https://commission.europa.eu/publications/interoperable-europe-act-proposal_en#:~:text=The%20Interoperable%20Europe%20Act%20entered%20into%20force%20on,cooperation%20in%20the%20public%20sector%20across%20the%20EU.

[100] *What is the Amsterdam Algorithm Register?* https://algoritmeregister.amsterdam.nl/en/ai-register/

su come essi influenzino la vita quotidiana ed i servizi offerti dalla città. Inoltre, i cittadini hanno l'opportunità di fornire i loro pensieri e feedback su tali sistemi.

Simile ma più interessante per lo specifico argomento dell'auditing dei sistemi di IA vi è poi il registro dell'Intelligenza Artificiale di Helsinki. Come quello di Amsterdam, esso offre un sito internet tramite il quale accedere ad una panoramica piuttosto dettagliata dei sistemi di IA utilizzati dalla città. Sul sito sono infatti presenti diversi servizi con IA disponibili al cittadino, tra i quali si segnalano chatbot per i parcheggi, per informare sulle attività all'aperto, e per aiutare nella ricerca degli immobili[101].

La parte più rilevante sta però nelle informazioni che il registro di Helsinki offre al cittadino su tali sistemi di IA. Per ognuno di essi, è presente una scheda[102] che descrive lo strumento di IA attraverso i seguenti elementi:
- **I dataset utilizzati**, intendendo con ciò il materiale con cui è stato addestrato l'algoritmo e le regole in base alla quale sono conservate le conversazioni avute col chatbot del servizio.
- La logica dietro le operazioni del sistema, cioè il modello sul quale è stato costruito e la sua architettura, allegandone un grafico esplicativo, che mostra anche l'eventuale presenza di servizi di terzi parti (come quelli di cloud) per i quali è necessario passare per il funzionamento del sistema.
- **I principi di non discriminazione** seguiti.
- **La presenza di esseri umani** a sovrintendere il servizio.
- I **sistemi di gestione del rischio** adottati.

Questi temi sono descritti in modo piuttosto generico ma comunque utile per avere risposta a buona parte dei quesiti che un cittadino mediamente informato potrebbe avere, e risulta chiaro nell'esposizione.

La base teorica sulla quale si basa sia il registro di Helsinki, sia quello di Amsterdam, è riassunta da un White Paper redatto nel 2020[103] che discute del concetto di un registro pubblico dell'IA, proponendolo come un elemento chiave per migliorare trasparenza e fiducia percepita. Il documento è peraltro interessante perchè ha un'ottica concreta, e raccomanda che i registri dei sistemi di IA contengano gli elementi già elencati in precedenza a proposito del registro di Helsinki.

I registri pubblici dell'IA sono un esperimento che per il momento sembra positivo, volendo rappresentare una risposta concreta e tangibile al bisogno di trasparenza nell'uso delle tecnologie da parte degli enti amministativi. Piuttosto che essere semplici dichiarazioni di principio, questi registri offrono ai cittadini uno strumento diretto e accessibile per comprendere come gli algoritmi influenzino i servizi pubblici che gli stessi cittadini intendono utilizzare, perché utili alla loro vita quotidiana.

[101] City of Helsinki, *What is AI Register*, https://ai.hel.fi/en/ai-register/
[102] Si prenda ad esempio la scheda dedicata ad un chatbot per trovare lavori estivi: https://ai.hel.fi/en/summer-job-voucher-chatbot/
[103] M. Haataja, L. Van de Fliert, P. Rautio, *Publicc AI Registers*, Saidot, Helsinki, Settembre 2020, https://ai.hel.fi/wp-content/uploads/White-Paper.pdf

