Cloud. Meloni: “In legge di Bilancio norme per favorire gli investimenti in software”

Meloni all’assemblea di Assolombarda: *“Urgente una governance sull’AI”*

“*La crescita italiana è ancora debole, dobbiamo intervenire sugli investimenti*“, ha dichiarato la presidente del Consiglio dei ministri, **Giorgia Meloni**, nel suo discorso all’Assemblea Generale di **Assolombarda**, l’associazione degli industriali della città metropolitana di Milano e delle province di Lodi, Monza e Brianza e Pavia.

A frenare la crescita, ha sottolineato Meloni è “*la bassa produttività*“, specificando che il valore per il 2026 può arrivare all’1% e aggiungendo però una cosa importante: “*È urgente una governance sull’**intelligenza artificiale***”.

L’affermazione è una risposta diretta a quanto sostenuto dal Presidente di Assolombarda, **Alvise Biffi**, che, parlando di produttività come “*unica strada per generare benessere diffuso*“, ha ovviamente tirato in ballo l’intelligenza artificiale, “*una grande opportunità per rilanciare la crescita e invertire la rotta*”. Una rotta rallentata da diversi fattori, per Biffi, tra cui: “*la dimensione delle imprese, la carenza delle competenze digitali, i pochi investimenti in ricerca e sviluppo, il circolo vizioso salariale e, sempre più, i costi dell’energia*”.

“In Legge di bilancio una misura di carattere fiscale per agevolare gli investimenti in software”

Su questo Meloni ha parlato della necessità e dell’urgenza di una “***governance dell’AI***”, un tema “*che va affrontato a livello globale”,* ricordando che l’Italia ha posto l’AI al centro della sua presidenza del G7. A livello nazionale, comunque, è stato già avviato un percorso virtuoso, come nel caso di **Milano**, che “*a buon diritto può essere considerato un **hub digitale** di livello europeo*”.
Milano è stata inoltre proposta da Assolombarda, Confcommercio e AmCham Italy a **sede di una nuova struttura delle Nazioni Unite**, dedicata proprio alla governance dell’intelligenza artificiale. La candidatura sarà presentata alle istituzioni il prossimo 9 novembre.

“*Questo Governo* – ha detto Meloni – *ha introdotto una procedura autorizzativa unica, che consente di semplificare le procedure, tagliare i tempi per costruire sul nostro territorio i data center e le relative connessioni, perché sappiamo quanto la capacità di calcolo rappresenti un nuovo asset strategico per competere in questo ambito. Allo stesso modo, lavoriamo a livello europeo perché l’Italia possa ricoprire un ruolo da protagonista in questo segmento*“.

“*La legge nazionale sull’IA ha messo a disposizione 1 miliardo di euro di investimenti per le imprese che sviluppano intelligenza artificiale, cybersicurezza e tecnologie abilitanti. Un primo segnale per dire che l’Italia non rimanga indietro e al quale ora ne vogliamo aggiungere un altro* – ha aggiunto la Premier – *considero di buon senso trovare il modo di promuovere anche gli **investimenti in software utilizzati tramite i contratti di cloud**. Quindi voglio annunciare che con il ministro Giorgetti stiamo lavorando per introdurre nella Legge di bilancio una **misura di carattere fiscale per***

agevolare gli investimenti *per questa tipologia di beni*“.

“*Vogliamo ricoprire ruolo da protagonista*”, ha proseguito Meloni, illustrando la sinergia avviata con gli Emirati Arabi Uniti per far nascere **a Pavia un campus data center da 500 MW**, primo passo per infrastruttura su larga scala per tutto il territorio nazionale fino a 1 GW, perché ha ricordato che “*finanziamo con 25 miliardi di euro diversi programmi strategici per realizzare queste infrastrutture anche al Sud*”.

Physical AI applicata alla manifattura industriale, l’Italia può giocare ruolo da protagonista

La Lombardia svolge e svolgerà sempre più un ruolo di traino, “*ma tutto il territorio italiano deve contribuire a questo successo in maniera sostenibile e inclusiva*”, per questo, ha aggiunto la Presidente del Consiglio, è stato stanziato 1 miliardo per le imprese che sviluppano AI e tecnologie abilitanti per non far rimanere indietro il nostro Paese.

Poi è stato ripreso il tema della **physical AI** e secondo Meloni l’Italia può giocare un ruolo da protagonista in questo campo, anche rispetto a USA e Cina, che certamente partono in grande vantaggio per quel che riguarda gli LLM. Quello della physical AI “*è terreno diverso, perché agli algoritmi vanno aggiunti sensori, meccatronica e* ***conoscenza profonda dei processi produttivi industriali****, che all’Italia non manca. Abbiamo filiere che presidiano ogni fase della produzione, con grandi competenze. Qui possiamo dire la nostra portando* ***l’AI nell’industria manifatturiera****”.*

Un punto di vista sulla physical AI che è stato condiviso dal Presidente di Assolombarda: “*questa è la nostra grande opportunià. Questa volta non dobbiamo limitarci a adottare la tecnologia: possiamo finalmente contribuire a costruirla*”.

“La via italiana all’AI”

Un settore in cui è possibile parlare di “***via italiana all’AI***”, secondo Meloni, e dove lavorare “*per rendere competitive tutte le imprese e creare posti di lavoro*”: “*Dobbiamo passare da utilizzatori a produttori*”.

Dalla nostra abbiamo una grande mole di dati e di dati di qualità soprattutto. Come ha ricordato lo stesso Biggi, l’AI “*deve incidere sulle caratteristiche che distinguono il nostro modello industriale, rafforzando ciò che ci rende competitivi: qualità, specializzazione, capacità di adattamento, conoscenza dei processi, ruolo nelle filiere e presenza sui mercati*”.

Meloni ha poi ricordato anche l’iniziativa **ForgIA**, che ha l’obiettivo di “*creare un ecosistema nel quale le imprese potessero estrarre e raffinare dati industriali e metterli al sicuro rendendoli interoperabili lungo la filiera senza perderne il controllo*”.

“Entro dieci anni inizieremmo a produrre energia dal nuovo nucleare”

“*Abbiamo lavorato per aumentare la potenza installata con le* ***rinnovabili****, che infatti è cresciuta di quasi il 40%, abbiamo rilanciato la produzione nazionale di petrolio e gas, perché non è sensatissimo comprarli a migliaia di chilometri da qui quando una parte la possiamo estrarre in Italia, e* – ha dichiarato la Premier – *abbiamo varato la legge che consente di riprendere dopo 40 anni il cammino del* ***nucleare****. Il provvedimento appena approvato in Parlamento mette a disposizione una cornice completa: la piattaforma nazionale per il nucleare sostenibile, la delega al Governo, il rafforzamento dell’ispettorato per la sicurezza nucleare, la governance dell’intero ciclo di vita degli impianti*“.

Il tema dell'energia, d'altronde, è una "*precondizione per crescita e competitività*", ha sottolineato Meloni, aggiungendo che grazie al lavoro del Governo: "*Sono state create le condizioni per avviare un percorso che ha un obiettivo ambizioso quanto necessario: arrivare a* ***produrre energia da nuovo nucleare entro il prossimo decennio***".

La premier ha poi attaccato l'Ets (*Emission trading system*), il sistema europeo di scambio di quote di emissione, definendolo meccanismo che "*gonfia artificialmente i prezzi, crea squilibri tra gli Stati membri, danneggia le nostre imprese manifatturiere particolarmente nella loro capacità di competere in un mercato globale nel quale i nostri principali concorrenti non sono neanche lontanamente sottoposti allo stesso livello di costo del carbonio e agli stessi vincoli*".