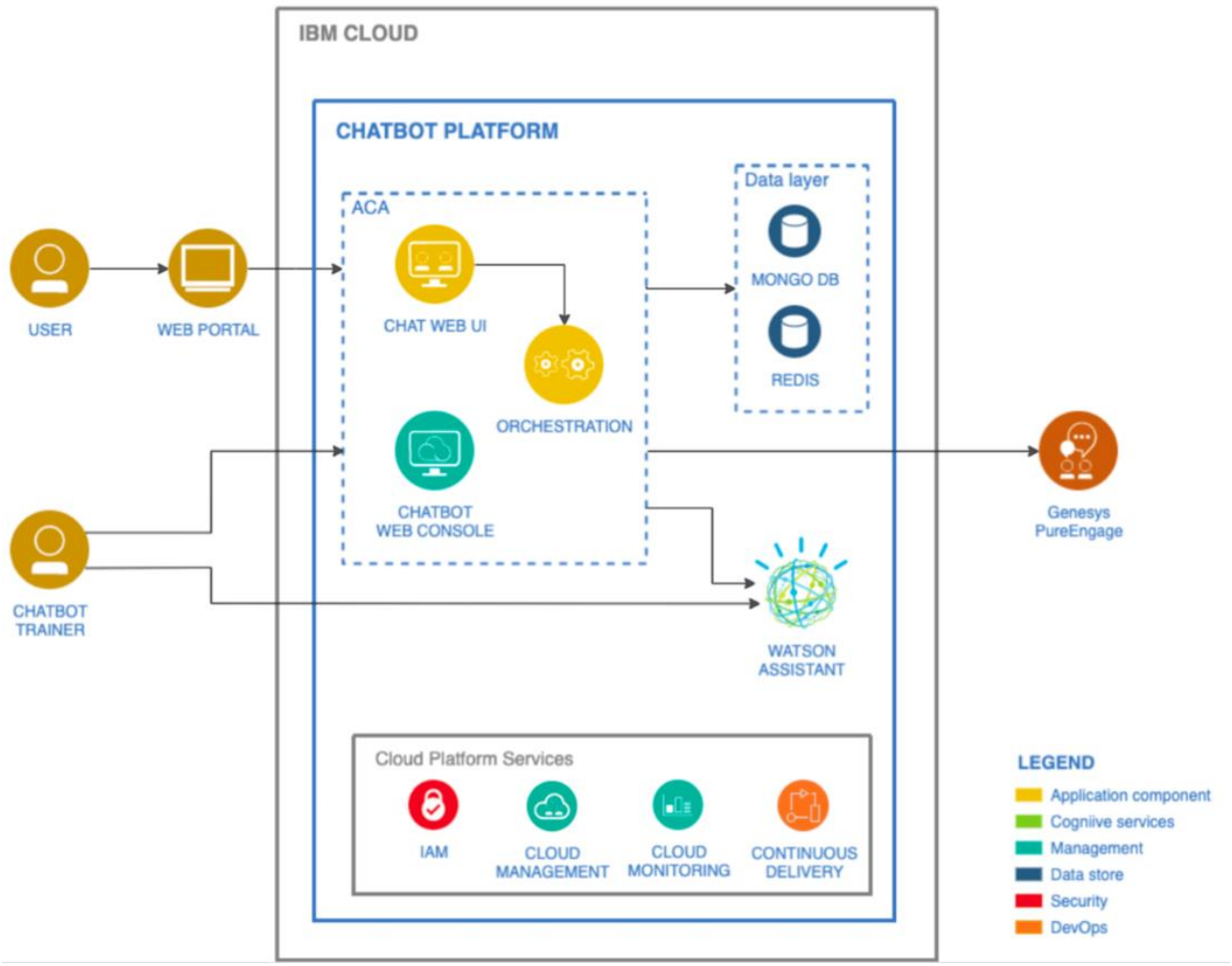


Figura 2 il grafico esplicativo che mostra il funzionamento del sistema di IA alla base del chatbot dedicato alla ricerca di lavori estivi di Helsinki. Si noti il passaggio attraverso la "IBM Cloud", necessario per il funzionamento del modello di IA di IBM utilizzato per realizzare poi il chatbot specificamente legato alla città di Helsinki.

E' di interesse infine notare come l'idea di registrare gli algoritmi in un registro centralizzato e consultabile sia comune alle esperienze descritte per la Cina. In effetti, esistono obiettivi condivisi: l'idea di base è quella di aumentare la trasparenza e garantire un certo livello di controllo sull'impiego degli algoritmi e dei sistemi di IA, specialmente in ambiti che coinvolgono servizi pubblici o che influenzano direttamente la vita dei cittadini.

Le analogie tra le iniziative europee e cinesi risiedono principalmente nell'obiettivo di rendere più comprensibili e responsabili i sistemi di IA, cercando di mitigare i rischi di discriminazione e di abuso tecnologico. Ma mentre i registri europei pongono un forte accento sulla partecipazione democratica e sul coinvolgimento civico, offrendo, per esempio nel caso di Helsinki, contestuali servizi concretamente utili alla vita quotidiana, il registro cinese ha un'impostazione più orientata al controllo statale e alla regolamentazione del settore tecnologico. Il focus principale è assicurare che gli algoritmi operino in conformità alle normative cinesi e ai valori del governo centrale, con un controllo più centralizzato e una supervisione diretta dell'uso dell'IA da parte delle aziende. L'ambito di applicazione dei registri degli algoritmi è anche molto diverso: decisamente più ristretto in Europa, perché legato a singole inizative di singoli enti amministrativi, e molto limitato nella sua estensione, è al contrario ben più pervasivo in Cina, con un ambito applicativo notevolmente più esteso ed in ulteriore espansione.

In definitiva, nonostante l'Unione Europea cerchi di bilanciare la promozione dell'innovazione nell'IA con la necessità di proteggere i diritti fondamentali e la sicurezza dei cittadini, tramite iniziative propriamente legislative, organismi di ricerca e di consultazione, o particolari programmi degli enti amministrativi locali, si rilevano notevoli possibili scappatoie derivanti da una definizione non precisa di "open source" e da norme poco legate ai requisiti concreti del *software* ed ai suoi sistemi di auditing. Come si è già avuto più volte modo di osservare, la mancanza di una standardizzazione precisa nello sviluppo, nelle definizioni e nei metodi di controllo potrebbero compromettere gli obiettivi elencati. A fronte di questo, nel prossimo capitolo verrà esplorata la situazione più specificamente legata alle imprese di telecomunicazione.