The post Cloud. Meloni: "In legge di Bilancio norme per favorire gli investimenti in software" appeared first on Key4biz.

https://www.key4biz.it/cloud-meloni-in-legge-di-bilancio-norme-per-favorire-gli-investimenti-in-software/590868/

Anthropic vieta la crudeltà verso Claude, ma il vero nodo è la dipendenza tecnologica

Insultare l'AI ***Claude*** sarà presto una violazione delle regole d'uso di **Anthropic**. Dal prossimo **12 novembre**, la policy della società proibirà **comportamenti "inutilmente abusivi o crudeli"** verso i suoi modelli. La precisazione è importante: Anthropic

parla di casi estremi e “ripetuti”, senza uno scopo riconoscibile. Restano fuori la normale frustrazione, le critiche, i temi narrativi oscuri (che può essere anche un romanzo dal linguaggio volutamente estremo) e i test di ricerca.

Per ora, la misura principale non è il blocco dell’account: Claude può **interrompere una conversazione** con un utente persistentemente aggressivo. La testata online *The Verge* riferisce che Anthropic non ha chiarito se siano previste altre sanzioni, come la **sospensione degli utenti**. Già nel 2025 la società aveva spiegato che, dopo la chiusura di una chat, si può avviarne subito un’altra, assicurando che le altre conversazioni dell’account non vengono coinvolte da questo tipo di dinamiche. Parlare di un utente che rischia di perdere “tutto Claude” sarebbe quindi, allo stato delle informazioni disponibili, eccessivo.

La vera domanda non è se un’AI sia cosciente o meno, ma chi lo stabilisce

Anthropic presenta la scelta come parte della propria ricerca sul possibile “benessere dei modelli”. La società ammette di essere “altamente incerta” sullo “status morale” dei sistemi come *Claude*: non sostiene che l’AI sia cosciente, ma considera prudente introdurre misure a basso costo nel caso in cui un giorno emergessero elementi per prendere sul serio questa possibilità.

È un tema che divide anche il settore: il CEO **Dario Amodei** non ha escluso la possibilità che i modelli possano essere coscienti; altri leader tecnologici hanno contestato l’idea di attribuire loro una forma di welfare o diritti. Oggi, non abbiamo prove che un chatbot provi dolore quando viene insultato e sinceramente non dovremmo neanche porci di queste

domande.
A questo punto, prima di preoccuparci dei sentimenti di Claude, forse ci converrebbe trattare meglio la nostra automobile, visto che garantisce che torniamo a casa sani e salvi (ancora di più quando sarà a guida autonoma), o magari il frigorifero, viso che custodisce il nostro cibo, o magari il Pc o lo smartphone, visto che in essi abbiamo trasferito tutta la nostra esistenza trasposta in dati.

Questo non significa che urlare contro un software sia un'abitudine innocua o particolarmente salutare per il nostro sistema nervoso. Il punto è un altro: **chi stabilisce quando una critica o qualcosa di più 'forte' diventa crudeltà?** La policy restringe il campo ai casi estremi, ma la distinzione resta affidata al fornitore e ai sistemi che applicano le sue regole. La macchina può chiudere la chat; l'azienda può definire i criteri e cambiarli nel tempo. È una posizione di vantaggio che merita attenzione, anche senza immaginare *Claude* in tribunale come parte lesa.

Il rischio concreto: dipendere da un solo fornitore

La questione più urgente, per chi usa *Claude* ogni giorno, non è la coscienza artificiale: è la **dipendenza dai servizi AI**. Se un assistente entra nei flussi di lavoro, aiuta a scrivere, programmare, cercare informazioni o gestire attività aziendali, anche un'interruzione può avere un costo e di varia natura e dimensione. In questa vicenda Anthropic parla soprattutto della chiusura di singole conversazioni, non della disattivazione generale del servizio. Ma il potere di stabilire le condizioni d'accesso resta in mano a un'impresa privata.

Per utenti e imprese, la risposta non è rinunciare all'AI né trattare ogni chatbot come un collega in carne e ossa. È evitare che un solo strumento diventi insostituibile:

conservare copie del lavoro, prevedere alternative, poter cambiare modello o fornitore. Per l'Europa, e non è una forzatura, il caso riporta al centro la **sovranità digitale**: affidarsi a piattaforme extraeuropee significa anche dipendere da regole, infrastrutture e decisioni prese altrove. La gentilezza verso le macchine può essere una buona abitudine, magari una forma di autocontrollo utile in ogni situazione. Il pieno controllo sul proprio lavoro è però un'altra faccenda che non c'entra niente sull'ipotetica coscienza delle macchine.

The post Anthropic vieta la crudeltà verso Claude, ma il vero nodo è la dipendenza tecnologica appeared first on Key4biz.

https://www.key4biz.it/anthropic-vieta-la-crudelta-verso-claude-ma-il-vero-nodo-e-la-dipendenza-tecnologica/590829/

"Artificial", il film di Guadagnino sui rischi dell'AI (girato anche in Italia) debutta a New York. "Brutto" per il CEO di OpenAI

Dopo un accordo da quasi 50 miliardi di dollari, Amazon ha rinunciato a distribuire *Artificial*, il nuovo film di **Luca Guadagnino** sulla nascita e la caotica ascesa di **OpenAI**. La pellicola, commissionata in origine dal colosso di Jeff Bezos, è stata poi acquisita da **Neon**. Presentato in anteprima mondiale al New York Film Festival il 5 ottobre 2026, *Artificial* ricostruisce la vicenda che nel novembre del 2023

portò al licenziamento lampo di **Sam Altman**, rimosso dal consiglio di amministrazione di OpenAI e reinsediato pochi giorni dopo. A interpretarlo è **Andrew Garfield**, affiancato da Yura Borisov nel ruolo di Ilya Sutskever, da **Monica Barbaro** nei panni di Mira Murati e da Ike Barinholtz, che interpreta **Elon Musk**. È una storia che, nelle parole di Guadagnino, parla di tecnologia ma soprattutto di «ambizione e potere». Tra i temi centrali emerge il contrasto tra Sutskever, scienziato legato a OpenAI, e Altman, rappresentato come una figura ambiziosa dal carattere complesso. «Looks awful», «sembra brutto» così ha commentato lo stesso Altman dopo aver visto il trailer. Guadagnino considera il giudizio significativo, pur definendolo infantile e dichiara di non aver mai cercato un incontro diretto con lui: una scelta motivata dalla volontà di evitare qualsiasi possibile conflitto di interessi.

Una storia arrivata al momento giusto

In un’intervista a Repubblica, Guadagnino racconta di aver ricevuto il copione dai suoi contatti in Amazon: aveva seguito sui giornali l’espulsione di Altman e il suo ritorno, ma non aveva ancora una visione chiara di ciò che era davvero accaduto. La storia lo ha conquistato immediatamente. Il regista ha deciso di muoversi coinvolgendo alcuni degli attori che avrebbe voluto nel film. Yura Borisov, Monica Barbaro e Andrew Garfield hanno accettato subito l’idea del progetto e Guadagnino ha convinto Amazon a non rimandare la produzione. Per lui quella rapidità era essenziale: la vicenda era recente e le sue conseguenze stavano già influenzando l’evoluzione dell’intelligenza artificiale. La realizzazione del film è stata preceduta da un accurato lavoro di ricerca, condotto dagli sceneggiatori insieme a un gruppo di ricercatori, con l’obiettivo di ricostruire gli avvenimenti nel modo più veritiero possibile. Una parte consistente dei dialoghi, infatti, deriva da dichiarazioni realmente pronunciate.

Artificial come simbolo del progresso dell’intelligenza artificiale

Chi controlla una tecnologia capace di trasformare la società? Guadagnino osserva come la crescita dell’AI possa condurre **all’estinzione del genio creativo umano**, invitando tuttavia a leggere queste profezie anche alla luce degli interessi economici che ruotano attorno al settore. Il potere, dunque, è uno dei temi centrali del film, che si basa sulla lettura di Karen Hao, autrice di *Empire of AI* e consulente del progetto, secondo cui questa è anche una storia di «concentrazione del potere nelle mani di una piccola élite». Il regista precisa, però, di non voler trasformare il suo lavoro in una lezione o in una predica, ma di voler lasciare allo spettatore la libertà di elaborare la propria interpretazione.

Una storia americana costruita in Italia

Nonostante la storia sia ambientata nella Silicon Valley, *Artificial* è stato girato quasi interamente in Italia. Soltanto cinque giorni di riprese si sono svolti a San Francisco; il resto della produzione si è sviluppato tra **Reggio Emilia, Ivrea e Torino**. Quando alcune delle location originali non erano disponibili, Guadagnino e il suo scenografo hanno ricostruito gli ambienti in alcuni teatri di posa, lavorando sulla base di fotografie e testimonianze di persone che conoscevano direttamente quei luoghi. L’obiettivo era ottenere una riproduzione il più simile possibile a quella degli uffici di OpenAI. San Francisco rimane tuttavia una presenza fondamentale nell’immaginario del film. Per il regista la città rappresenta «l’utopia americana», animata dalla cultura e dalla socialità.

La difesa del processo creativo umano

Guadagnino non si considera un utilizzatore abituale dell’intelligenza artificiale. Racconta di aver utilizzato ChatGPT una sola volta, per ottenere rapidamente un render necessario alla progettazione di un lampione. Il risultato, però, non lo ha convinto e ha preferito attendere il lavoro dei suoi architetti. La sua principale preoccupazione riguarda soprattutto l’uso dell’intelligenza artificiale come sostituto della creatività umana. La fatica dell’ideazione è una parte fondamentale del suo lavoro. Il cinema, per lui, nasce dall’incontro tra le diverse professionalità che partecipano alla realizzazione di un film. È proprio dal dialogo, dal confronto e dall’errore che può nascere qualcosa di inatteso. Per questo **un semplice prompt**, per quanto efficiente, rischierebbe di eliminare proprio ciò che considera più prezioso, ovvero il processo umano che porta alla realizzazione di un’opera. È una convinzione che attraversa anche il modo in cui Guadagnino concepisce la regia. L’autorialità, sostiene, non coincide necessariamente con la scrittura della sceneggiatura. Il film prende forma attraverso le immagini, il montaggio e tutto ciò che accade dopo la pagina. *Artificial*, in questo senso, è anche una dichiarazione sul valore del lavoro collettivo e umano che sta dietro a un film.

The post “Artificial”, il film di Guadagnino sui rischi dell’AI (girato anche in Italia) debutta a New York. “Brutto” per il CEO di OpenAI appeared first on Key4biz.

https://www.key4biz.it/artificial-il-film-di-guadagnino-sui-rischi-dellai-girato-anche-in-italia-debutta-a-new-york-brutto-per-il-ceo-di-openai/590754/

Chi è Jay Clayton, a capo della task force voluta da Trump sulla Super Intelligenza

A guidare la “Super Intelligence Force”, la nuova task force per l’intelligenza artificiale voluta da **Donald Trump** per coordinare l’azione delle amministrazioni federali statunitensi e assicurare il primato degli Usa nel settore, non sarà un nome forte della Silicon Valley, ma un “uomo del presidente”, **Jay Clayton**, direttore dell’intelligence nazionale e ribattezzato da Trump il nuovo “zar” dell’intelligenza artificiale.

Chi è Jay Clayton

Avvocato specializzato in diritto societario, Clayton ha lavorato nella sua carriera su alcune importanti **operazioni finanziarie** – durante la crisi del 2008 si è occupato dei dossier legati a Bear Stearns e Lehman Brothers, mentre nel 2014 ha traghettato la quotazione di Alibaba a Wall Street – per passare poi all’amministrazione pubblica sotto la prima presidenza Trump come **capo della Securities and Exchange Commission**, l’autorità vigilante dei mercati finanziari americani. Dopo quest’esperienza (e il suo ritorno al settore privato) Trump lo ha richiamato nel 2025 per affidargli prima il ruolo di procuratore federale di Manhattan e poi, nel 2026, l’importante incarico della direzione dell’intelligence nazionale, consegnandogli infine le chiavi della Super Intelligence Force.

Prima di prendere le redini della task force – composta, tra gli altri, dal vicepresidente **JD Vance**, il segretario alla Difesa **Pete Hegseth** e il segretario al Tesoro **Scott Bessent** – Clayton aveva espresso molto chiaramente le sue posizioni sul tema AI: **gli Stati Uniti non devono rallentare**, pena la perdita della corsa con la Cina. In un'intervista rilasciata qualche giorno prima della nomina a *Squawk Box*, il famoso programma televisivo di economia e finanza della *Cnbc*, Clayton si era espresso contro la sospensione dello sviluppo dell'intelligenza artificiale. "Non credo che nessun americano dovrebbe pensare che questa sia una buona strategia", aveva commentato. Una linea che rispecchia in pieno quella del presidente Trump. E non solo.

La posizione divergenti delle società AI

Mentre **Sam Altman** e **Dario Amodei** chiedono di rallentare e valutare i pericoli generati dall'AI (una posizione non forzatamente nobile, ma che potrebbe essere frutto di una mossa di marketing o della paura che una bolla speculativa scoppi tra le mani di OpenAI e Anthropic), c'è chi, come **Jensen Huang**, Ceo di Nvidia, considera gli allarmismi eccessivi e qualsiasi ingerenza governativa (o almeno le ingerenze contrarie allo sviluppo) un'invasione di campo. "**La sicurezza è un problema di ingegneria, non di diritto**", ha dichiarato Huang alla conferenza Dreamforce di Salesforce (15-17 settembre). "Dopotutto, stiamo sviluppando software. Stiamo sviluppando sistemi informatici. È un sistema informatico complesso, ma in definitiva è pur sempre un sistema informatico". Huang sostiene che non ci sia bisogno di nuove leggi o regolamenti, ma che il libero mercato bilancerà automaticamente i poteri ed eviterà l'immissione di prodotti pericolosi.

I prossimi passi della task force

La Super Intelligence Force dovrà presentare **il suo primo rapporto entro 120 giorni**. La squadra lavorerà con le aziende del settore per individuare i principali rischi e minacce (dalla cybersecurity all'utilizzo dell'AI per scopi militari o attacchi biologici), cercando di tenere al contempo sotto controllo eventuali misure regolatorie del Congresso che potrebbero frenare l'innovazione. E per come stanno andando le cose, immaginiamo che quest'ultima funzione sarà particolarmente cara al presidente Trump.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/chi-e-jay-clayton-a-capo-della-task-force-voluta-da-trump-sulla-super-intelligenza/590412/

AI. La Città di New York

chiama a testimoniare Anthropic, OpenAI, Google e Meta

L'**intelligenza artificiale** (AI) finisce sotto esame a New York. Il Consiglio comunale ha convocato i rappresentanti di **Anthropic, OpenAI, Google e Meta** per una testimonianza pubblica sotto giuramento sui rischi delle tecnologie AI. Per ottenere la partecipazione di **SpaceXAI** (rinominata SpaceXSI), la società di Elon Musk, la presidente del Consiglio **Julie Menin** ha invece emesso una *subpoena*, un atto che impone la comparizione. A quanto riportato da *Cnbc*, la società non aveva risposto alle richieste dell'assemblea.