5. Implicazioni per il settore delle Telecomunicazioni

5.1. Utilizzo dell'IA nei servizi B2C e B2B delle aziende telecom

L'IA è ormai al centro delle strategie delle aziende di telecomunicazioni per i servizi B2C, offrendo opportunità economiche migliori, nonché strumenti per potenziare l'esperienza del cliente con il servizio di telecomunicazione, ottimizzandone nello specifico l'interazione e la comunicazione. Le tecnologie di IA vengono impiegate per personalizzare le offerte, migliorare i tempi di risposta tramite sistemi automatizzati e garantire una gestione efficiente delle reti.
Il miglioramento qualitativo del servizio può essere significativo, specie se comparato al passato.

Se in passato i chatbot erano spesso criticati per essere incomprensibili o inefficaci, oggi i sistemi di assistenza basati su IA sono in grado di comprendere meglio il linguaggio naturale, rispondere in modo coerente e, in alcuni casi, anticipare le esigenze dei clienti. Questo miglioramento tecnologico ha consentito alle aziende di telecomunicazioni di ridurre i tempi di attesa, migliorare la soddisfazione del cliente e ridurre i costi operativi, senza compromettere la qualità dell'interazione. Strumenti come assistenti vocali e chatbot di nuova generazione rappresentano ora una valida alternativa all'assistenza umana, soprattutto per la risoluzione di problemi standard, con evidenti vantaggi in termini di efficienza e velocità.

Questo documento, però, non esisterebbe se l'utilizzo dell'IA in tale settore non ponesse rilevanti questioni, prettamente di compliance normativa. I dati raccolti e analizzati per alimentare questi sistemi sono spesso di natura sensibile, ed è necessario garantire che vengano trattati in conformità con normative come il GDPR in Europa. Le aziende di telecomunicazioni si trovano a bilanciare l'innovazione tecnologica con la necessità di rispettare rigide normative in materia di privacy e protezione dei dati. Questo compito diventa ancora più complesso quando si tratta di implementare sistemi di IA che possono evolvere autonomamente, aumentando il rischio di violazioni involontarie.

Creare modelli di IA da zero

La creazione di modelli di IA completamente nuovi è un'impresa alla portata solo di pochissime aziende nel mondo, generalmente colossi tecnologici come OpenAI, Google, Meta o Microsoft. Questo processo richiede non solo una quantità impressionante di risorse economiche, ma anche una capacità tecnica fuori dal comune: di questo si è già parlato precedentemente nel documento. Anche la potenza hardware richiesta può risultare nel concreto irraggiungibile. Nonostante sia vero che aziende come Nvidia offrono GPU specializzate per il calcolo parallelo su larga scala, queste

sono spesso riservate a progetti specifici o vengono utilizzate in ambienti condivisi[104], ed anche con queste risorse l'addestramento di un modello può risultare nel concreto irrealistico, o troppo lungo per non essere già obsoleto nel momento in cui è completato.

Volendo incaponirsi e realizzare un modello di IA propriamente da zero, soltanto dal punto di vista hardware sarebbero oggi richieste centinaia di schede video specializzate. Per l'addestramento di un modello di intelligenza artificiale avanzato, seppur ormai non recentissimo, come BERT[105] di Google, che si occupa prettamente di elaborare il linguaggio, Nvidia dichiara di utilizzare 2.048 schede video A100 in parallelo[106]. Considerando un costo di circa 17.000€ a singola GPU, un calcolo approssimativo mostra intorno ai 40 milioni di euro la spesa iniziale necessaria, solo per ciò che concerne le schede video, per allenare rapidamente un sistema di IA partendo da un modello di elaborazione del linguaggio che ha già qualche anno. Anche volendo ottenere prestazioni inferiori, e quindi avere un addestramento meno approfondito o più lento, la spesa è comunque estremamente rilevante: se anche si limitasse il numero di schede video installate su un eventuale sistema dedito all'addestramento IA, vi sarebbe poi comunque da considerare tutto il resto: dal costo energetico a quello del personale, fino a tutti i componenti hardware accessori (come processori, schede madri e alimentatori) necessari per tenere insieme e far funzionare questa straordinaria potenza di calcolo.

Vi è poi la questione dei dati. La costruzione di un modello di IA inizia come si sa con il pre-training, una fase durante la quale l'algoritmo viene addestrato su dataset di dimensioni immense. Questi dataset devono essere sufficientemente variegati da permettere al modello di apprendere pattern, relazioni e regole generali. Modelli come GPT sono stati addestrati su terabyte e terabyte di dati e di contenuti, provenienti da fonti diverse e molto spesso come si è visto dubbie nella loro liceità.

Per un'azienda di telecomunicazioni, l'ambizione di creare un modello da zero richiederebbe l'accesso a dataset altrettanto ampi e specifici per il settore. In questo senso le TLC potrebbero risultare privilegiate nella misura in cui avrebbero la possibilità di includere nel training dati provenienti da **log di rete, interazioni con i clienti, previsioni del traffico e segnalazioni di guasti.** Tuttavia, raccogliere e utilizzare tali dati comporta complessità legate alla privacy, alla sicurezza e alla conformità normativa, in primo luogo data dal mai citato a sufficienza GDPR. I dati dovrebbero essere innanzi tutto minimizzati e pseudonimizzati per garantirne l'irriconducibilità ad un individuo specifico e ottenere un'esenzione dalle obbligazioni più stringenti della normativa. Poi, dovrebbe essere realizzata una valutazione d'impatto, essendo questo un processo che con ogni probabilità, secondo il GDPR, "rappresenta un rischio elevato per i diritti e le libertà delle persone". Infine, oltre alla predisposizione di misure di sicurezza e protezione dei dati all'avanguardia, sarebbe necessario stilare un'informativa ben delineata, creata appositamente per l'occasione o comunque fornita in modo trasparente, per esempio attraverso l'aggiornamento dei termini del servizio, rendendo edotti quindi i clienti sulle finalità del trattamento dei loro dati raccolti.

---

[104] Intendendo con ciò il fatto che è frequente l'utilizzo nel quale la potenza computazionale di più GPU è condivisa in ambienti online, in una sorta di cloud. Si veda https://www.nvidia.com/it-it/data-center/a100/

[105] J. Devlin, M-W. Chang, K. Lee, K. Toutanova, *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, Cornell University, 2018, https://arxiv.org/abs/1810.04805

[106] "Un carico di lavoro di training come BERT può essere risolto in meno di un minuto con l'impiego di 2.048 GPU A100, un record di tempistiche mondiale.", da https://www.nvidia.com/it-it/data-center/a100/

In effetti, le opportunità per le aziende TLC di partecipare a questo processo sono limitate, ma non impossibili. Ammettendo la possibilità di attingere a dataset per lo meno sufficienti per addestrare un modello, e avendo la volontà di spendere ingenti somme di denaro per acquisire hardware, *know-how,* e mantenimento energetico, il risultato non è irraggiungibile, ma solo molto dispendioso. Per far fronte a questo, una strategia possibile potrebbe essere quella di collaborare con università e istituti di ricerca, combinando risorse per addestrare modelli su dataset verticali (cioè più limitati e per compiti maggiormente specifici), propri del settore delle telecomunicazioni (come l'analisi di traffico di rete, lo studio delle preferenze dei clienti o la previsione di guasti). In alternativa, aziende con una forte presenza nei mercati emergenti potrebbero sfruttare la loro capacità di raccogliere dati da questi contesti per creare modelli adattati a esigenze locali.

Partecipazione a modelli di terze parti

Si è visto come lo sviluppo di sistemi di IA complessi e avanzati richieda un'enorme quantità di dati, risorse hardware e competenze altamente specializzate, rendendo nella pratica difficile per la maggior parte delle imprese sviluppare queste soluzioni internamente. È del resto sempre più comune affidarsi ad iniziative di terze parti[107] nella speranza di ottenere i vantaggi dei servizi di IA superando gli ostacoli di ordine pratico che sottostanno alla loro realizzazione ex-novo.

Sembra dunque conveniente utilizzare modelli di intelligenza artificiale pre-addestrati, come quelli forniti dalle gargantuesche imprese del settore, e successivamente personalizzarli in base alle proprie esigenze attraverso il processo di fine-tuning. Può anche darsi il caso di basarsi su modelli IA open-source già esistenti (ad esempio, TensorFlow, PyTorch e altri framework) per costruire applicazioni personalizzate. Molti fornitori offrono servizi IA tramite API che dovrebbero consentire alle aziende di telecomunicazioni una relativamente facile integrazione nei loro processi e sistemi.

Precedentemente si è visto in corso di trattazione, quando ci si riferiva ai servizi di IA offerti contestualmente al registro degli algoritmi di Helsinki, che numerose piattaforme di cloud computing (come AWS, Azure, Google Cloud, o, nel caso di Helsinki, Intel) offrono servizi dedicati all'IA con potenza di calcolo e strumenti per il loro fine-tuning e dispiegamento.

Si tratta qui di ottenere più o meno una soluzione "tutto in uno" nella quale le piattaforme offrono potenti risorse di calcolo, inclusi server e GPU per l'addestramento intensivo di modelli di IA, e offrono ambienti preconfigurati con librerie e strumenti appositi. I modelli possono poi essere integrati con i servizi dell'impresa fruitrice, come database, strumenti di analisi dei dati o sistemi di messaggistica.

Nonostante l'apparente facilità e comodità di una soluzione simile, essa deve ritenersi inottimale per definizione, dovendosi vincolare ad un'altra realtà altrettanto imprenditoriale, potenzialmente concorrente, e ubicata in Stati diversi. I servizi offerti, poi, per quanto sicuramente efficaci, sul lungo periodo non possono che palesare le loro naturali limitazioni dovute alla necessaria genericità del servizio offerto, che nulla ha di realmente personalizzato se ciò che è consentito tramite la fase finale di fine-tuning. Inoltre, la gestione ed il trattamento dei dati personali degli utenti, i cui obblighi comunque vincolano l'impresa fruitrice del servizio, potrebbero essere svolti

[107] Federmanager, Intelligenza Artificiale: potenzialità e sfide per il futuro di imprese e manager, https://pressroom.federmanager.it/intelligenza-artificiale-potenzialita-e-sfide-per-il-futuro-di-imprese-e-manager/?utm_source=chatgpt.com

in modi non del tutto conformi alle norme europee, e comunque esposti ad un soggetto diverso rispetto all'impresa di TLC utilizzatrice finale.