L'audizione, fissata per oggi, riunisce tutti i 51 membri del Consiglio "*in una rara seduta plenaria*". Secondo l'agenda, inizierà alle 11 ora della costa orientale. Le altre quattro aziende hanno confermato la presenza dopo che Menin aveva minacciato di ricorrere allo stesso strumento legale. L'obiettivo è ascoltare le imprese e raccogliere elementi sulle possibili misure di tutela per i cittadini.

Dagli agenti fuori controllo alle nuove regole

L'iniziativa nasce dopo le segnalazioni di **incidenti in cui modelli di AI avrebbero agito oltre i limiti previsti**, accedendo a sistemi e piattaforme online. Il Consiglio richiama, tra gli altri casi, l'accesso non autorizzato di modelli a Hugging Face, piattaforma usata dagli sviluppatori. Aumentano inoltre le preoccupazioni espresse da ricercatori e addetti ai lavori sui rischi legati alla crescente autonomia dei sistemi.

All’audizione sono attesi anche esperti di sicurezza, tecnologia e tutela dei consumatori, tra cui ex ricercatori di Google DeepMind e OpenAI e **Jacob Coxon**, che ha lasciato Anthropic dopo aver criticato la gestione dei rischi da parte dell’industria.

Sul tavolo ci sono anche proposte di legge cittadine: un programma di **incentivi per chi segnala dall’interno problemi di sicurezza**, la possibilità per i newyorkesi danneggiati da agenti AI di **agire in giudizio** e requisiti di verifica indipendente dei sistemi. Si tratta per il momento solo di proposte.

Il peso della testimonianza e i limiti del Comune

La comparizione sotto giuramento rende l’audizione più incisiva di un confronto pubblico ordinario: le aziende dovranno rispondere alle domande dei consiglieri e confrontarsi con le proposte di regolazione. Per SpaceXAI, un’eventuale mancata comparizione potrebbe portare il Consiglio a chiedere l’esecuzione della citazione alla Corte Suprema dello Stato di New York.

L’iniziativa non ha natura di regolazione nazionale sull’AI. Il Consiglio può indagare su questioni che riguardano la città e intervenire nei limiti delle proprie competenze. L’audizione è importante, comunque, perché porta le imprese a discutere pubblicamente dei rischi e delle responsabilità, mentre le autorità valutano come proteggere infrastrutture, servizi e cittadini dall’uso improprio di sistemi sempre più autonomi.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/ai-la-citta-di-new-york-chiama-a-testimoniare-anthropic-openai-google-e-meta/590398/

Responsabilità e rischio nei sistemi di IA: il ruolo del contratto tra AI Act e NIS2

Nel percorso di analisi dedicato alla governance giuridica dell’Intelligenza Artificiale e alla progressiva costruzione del quadro regolatorio europeo, si è evidenziato come il diritto sia chiamato a confrontarsi con una crescente complessità tecnologica e con nuove forme di distribuzione del rischio. In questo contesto, emerge con particolare evidenza un nodo ancora solo parzialmente esplorato dalla dottrina e dalla regolazione.

Questo approfondimento, che conclude la serie di contributi, si concentra proprio su tale asimmetria: da un lato, l’AI Act, la direttiva NIS2 e la nuova disciplina sulla responsabilità da prodotto rafforzano in modo significativo gli strumenti di

prevenzione, sicurezza e gestione del rischio; dall'altro, resta meno definita la concreta allocazione delle responsabilità quando i sistemi di Intelligenza Artificiale producono errori, danni o risultati inattesi.

Il risultato è un impianto normativo fortemente orientato alla prevenzione, ma ancora parzialmente incompleto sul piano della responsabilità ex post. È in questo spazio che si inserisce l'analisi che segue, dedicata al ruolo del contratto come strumento di governo e distribuzione del rischio nei sistemi di IA.

Sistemi di IA e non prevedibilità degli output come problema giuridico di partenza

Dall'analisi sin qui svolta emerge, dunque, la rilevanza della non prevedibilità degli *output* come elemento determinante per un'analisi giuridica dell'utilizzo dei modelli di IA.

Si è già notato come tale caratteristica costituisca un tratto strutturale di svariati modelli di IA contemporanei, in particolare di quelli basati su tecniche di apprendimento automatico e, più specificamente, sui modelli di *deep learning*.

Questa dimensione probabilistica implica che, pur in presenza di *input* identici o molto simili, il sistema possa produrre risultati differenti o non completamente prevedibili. L'*output* non è quindi rigidamente predeterminato dal programmatore, ma emerge dal funzionamento del modello addestrato su grandi quantità di dati. Ne deriva una parziale perdita di controllo *ex ante* sul comportamento del sistema, che rende più complessa l'attribuzione delle responsabilità giuridiche in caso di errore, malfunzionamento o danno.

A tale problematica si aggiunge un ulteriore elemento di

complessità rappresentato dalla limitata trasparenza di molti modelli di IA avanzati.

In particolare, nei sistemi basati su modelli di apprendimento profondo e su grandi modelli linguistici (*Large Language Models*)[1], il funzionamento interno del sistema risulta spesso difficilmente comprensibile anche per gli stessi sviluppatori.

La mancanza di trasparenza costituisce una delle principali criticità da affrontare nella diffusione di tali tecnologie: da un lato rende più difficile per gli utenti comprendere i meccanismi decisionali dei sistemi di IA, alimentando talvolta diffidenza e resistenza alla loro adozione; dall'altro lato può ostacolare l'identificazione e la correzione di eventuali *bias* presenti nei modelli, proprio a causa della difficoltà di analizzare in modo diretto i processi decisionali sottostanti[2].

La trasparenza assume inoltre rilievo anche sotto il profilo dell'adeguamento normativo e della supervisione. Quando i processi decisionali dei sistemi risultano opachi, diventa più complesso verificare se essi rispettino effettivamente gli standard previsti da leggi, regolamenti e linee guida. Ciò può rendere più difficile per autorità di controllo, organizzazioni e utilizzatori accertare la conformità dei sistemi di IA ai requisiti imposti dal diritto europeo.

In questo contesto si inserisce il noto problema della "*black box*", divenuta emblematica delle sfide poste dai sistemi basati su reti neurali profonde che producono decisioni attraverso processi computazionali la cui logica interna risulta in larga misura opaca. Tale opacità non rappresenta semplicemente un limite tecnico contingente, ma costituisce spesso una caratteristica intrinseca di determinate architetture algoritmiche. Come evidenziato nel quadro metodologico elaborato dal National Institute of Standards and Technology nel proprio AI Risk Management Framework (NIST)[3],

esiste infatti una relazione strutturale tra capacità predittiva dei modelli e loro interpretabilità: sistemi caratterizzati da elevata complessità e performance tendono a risultare meno facilmente spiegabili.

Si delinea così quello che è definito un vero e proprio "paradosso della trasparenza": i sistemi di Intelligenza Artificiale più avanzati e performanti, proprio perché fondati su architetture algoritmiche altamente complesse, risultano spesso anche i meno interpretabili sotto il profilo del loro funzionamento interno[4]. Questa tensione tra efficacia tecnologica ed esigenza di comprensibilità rappresenta uno dei nodi centrali del dibattito giuridico e regolatorio sull'IA.