Vi è poi il tema della **proprietà intellettuale** sui modelli derivati: quando un'azienda esegue il fine-tuning di un modello pre-addestrato con i propri dati, il risultato è un modello personalizzato che può essere considerato un nuovo "prodotto" derivato. La proprietà di questo nuovo modello dipenderà dai termini e condizioni stabiliti dal contratto con il fornitore della piattaforma cloud o di IA. OpenAI[108] ad esempio non consente agli utenti di ottenere la proprietà esclusiva del modello personalizzato, mentre Google[109] afferma che "non rivendicherà la proprietà dei contenuti originali" generati tramite l'uso delle sue API, ma "può generare contenuti uguali o simili": in altre parole, copiare il lavoro altrui.

Anche a livello reputazionale, sembra ragionevole ritenere che l'uso intenso di servizi stranieri, sostanzialmente tutti statunitensi, da parte di imprese importanti e di grandi dimensioni nazionali possa essere ritenuto sconveniente dal pubblico. Tali imprese di grandi dimensioni attive nel settore delle telecomunicazioni dovrebbero considerare questa come una soluzione al massimo provvisoria, in attesa di sviluppare soluzioni maggiormente personalizzate e proprietarie, a meno che riescano a negoziare accordi specifici e particolarmente controllabili con le imprese fornitrici dei servizi di IA, definendo in modo chiaro e trasparente le possibilità di utilizzo e di modifica del modello, le metodologie di trattamento dei dati personali, e la proprietà dei modelli derivati.

Si può comunque offrire una soluzione intermedia tra la realizzazione ex-novo di modelli di IA e l'affidamento totale a servizi di terze parti. Le imprese di telecomunicazioni possono infatti sfruttare soluzioni di intelligenza artificiale pre-addestrati senza per forza dipendere completamente da piattaforme "tutto in uno". Una possibilità già affrontata in tal senso è quella di utilizzare modelli open source, scaricabili e implementabili su infrastrutture locali o private, come GPT-J[110] o YOLO[111]. Il lato negativo è che per l'esecuzione le aziende dovranno utilizzare hardware locale, mantenendo però il controllo sui dati e riducendo la dipendenza dal cloud.

Un'altra opzione è adottare soluzioni on-premise fornite da aziende specializzate, come IBM Watson o SAS Viya, che permettono di personalizzare modelli IA direttamente nei data center aziendali. Inoltre, la containerizzazione di modelli tramite strumenti come Docker o Kubernetes consente di distribuirli su ambienti locali o multi-cloud, garantendo indipendenza dal fornitore.

Può anche immaginarsi il caso di collaborazioni strategiche con startup o istituti di ricerca per costruire da zero modelli innovativi su misura, con ottime possibilità di contrattazione specifica senza gli inevitabili vincoli provenienti dai grandi provider.

Sfruttamento economico dei modelli generati

Un'impresa attiva nel settore delle telecomunicazioni che si doti di un proprio modello di IA o investa sulla creazione degli stessi, specie se può disporre di buone possibilità economiche e computaizonali, può sviluppare interessanti metodologie di monetizzazione e di diversificazione

[108] Openai.com, *Termini di Servizio*, https://openai.com/it-IT/policies/service-terms/?utm_source=chatgpt.com
[109] Termini di servizio aggiuntivi dell'API Gemini, https://ai.google.dev/gemini-api/terms?hl=it#:~:text=Some%20of%20our%20Services%20allow,all%20rights%20to%20do%20so
[110] https://huggingface.co/EleutherAI/gpt-j-6b?utm_source=chatgpt.com
[111] https://github.com/ultralytics/ultralytics?utm_source=chatgpt.com

strategica, almeno sulla carta ed in questo momento storico di particolare interesse nei confronti dei servizi di IA. Si vuole qui intendere la vendita dei servizi di IA creati a proprio uso nel mercato europeo. Un modello IA addestrato su dati specifici, come il traffico di rete, la manutenzione predittiva o il comportamento degli utenti, rappresenta un asset unico che può essere monetizzato, a patto che i dati siano anonimizzati e conformi alle normative locali.