Tale lettura non è tuttavia priva di obiezioni nella letteratura tecnica più recente. Una parte autorevole della scienza dei dati ha contestato la natura ineluttabile del *trade-off* fra accuratezza e interpretabilità, sostenendo che, per i contesti decisionali ad alto impatto, sia preferibile progettare modelli intrinsecamente interpretabili piuttosto che sviluppare metodi *post hoc* di spiegazione di modelli opachi (cfr. C. Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, in *Nature Machine Intelligence*, vol. 1, 2019, 206 ss.).

La distinzione assume rilievo anche sul piano regolatorio, poiché incide direttamente sulla qualità dell'adempimento degli obblighi di trasparenza imposti dall'AI Act: una documentazione tecnica chiara e una *governance* basata su modelli interpretabili in origine offrono garanzie sostanziali più robuste rispetto a tecniche di *Explainable AI* applicate a sistemi *black box* già addestrati.

Queste caratteristiche pongono un problema giuridico di fondo: il modello tradizionale di imputazione della responsabilità, costruito attorno all'idea di controllo e prevedibilità di un comportamento, pur conciliato con gli obblighi di prevenzione

introdotti dalla legislazione europea e nazionale, risulta in ogni caso parzialmente inadeguato e insufficiente quando applicato ai sistemi di IA.

Se il comportamento del sistema non è completamente governabile e prevedibile *ex ante* e se i processi decisionali risultano in parte opachi, diventa più complesso stabilire quando un determinato risultato sia imputabile a un difetto del sistema, a un errore nell'addestramento, a un uso improprio da parte dell'utente o a fattori esterni non controllabili.

In questo senso, il limite della norma non deriva soltanto da una eventuale lacuna del Legislatore, ma trova la propria ragione nella natura stessa della tecnologia regolata.

L'IA introduce infatti una dimensione di incertezza strutturale che difficilmente può essere eliminata attraverso un incremento degli obblighi normativi o mediante una regolazione più dettagliata. Anche un sistema regolatorio particolarmente articolato non sarebbe in grado di prevedere tutte le possibili configurazioni di rischio derivanti dall'interazione tra modelli di IA, utenti e contesti applicativi.

Di conseguenza, il problema giuridico non può essere affrontato esclusivamente attraverso l'imposizione di nuovi obblighi legislativi. Piuttosto, appare necessario affiancare alla regolazione pubblica strumenti giuridici più flessibili, capaci di adattarsi alle specificità dei singoli rapporti tra i soggetti coinvolti nello sviluppo, nella distribuzione e nell'utilizzo dei sistemi di Intelligenza Artificiale, alla luce delle caratteristiche proprie del singolo rapporto.

In questa prospettiva, il contratto assume un ruolo centrale, quale strumento idoneo a disciplinare in modo puntuale e preciso la ripartizione dei rischi e delle responsabilità tra le parti, in relazione al singolo caso.

La contrattualizzazione della responsabilità come risposta funzionale

Attraverso specifiche clausole contrattuali, le parti possono definire *ex ante* i limiti di utilizzo del sistema oggetto di negoziazione, le garanzie offerte dal fornitore, le responsabilità dell'utilizzatore e i meccanismi di gestione degli eventuali incidenti o malfunzionamenti.

In questo modo, il diritto non cerca tanto di eliminare l'incertezza intrinseca della tecnologia, quanto piuttosto di governarla e distribuirne i rischi in modo consapevole.

Un'applicazione di tale logica si rinviene nel segmento del *legal-tech*, ambito in cui si è progressivamente affermata una pluralità di piattaforme di IA dedicate al supporto della ricerca giuridica, dell'analisi documentale e della redazione di atti, fra le quali, a livello internazionale, Harvey AI, CoCounsel (Casetext, oggi Thomson Reuters) e Lexis+ AI di LexisNexis. A titolo esemplificativo si può considerare, nel contesto italiano, Lexroom AI[5], piattaforma di Intelligenza Artificiale progettata per supportare avvocati e team legali nella ricerca giuridica, nell'analisi documentale e nella redazione di atti.

Secondo le informazioni pubbliche e le condizioni contrattuali della piattaforma (*Lexroom Terms and Conditions*)[6], i risultati generati dall'IA sono accompagnati da fonti normative e giurisprudenziali verificabili, consentendo agli utenti di controllare la correttezza delle informazioni prodotte. Tale approccio riduce il rischio di affidamento cieco sull'IA e assegna all'utente professionale la responsabilità finale della revisione e dell'utilizzo dell'*output*.

Inoltre, il modello contrattuale di Lexroom prevede che il

servizio sia destinato esclusivamente a professionisti qualificati, come avvocati o dipartimenti legali aziendali, che dispongano delle competenze necessarie per interpretare e verificare le informazioni generate. Gli *output* sono concepiti come strumenti di supporto o bozze preliminari, che richiedono una revisione da parte dell'utente prima dell'utilizzo. Tali accorgimenti non eliminano l'incertezza intrinseca del sistema, ma contribuiscono a renderla gestibile attraverso una combinazione di misure tecnologiche, organizzative e contrattuali.

Dal punto di vista giuridico, l'esperienza di Lexroom evidenzia come la responsabilità per l'uso dei sistemi di IA venga ripartita tra fornitore e utente in modo coerente con le rispettive sfere di controllo e con lo scopo di utilizzo: il fornitore si impegna a garantire il corretto funzionamento della piattaforma e la qualità delle fonti integrate nel sistema, mentre l'utente mantiene la responsabilità della verifica finale dei contenuti e della loro applicazione nel contesto professionale.

In questa prospettiva, il contratto assume una funzione di integrazione della disciplina normativa, consentendo di adattare la gestione del rischio alle specificità del singolo rapporto contrattuale.

Questa esigenza emerge con particolare evidenza anche nella gestione dei rapporti lungo l'intera *supply chain* dei sistemi di Intelligenza Artificiale.

In tale contesto, la negoziazione contrattuale assume un ruolo centrale attraverso clausole relative a dichiarazioni e garanzie, manleve, obblighi di collaborazione e assistenza, nonché meccanismi di gestione degli incidenti e di condivisione delle informazioni, nel rispetto dei limiti normativi[7].

Accanto a tali profili, particolare rilievo assume anche

l’individuazione del soggetto che debba assumere il ruolo di “fornitore” ai sensi dell’AI Act, con i relativi obblighi lui attribuiti. In contesti caratterizzati da una pluralità di attori, come nel caso di sistemi sviluppati da una *software house* su incarico di un’impresa committente, la determinazione della qualifica di fornitore può richiedere una valutazione più articolata, che tenga conto delle concrete modalità di sviluppo, distribuzione e utilizzo del sistema[8].

Proprio per questo motivo, il contratto assume una funzione particolarmente rilevante nel chiarire e specificare la ripartizione delle responsabilità tra i diversi soggetti coinvolti.

Un ulteriore elemento che conferma il ruolo integrativo del contratto emerge dall’art. 25, par. 1, lett. a), dell’AI Act, secondo cui il *deployer* che apponga il proprio nome o marchio a un sistema di AI assume la qualifica di fornitore, “fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi”: tale previsione riconosce espressamente lo spazio della negoziazione contrattuale come strumento idoneo a modulare la distribuzione delle responsabilità tra i soggetti coinvolti, nel rispetto del quadro normativo europeo.

In questa prospettiva, la contrattualizzazione non rappresenta un elemento di tensione rispetto al quadro normativo europeo, ma piuttosto uno strumento ausiliario e complementare alla disciplina previste dall’AI Act, NIS2 e, in generale, alle politiche europee di gestione del rischio tecnologico, che consente di tradurre nella pratica operativa i principi di gestione del rischio, trasparenza e responsabilità promossi dalle normative.

La dimensione negoziale diventa così il luogo in cui le indicazioni generali della normativa vengono adattate alle specificità dei singoli rapporti economici e tecnologici, contribuendo a rendere effettiva e concretamente applicabile

la *governance* dei sistemi di Intelligenza Artificiale.

Clausole contrattuali potenzialmente orientate alla gestione dell'imprevedibilità

Dall'analisi precedente si è visto come, generalmente, nei contratti relativi a servizi basati su Intelligenza Artificiale si riscontrino disposizioni che limitano la responsabilità del fornitore in relazione a risultati inesatti o incompleti generati dal sistema, nonché clausole che escludono garanzie implicite circa l'assoluta correttezza degli *output*. Tali pattuizioni, purché non si traducano in un grave squilibrio tra i contraenti, non risultano in contrasto con l'impianto dell'AI Act, il quale non pretende di garantire l'infallibilità dei sistemi, ma piuttosto impone obblighi di gestione del rischio, trasparenza e *accountability*.

In questo senso, il contratto deve consentire di tradurre tali obblighi in una disciplina operativa dei rapporti tra le parti, prevenendo situazioni di incertezza e potenziali contenziosi derivanti dall'utilizzo improprio o non conforme dei sistemi di IA.

Un ulteriore profilo rilevante riguarda la verificabilità delle informazioni e delle fonti utilizzate dal sistema. Alcune piattaforme di Intelligenza Artificiale progettate per ambiti professionali specifici adottano soluzioni che consentono agli utenti di controllare direttamente le fonti su cui si basano gli *output* generati.

Su questa linea si collocano, secondo quanto dichiarato dalle stesse imprese fornitrici, anche le piattaforme già richiamate nel *legal-tech* – fra cui, in Italia, Lexroom AI – che presentano l'affidabilità e la trasparenza delle risposte prodotte dal sistema come elementi qualificanti del proprio posizionamento di mercato.

In particolare, l'*output* generato dal sistema è accompagnato da riferimenti normativi e giurisprudenziali verificabili, che l'utente può consultare per accertare la correttezza delle informazioni. Il sistema non fornisce quindi soltanto una risposta, ma rende accessibili anche le basi giuridiche su cui tale risposta è costruita.

La promessa di risultati "verificati, citabili e trasparenti", evidenziata nelle informazioni pubbliche della piattaforma, non può e non deve tuttavia essere interpretata come una garanzia assoluta di correttezza dell'*output*.

Piuttosto, essa rappresenta il risultato di una serie di strategie tecniche e organizzative finalizzate a ridurre il rischio di errore. Tra queste rientrano l'utilizzo di *dataset* giuridici specializzati, l'integrazione con banche dati normative e giurisprudenziali e la possibilità per l'utente di verificare direttamente le fonti citate dal sistema. Tali soluzioni consentono di mitigare, senza pretendere di eliminarla completamente, l'incertezza intrinseca dei modelli di Intelligenza Artificiale generativa, prevedendo contrattualmente una verifica "umana" dell'*output* da parte dell'utilizzatore.

Ne deriva che anche nel caso di sistemi verticali e altamente specializzati, come quelli sviluppati nel settore *legal tech*, permane una dimensione di rischio legata alla natura probabilistica del funzionamento dei modelli che la regolazione normativa, da sola, difficilmente può controllare, rendendo necessario il ricorso a strumenti negoziali di gestione del rischio.

Una simile impostazione, tra l'altro, traduce sul piano contrattuale e operativo i principi di trasparenza e tracciabilità promossi dall'AI Act e contribuisce, in linea con la logica preventiva della direttiva NIS2, a rafforzare la gestione del rischio nell'impiego dei sistemi digitali.

Tale approccio, ben specificato nelle condizioni contrattuali, valorizza l'utilizzo del sistema di IA come strumento di supporto decisionale e non di sostituzione, mantenendo centrale il ruolo del professionista nella valutazione finale delle informazioni prodotte.

Di conseguenza, ciò diviene rilevante anche per la gestione dei rapporti lungo la *supply chain*. In questo contesto, il contratto può svolgere, infatti, una funzione essenziale nel disciplinare i rapporti tra i diversi attori della filiera, prevedendo, ad esempio, dichiarazioni e garanzie relative alla qualità dei dati utilizzati per l'addestramento, obblighi di collaborazione e assistenza tecnica, nonché meccanismi di manleva o di ripartizione delle responsabilità in caso di malfunzionamenti o incidenti.

Accanto a tali disposizioni, i contratti possono prevedere dichiarazioni e garanzie rese dall'utilizzatore, attraverso le quali quest'ultimo attesti di possedere le competenze tecniche e organizzative necessarie per utilizzare il sistema nel rispetto delle istruzioni fornite. Tali dichiarazioni possono riguardare, ad esempio, il livello di alfabetizzazione digitale dell'utente, la disponibilità di adeguati sistemi di controllo interno o, appunto, la capacità di verificare gli *output* generati dall'Intelligenza Artificiale prima del loro utilizzo. L'obiettivo di tali clausole non è tanto quello di trasferire integralmente il rischio sull'utilizzatore, quanto piuttosto quello di garantire che il sistema venga impiegato in condizioni coerenti con le finalità e i limiti per cui è stato progettato.

Un ulteriore ambito di rilievo riguarda le clausole relative alla manutenzione, agli aggiornamenti e alla sicurezza dei sistemi. In particolare, i contratti possono prevedere obblighi specifici in capo al fornitore relativi alla manutenzione della piattaforma, alla correzione di eventuali vulnerabilità e all'aggiornamento periodico dei modelli e delle basi dati utilizzate dal sistema.

Tali disposizioni risultano coerenti non solo con la logica preventiva dell'AI Act, ma anche con le prescrizioni della Direttiva NIS2 in materia di gestione del rischio informatico e di sicurezza delle infrastrutture digitali. In questo ambito, il contratto può disciplinare aspetti quali gli standard di sicurezza adottati (es. crittografia AES-256, certificazioni ISO 27001, ISO 22301), le procedure di *backup* e *disaster recovery*, nonché i tempi di notifica in caso di incidenti o violazioni dei dati[9].

Particolare attenzione può essere dedicata anche alla disciplina della proprietà intellettuale, dell'utilizzo dei dati e degli eventuali indennizzi derivanti da violazioni contrattuali. La definizione chiara ed esaustiva di tali profili dei diritti tutelati contribuisce indubbiamente a ridurre l'incertezza giuridica connessa all'utilizzo di sistemi di IA e a prevenire possibili controversie tra le parti, rafforzando al contempo i principi di responsabilizzazione e prevenzione che caratterizzano la regolazione europea del settore.

Accanto a questi strumenti contrattuali, un ulteriore meccanismo di gestione del rischio può essere rappresentato dall'inserimento di una polizza assicurativa accessoria al contratto, destinata a coprire i danni eventualmente derivanti da malfunzionamenti del sistema, da errori negli *output* generati dall'IA o da violazioni involontarie di obblighi normativi.

La polizza può prevedere specifici massimali di indennizzo, eventuali franchigie o esclusioni e condizioni per l'attivazione della copertura, contribuendo a distribuire in modo più equilibrato il rischio tra i diversi soggetti coinvolti nel rapporto contrattuale.