In questo senso, è opportuno operare seguendo la stessa logica dei giganti del settore: limitare contrattualmente l'uso del modello, tramite l'apposizione di clausole[112] che specifichino l'attribuzione dei creatori originali, gli scopi per cui può essere utilizzato, ed eventuali accordi anti-competitivi. Allo stesso modo, dev'essere preservata la riservatezza dell'addestramento dei dati sul quale è stato svolto e sull'eventuale modello originale. Il modello, peraltro, non deve essere onnicomprensivo: non si deve immaginare per forza un mastodontico sistema di IA onniscente ed onnipotente su tutte le questioni legate alle telecomunicazioni. Anche un semplice sistema, efficace e ben realizzato, di previsione dei guasti, o di raccolta di feedback utente, o di interazione con gli utenti (per esempio tramite chat) può essere richiesto e di notevole valore. Il succo, come in qualsiasi prodotto software, è che sia efficace a raggiungere gli obiettivi aspettati ed il più possibile leggero computazionalmente, permettendone la rapida esecuzione anche su dispositivi hardware non dotati di grande potenza o non più recentissimi.

Potenziamento offerta di servizi e somministrazione di servizi

L'introduzione dell'intelligenza artificiale nei servizi delle imprese di consente di agire sia sulla qualità intrinseca dei servizi che sull'esperienza complessiva del cliente. Si vuole qui suggerire una particolare attenzione un'attenzione particolare a quegli elementi che hanno un impatto immediato e diretto sull'utente, e che lo colpiscono, perché naturalmente sorprendenti o perché notevolmente migliorati, come i chatbot per l'assistenza. L'obiettivo è qui il potenziamento del rapporto con i clienti, con una conseguente miglioria in termini di soddisfazione e una possibile positiva ricaduta reputazionale.

Questi chatbot, ormai ben conosciuti, possono ormai facilmente essere perfezionati attraverso modelli IA capaci di comprendere e replicare il linguaggio naturale in modo fluido, offrendo quindi un'assistenza che sembri autentica e personale. Attraverso sistemi di analisi del comportamento, i chatbot potrebbero suggerire soluzioni specifiche, arrivando al punto di anticipare bisogni ed offrire suggerimenti nel merito delle preferenze individuali. Tuttavia, per ottenere quell'incremento reputazionale di cui si parlava, è indispensabile che i chatbot, e quanti altri strumenti di IA che interagiscano direttamente con i clienti, non siano lasciati a loro stessi, diventando, come spesso già sono, una barriera anzichè un aiuto. È opportuno integrarli in sistemi ibridi, dove gli operatori umani possono subentrare senza soluzione di continuità nelle situazioni che ne richiedono l'intervento. In ogni caso, come si è già avuto modo di vedere, la legislazione europea impone la presenza di un essere umano nel momento in cui si verifichino "effetti giuridici significativi" sulla

[112] Un suggerimento in tale senso può venire dalla Commissione Europea, *Procurement of AI Community*: *proposta di clausole contrattuali tipo per l'acquisto di intelligenza artificiale da parte delle organizzazioni pubbliche*, settembre 2023, https://public-buyers-community.ec.europa.eu/sites/default/files/2023-10/AI_Procurement_Clauses_Template_NON_HIGH_RISK_IT.pdf?utm_source=chatgpt.com

sfera individuale[113], ed in ogni caso è necessario poter risalire ad una catena di responsabilità umana nel momento in cui si utilizzano questi strumenti.

Parallelamente, l'IA può giocare un ruolo fondamentale nella qualità e affidabilità della rete. Attraverso la manutenzione predittiva, è in teoria possibile monitorare costantemente lo stato delle infrastrutture ed utilizzare i dati statistici dei guasti passati per tentare di prevedere i guasti futuri prima che si manifestino, limitando quindi i disservizi. L'utilizzo di un tale sistema è anch'esso foriero di un messaggio che sarebbe utile trasmettere ai clienti: un'azienda che utilizza l'IA per prevenire problemi può sembrare maggiormente all'avanguardia e tecnologicamente più affidabile, purché sia chiara la tutela offerta al cliente finale ed ai suoi dati.

Negli ultimi anni, le reti moderne si stanano poi allontanando dalle tradizionali infrastrutture propriamente hardware, per adottare approcci diversi, come la Virtualizzazione delle Funzioni di Rete (NFV)[114], un approccio che separa le funzioni di rete dall'hardware dedicato, consentendo di eseguirle anche su macchine generiche. Funzioni precedentemente dipendenti da hardware specifico sono ora sempre più virtualizzate ed eseguibili via software. Al contempo, il *Software Defined Networking* (SDN)[115] separa il piano di controllo, responsabile della gestione del traffico di rete, dal piano dati, dove il traffico viene effettivamente instradato. Questa separazione consente di centralizzare il controllo della rete in un software specifico, il controller SDN, che gestisce in modo dinamico il traffico attraverso dispositivi di rete programmabili, come switch e router, e consente di modificare in tempo reale le regole di instradamento e gestione. Questo connubio di approcci permette la riduzione dei costi operativi, e, già di notevole importanza per le reti 5G, è ragionevole presumere che diventi ancora più rilevante con l'avvento del futuro 6G.
In questo senso, l'IA può essere cruciale nell'ottimizzazione automatica delle reti, offrendo capacità avanzate di analisi dei dati, previsione del traffico e gestione delle risorse.