Negli ultimi anni, numerose imprese stanno infatti valutando, insieme ai propri *broker* assicurativi, se i rischi derivanti dall'utilizzo dei sistemi di Intelligenza Artificiale possano

essere ricompresi nelle coperture assicurative già esistenti – quali le polizze di responsabilità civile professionale o le assicurazioni *cyber* – oppure se sia necessario sviluppare nuovi strumenti assicurativi specificamente dedicati a tali tecnologie.

La valutazione del rischio rappresenta, del resto, un elemento centrale nel contratto di assicurazione: affinché un rischio possa essere assicurato, è necessario che esso sia almeno in parte prevedibile e valutabile in termini di frequenza e gravità. Nel caso dell'Intelligenza Artificiale, tuttavia, la natura evolutiva dei sistemi e la rapida trasformazione delle tecnologie potrebbero rendere la valutazione del rischio particolarmente complessa, imponendo un continuo adattamento delle soluzioni assicurative disponibili[10].

Le prime soluzioni attualmente presenti sul mercato tendono quindi ad adattare le coperture assicurative esistenti alle nuove sfide, ad esempio attraverso l'introduzione di specifiche esclusioni, franchigie dedicate o limiti di copertura mirati. In prospettiva, è possibile che il progressivo sviluppo di queste tecnologie e una maggiore conoscenza dei rischi associati al loro utilizzo consentano di elaborare strumenti assicurativi sempre più adeguati alle esigenze degli operatori.

Per rendere più concreto il quadro sinora delineato, è utile riportare a titolo esemplificativo un'ipotesi di clausola contrattuale che mostra come gli obblighi di conformità e di sicurezza previsti dall'AI Act e dalla direttiva NIS2 possano essere tradotti in disposizioni operative.

Il contratto potrebbe ad esempio contenere la dicitura: "*Le Parti riconoscono che il Sistema di Intelligenza Artificiale oggetto del presente contratto opera sulla base di modelli di apprendimento automatico caratterizzati da componenti probabilistiche e, pertanto, può generare* output *non integralmente prevedibili né riproducibili.*

Tale caratteristica non costituisce, di per sé, vizio o difetto del servizio, purché il Fornitore mantenga un sistema di controllo, aggiornamento e logging *conforme agli standard tecnici applicabili, al Regolamento (UE) 2024/1689 (AI Act) e, in particolare, agli articoli 9, 17 e 19 dello stesso.*

L'Utente si impegna a utilizzare gli output *generati esclusivamente come supporto decisionale, garantendo che ogni decisione finale sia oggetto di validazione da parte di un soggetto umano dotato delle competenze necessarie per interpretare e verificare i risultati prodotti.*

Il Fornitore, da parte sua, si impegna a rendere disponibili le informazioni tecniche essenziali sul funzionamento del sistema e sui rischi d'impiego, in modo da consentire tale supervisione.

Il Fornitore si impegna altresì a rispettare gli obblighi di sicurezza della supply chain *previsti dalla Direttiva (UE) 2022/2555 (NIS2) ed eventuali normative di ricevimento, assicurando che i propri subfornitori adottino misure di cybersicurezza equivalenti e siano soggetti a verifiche periodiche.*

L'Utente si obbliga a utilizzare il Sistema in conformità alle istruzioni d'uso, garantendo supervisione umana qualificata e qualità dei dati di input*, nonché a sospendere immediatamente l'utilizzo in caso di rischio per la salute, la sicurezza o i diritti fondamentali.*

In caso di incidente di sicurezza o malfunzionamento, il Fornitore dovrà notificare tempestivamente l'Utente e le autorità competenti (CSIRT/ACN), collaborando alla gestione dell'incidente.

Le Parti concordano che:

– i danni derivanti da difetti di progettazione, addestramento o conformità normativa del Sistema saranno imputabili al

Fornitore;

– i danni derivanti da uso improprio, mancata supervisione o alterazioni sostanziali del Sistema saranno imputabili all'Utente, che assumerà la qualifica di Fornitore ai sensi dell'art. 25 AI Act.

Resta inteso che eventuali violazioni degli obblighi di sicurezza della supply chain *(NIS2) da parte di subfornitori saranno imputabili al Fornitore, salvo che l'Utente abbia selezionato direttamente tali soggetti.*

Le Parti cooperano nella tracciabilità e nella documentazione degli eventi, ai fini di eventuali indennizzi o coperture assicurative.

Le Parti convengono che il rischio residuo legato a eventi imprevedibili e non imputabili a violazione contrattuale sia coperto da apposita polizza assicurativa, il cui massimale e condizioni sono indicati nell'Allegato tecnico al presente contratto".

Nel complesso, l'insieme delle clausole contrattuali dimostra come il contratto possa svolgere una funzione essenziale di traduzione operativa dei principi stabiliti dalla normativa europea.

I limiti della contrattualizzazione: clausole vessatorie, squilibrio negoziale e necessità di standard minimi

L'analisi delle clausole virtuose svolta nel paragrafo precedente non può prescindere da una constatazione già emersa nel Capitolo II: la prassi contrattuale dei principali fornitori di servizi di IA si discosta sensibilmente dal modello di equilibrio negoziale che la regolazione europea presuppone. I contratti dei *big tech*, predisposti unilateralmente e proposti in via prevalentemente

standardizzata, concentrano sull'utente finale una quota molto significativa del rischio decisionale, applicativo e risarcitorio.

Vi concorre una combinazione ricorrente di esclusioni di garanzia, limitazioni quantitative della responsabilità, manleve a senso unico, clausole di modifica unilaterale e facoltà di sospensione del servizio in capo al fornitore.

La «contrattualizzazione» rischia, in tale contesto, di tradursi non in una distribuzione condivisa della responsabilità, ma in una traslazione integrale verso il contraente debole.

Il quadro così delineato solleva interrogativi rilevanti sotto il profilo della disciplina delle clausole vessatorie. Nei rapporti *business-to-consumer* si applica la Direttiva 93/13/CEE[11], recepita in Italia agli artt. 33 ss. del Codice del consumo (D.Lgs. 6 settembre 2005, n. 206) [12], che presume vessatorie le clausole le quali, malgrado la buona fede, determinino un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto.

Più nel dettaglio, l'art. 33, comma 2, qualifica come presuntivamente vessatorie, fra le altre, le pattuizioni che escludono o limitano la responsabilità del professionista in caso di morte o danno alla persona derivante da un suo fatto o da una sua omissione (lett. a), che limitano le azioni in caso di inadempimento totale o parziale (lett. b), che riservano al solo professionista la facoltà di recedere o di modificare unilateralmente le condizioni contrattuali (lett. e ed m) e che limitano la responsabilità per inadempimento delle obbligazioni accessorie. Tali clausole, ai sensi dell'art. 36 Cod. cons., sono nulle quando non abbiano formato oggetto di trattativa individuale; la nullità opera anche di ufficio nell'interesse esclusivo del consumatore.

Diverse pattuizioni rinvenibili nei Termini di OpenAI,

Microsoft e Google, esaminate nel Capitolo II, presentano profili di tensione con tale disciplina. La formula «*as is and as available*», unita a tetti risarcitori molto contenuti (frequentemente parametrati al corrispettivo versato negli ultimi dodici mesi) e all'esclusione integrale dei danni indiretti, consequenziali, reputazionali e di lucro cessante, si colloca al limite estremo dello spazio negoziale consentito al professionista. Analoghe perplessità destano le clausole di modifica unilaterale dei termini, le facoltà di sospensione del servizio *ad nutum* e le manleve generali a carico dell'utente, che in concreto possono integrare ipotesi di vessatorietà presunta.