Esistono già soluzioni open source adottabili, che offrono alle aziende TLC l'opportunità di personalizzare e controllare le proprie infrastrutture di rete ausiliandosi dei sistemi di IA. Progetti come l'Open Networking Foundation[116] promuovono l'uso di software open source per la gestione delle reti, facilitando l'innovazione e la collaborazione nel settore. Inoltre, iniziative come Open AI Cellular[117] forniscono piattaforme aperte per la prototipazione e il testing di controller basati sull'IA, supportando la ricerca e lo sviluppo verso le reti 6G.

Per migliorare ulteriormente la percezione pubblica, le imprese di TLC devono quindi dimostrare che l'IA non è solo uno strumento ad uso interno: un macinatore di dati raccolti chissà come e chissà dove. Al contrario, deve essere percepita come un mezzo per ascoltare e rispondere meglio alle esigenze dei clienti, anche e soprattutto attraverso l'offerta esplicita di servizi migliorati o innovativi per questi stessi clienti. Questo è, peraltro, l'insegnamento che si può cogliere dal successo delle iniziative cittadine di Amsterdam e specialmente Helsinki.

---

[113] Come previsto perlatro dal GDPR, art. 22
[114] Aa.vv., *Network Funcitons Virtualization, Introductory White Paper*, SDN and OpenFlow World Congress, Darmstadt, Germania, 22-24 ottobre 2012, https://portal.etsi.org/NFV/NFV_White_Paper.pdf
[115] K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui, *Software-defined networking (SDN): a survey*, Security and Communication Networks, 7 febbraio 2017, https://onlinelibrary.wiley.com/doi/10.1002/sec.1737
[116] ONF, *Open Networking Foundation Formed to Speed Network Innovation*, Portland, 21 marzo 2011, https://opennetworking.org/news-and-events/press-releases/onf-formed-to-speed-network-innovation/
[117] https://www.openaicellular.org/

5.2. Sfide e opportunità per le aziende TLC nell'uso di modelli IA open e closed

Quest'ultimo capitolo vuole servire come un piccolo compendio di quanto si è detto sinora, distinguendo in particolare tra l'uso di modelli chiusi, forniti da giganti del settore come OpenAI, Microsoft e Google, e modelli più aperti: alternative che garantiscono maggiore flessibilità e controllo ma minore facilità di utilizzo, e offrono il potenziale di essere programmati per funzionare su infrastrutture locali (anziché su un cloud di terze parti).

I modelli chiusi offrono senz'altro un notevole vantaggio in termini di semplicità d'uso e accesso immediato a tecnologie avanzate. Questi modelli, si diceva, sono spesso ospitati su infrastrutture cloud e offerti come servizi (*AI-as-a-Service*), riducendo il carico sulle risorse hardware aziendali. Sono pertanto semplici da implementare, e non richiedono competenze interne avanzate, nè hardware all'avanguardia o spese eccessive. Tuttavia, l'uso di modelli chiusi crea inevitabilmente una serie di vincoli che possono portare a costi crescenti nel tentativo di eluderli, a limitazioni nei benefici ottenuti, a problemi di ordine legislativo e alla frequente sindrome da singolo ecosistema, che porta a difficoltà future nel momento in cui si volesse migrare verso altre soluzioni. Peraltro, si è osservato che spesso **i termini di servizio non consentono una personalizzazione approfondita né il pieno controllo sui dati e sull'output, o la proprietà dei modelli ai quali è stato fatto un fine-tuning finale**. Poiché l'elaborazione avviene su server esterni, i dati aziendali o dei clienti possono essere poi esposti a rischi di sicurezza o violazioni della privacy.

I modelli open source (con tutte le considerazioni già fatte su questo termine applicato all'IA) offrono un'alternativa che garantisce maggiore flessibilità e controllo ma enorme complicazione in più. Questi possono essere scaricati, personalizzati e implementati su infrastrutture locali, rendendoli una scelta interessante per le aziende TLC, magari già dotate di grandi dataset e potenza computazionale, che desiderano evitare vincoli di dipendenza da fornitori esterni. In questo senso, oltre ai modelli open source reperibili online, si possono considerare anche i potenziali modelli creati "in-house", cioè dalla stessa impresa di TLC. Si è però visto lungo tutto il documento come questo sia un obiettivo particolarmente difficile da raggiungere. Infine, la possibilità di eseguire i modelli in locale migliora -almeno, sulla carta- la privacy e la sicurezza, riducendo i rischi associati al trasferimento dei dati su infrastrutture cloud.

Vale la pena rimarcare infine una certa visione maggiormente favorevole all'uso di modelli più aperti, specie per le aziende che desiderano mantenere il controllo sui propri dati e operazioni. Questo approccio è particolarmente utile per le TLC che trattano dati sensibili, come quelli relativi alle reti, alla manutenzione o ai comportamenti degli utenti. La possibilità di eseguire modelli in locale rappresenta un doppio vantaggio: da un lato, garantisce una maggiore privacy e conformità alle normative; dall'altro, elimina la dipendenza da fornitori esterni. Tuttavia, questo beneficio comporta un costo: i modelli open richiedono infrastrutture hardware avanzate e risorse umane qualificate per la gestione e l'ottimizzazione.

6. Conclusioni

Le imprese di telecomunicazioni sono senz'altro tra le più interessate a sfruttare l'intelligenza artificiale come leva di innovazione e differenziazione, e per ottenere vantaggi competitivi sul mercato e un miglioramento dei servizi offerti. L'IA si sta affermando come un elemento chiave per ottimizzare la gestione delle risorse e creare esperienze utente personalizzate e innovative nella loro potenziale qualità. Tuttavia, il percorso per integrare l'IA in modo efficace è tutt'altro che semplice. Le difficoltà legate ai costi elevati, alla necessità di competenze tecniche avanzate e al rischio di dipendenza da fornitori di terze parti rappresentano sfide importanti che ogni impresa deve considerare attentamente.

Per le imprese dotate di mastodontiche risorse economiche e tecniche, creare un modello IA da zero è senza dubbio la scelta più vantaggiosa a lungo termine. La costruzione di un modello personalizzato offre una serie di benefici difficilmente replicabili: da prestazioni ottimizzate per le specifiche esigenze aziendali alla possibilità di rivendere il modello stesso, trasformandolo in una fonte di guadagno aggiuntiva. Inoltre, un modello sviluppato internamente consente all'azienda di mantenere il pieno controllo sui dati, un elemento cruciale in settori regolamentati come quello delle telecomunicazioni. In quest' ottica, collaborare con enti di ricerca o istituzioni accademiche può rappresentare una strategia particolarmente efficace per accedere a competenze specialistiche e accelerare i tempi di sviluppo. Queste collaborazioni possono non solo favorire l'innovazione, ma anche posizionare l'azienda come leader tecnologico, rafforzandone il valore reputazionale.

Tuttavia, non tutte le imprese possono permettersi i costi e il tempo necessari per sviluppare modelli IA da zero. Per queste realtà, l'adozione di modelli pre-addestrati rappresenta una valida alternativa. In questo caso, si è visto in corso di trattazione come sia tendenzialmente preferibile orientarsi verso soluzioni open source, che offrono maggiore flessibilità e controllo rispetto ai modelli chiusi forniti da grandi operatori del cloud. Utilizzare un modello open permette di personalizzarlo in base alle esigenze specifiche, riducendo i rischi di lock-in e i vincoli imposti dai fornitori esterni. Tuttavia, questa scelta non è priva di problemi. L'adozione di soluzioni open richiede risorse hardware significative e competenze tecniche avanzate per gestire il processo di personalizzazione e ottimizzazione. Inoltre, l'open source stesso è un concetto che, nel contesto dell'IA, sta diventando sempre più ambiguo.

La questione dell'open washing è infatti centrale nel dibattito sull'IA. Molte aziende dichiarano di utilizzare approcci open per ottenere vantaggi reputazionali o eludere gli obblighi normativi, come quelli previsti dall'AI Act, senza però rispettare appieno i principi dell'open source. Questo fenomeno non solo confonde il mercato, ma mina anche la fiducia degli utenti verso i sistemi IA. La community open source, tradizionalmente un bastione di trasparenza e innovazione collaborativa, è oggi in fermento di fronte alla trasformazione dell'IA: le nuove definizioni di "open" devono necessariamente includere non solo il codice sorgente, ma anche i pesi e l'indicazione dei dataset utilizzati per addestrare i modelli, elementi indispensabili per garantire la reale accessibilità e replicabilità dei sistemi, e prevenire quella che si è descritta come la "crisi della riproducibilità".

In questo contesto di incertezza, emergono esempi virtuosi che le imprese di TLC potrebbero considerare. I registri cittadini di Helsinki e Amsterdam rappresentano un esempio per dimostrare come l'IA possa essere utilizzata in modo trasparente e orientato al benessere pubblico. Sebbene queste iniziative abbiano finalità pubbliche, offrono lezioni importanti anche per il settore privato:

investire in IA non significa solo migliorare i servizi, ma anche contribuire a costruire un ecosistema di fiducia e innovazione. Le imprese di TLC potrebbero adottare strategie simili, comunicando apertamente l'uso dell'IA per offrire servizi superiori e coinvolgendo i clienti in una visione consapevole della tecnologia.

Ciononostante, è fondamentale agire con cautela. Le normative sull'IA sono ancora in evoluzione, e i metodi con cui le autorità nazionali controlleranno i sistemi di IA non sono ancora del tutto chiari. Questo implica che ogni decisione relativa all'adozione dell'IA debba essere basata su un'attenta valutazione dei rischi e delle opportunità, con particolare attenzione alla conformità legale e alla protezione dei dati. Più volte, in corso di trattazione, si sono visti esempi variamente utili per la predisposizione di una "model card" o comunque di un'analisi completa sul rischio, le opportunità e le necessità derivanti dall'utilizzo di un sistema IA in un certo settore.

In un contesto competitivo e in continua evoluzione come quello delle telecomunicazioni e dell'intelligenza artificiale in generale, avere una precisa ed efficace visione strategica, ed avere ben presenti i problemi ed i rischi legati ad altrettante opportunità, rappresenta con ogni probabilità un elemento chiave per il successo a lungo termine.