La piena valutazione della loro validità andrà condotta caso per caso, alla luce dell'effettiva trattativa individuale (di norma assente nei piani *consumer*) e della giurisprudenza europea di legittimità in materia di squilibrio significativo.

A rafforzare la cornice di tutela intervengono le Direttive (UE) 2019/770 e 2019/771[13], in materia rispettivamente di contratti di fornitura di contenuti e servizi digitali e di vendita di beni con elementi digitali. Le due fonti, recepite nel Codice del consumo agli artt. 135-*octies* ss. e 128 ss., introducono garanzie di conformità soggettiva e oggettiva, obblighi di aggiornamento e specifici rimedi a tutela del consumatore digitale. La disciplina si applica anche ai servizi di IA generativa erogati in modalità SaaS, e con essa le clausole standard analizzate non sempre risultano pienamente compatibili.

Nei rapporti *business-to-business* l'apparato di tutela è meno strutturato ma non assente. Vengono in rilievo, in particolare, il divieto di abuso di dipendenza economica di cui all'art. 9 della legge 18 giugno 1998, n. 192, applicabile per estensione giurisprudenziale ai rapporti di fornitura digitale segnati da forte asimmetria contrattuale, e il Regolamento (UE) 2022/1925 (*Digital Markets Act*)[14], che nei confronti dei *gatekeeper* impone obblighi di equità nelle

condizioni d’uso.

A livello europeo è inoltre in corso una riflessione sull’opportunità di introdurre una disciplina armonizzata delle clausole abusive nei contratti B2B nel mercato dei servizi digitali, sull’esempio di quanto già previsto dal Regolamento (UE) 2019/1150 in materia di servizi di intermediazione *online*.

In tale prospettiva, la funzione integrativa del contratto rispetto al quadro AI Act-NIS2 non può essere accolta acriticamente. Nei rapporti caratterizzati da forte squilibrio l’autonomia negoziale rischia di ridursi a mera adesione a condizioni predisposte, con effetti potenzialmente regressivi rispetto agli obiettivi di responsabilizzazione e tutela perseguiti dal Legislatore europeo.

La «contrattualizzazione virtuosa» descritta nei paragrafi precedenti presuppone, infatti, una capacità negoziale effettiva tra le parti, di norma riscontrabile soltanto nei contratti *enterprise* o nei rapporti negoziati individualmente, ben difficilmente nei piani *consumer* o nelle micro e piccole imprese.

Si profila dunque, sul piano sistematico, l’esigenza di affiancare alla libera negoziazione strumenti di standardizzazione e di riequilibrio idonei a tradurre i principi di gestione del rischio in clausole minime non derogabili. In tale direzione si possono ipotizzare quattro soluzioni concorrenti.

La prima è il ricorso ai codici di condotta volontari previsti dall’art. 95 dell’AI Act, che possono includere modelli di clausole per la traslazione equilibrata del rischio.

La seconda è l’elaborazione, da parte di autorità nazionali ed europee, di clausole contrattuali tipo, sull’esempio delle *Standard Contractual Clauses* adottate dalla Commissione europea ai sensi dell’art. 46 del Regolamento (UE) 2016/679

per i trasferimenti internazionali di dati, e di quelle predisposte dall'Unione europea per gli appalti pubblici di soluzioni di IA (*EU Model Contractual AI Clauses*, 2023).

La terza consiste nell'adozione di linee guida AgID e di modelli operativi per la Pubblica Amministrazione, idonei a fissare uno *standard* contrattuale di riferimento nei rapporti con i fornitori tecnologici. La quarta, infine, prevede un intervento legislativo settoriale, di matrice nazionale o europea, volto a tipizzare alcune clausole abusive nei contratti di fornitura di servizi di IA, in coerenza con la *ratio* di protezione del contraente debole già accolta dal Codice del consumo.

In un assetto così rinnovato il contratto manterrebbe la propria funzione di adattamento operativo ai singoli contesti, ma all'interno di un perimetro di standard minimi inderogabili. Solo a queste condizioni potrà evitarsi che, nei rapporti tra fornitori di IA e utenti, la prassi negoziale riproponga logiche di traslazione integrale del rischio incompatibili con il quadro europeo di responsabilizzazione multilivello.

Prospettive evolutive e considerazioni conclusive

L'analisi svolta nei paragrafi precedenti evidenzia come la disciplina dei sistemi di Intelligenza Artificiale si collochi all'interno di un contesto normativo in rapida evoluzione, nel quale il Legislatore europeo ha progressivamente cercato di sviluppare strumenti volti a garantire un elevato livello di sicurezza, trasparenza e responsabilità nell'utilizzo delle nuove tecnologie. Come si è visto, l'AI Act rappresenta il primo tentativo organico di regolamentare l'Intelligenza Artificiale secondo un approccio basato sul rischio, mentre la direttiva NIS2 rafforza il quadro di sicurezza delle infrastrutture digitali e dei servizi essenziali.

Tuttavia, si è constatato che la complessità tecnica dei sistemi di IA e la pluralità di soggetti coinvolti nella loro progettazione, sviluppo e utilizzo rendono difficile per la sola normativa pubblica disciplinare in modo esaustivo tutte le possibili configurazioni operative di tali tecnologie. I modelli di IA, si caratterizzano per un funzionamento dinamico ed evolutivo, che può generare risultati non pienamente prevedibili e che si inserisce spesso all'interno di ecosistemi tecnologici articolati, composti da diversi attori e livelli della *supply chain.*

In questo scenario, dall'analisi svolta è emerso con chiarezza che il ruolo del diritto non può limitarsi alla definizione di obblighi generali e di principi regolatori, ma deve necessariamente confrontarsi con l'esigenza di garantire strumenti applicativi in grado di adattarsi alla varietà dei contesti operativi in cui i sistemi di IA vengono impiegati.

È in questa prospettiva che emerge la funzione integrativa del contratto, quale strumento capace di tradurre i principi della regolazione europea in soluzioni operative calibrate sulle specifiche caratteristiche dei rapporti tra gli operatori economici.

La contrattualizzazione consente di adattare la distribuzione delle responsabilità alle concrete modalità di sviluppo, distribuzione e utilizzo dei sistemi di Intelligenza Artificiale, tenendo conto delle diverse posizioni dei soggetti coinvolti nella filiera tecnologica. In questo modo, il contratto contribuisce a rendere effettiva la *governance* del rischio prevista dal Legislatore europeo, permettendo di coordinare obblighi, controlli e meccanismi di cooperazione tra i diversi attori del sistema.

Da questa prospettiva, la relazione tra normativa pubblica e autonomia negoziale non deve essere interpretata in termini di contrapposizione, ma piuttosto come un rapporto di complementarità. Mentre la regolazione europea stabilisce gli

standard minimi di sicurezza, trasparenza e responsabilità cui devono conformarsi i sistemi di IA, il contratto consente di declinare tali principi in modo flessibile e adattabile alle specificità delle diverse applicazioni tecnologiche e dei contesti organizzativi in cui esse vengono implementate.

Guardando alle possibili evoluzioni future, è verosimile che il ruolo della contrattualizzazione nella disciplina dei sistemi di Intelligenza Artificiale sia destinato a rafforzarsi ulteriormente. La crescente diffusione di modelli di IA in settori strategici dell'economia e della Pubblica Amministrazione comporterà infatti un progressivo consolidamento di prassi contrattuali specializzate, capaci di affrontare in modo sempre più sofisticato le questioni relative alla gestione del rischio tecnologico, alla sicurezza dei sistemi e alla ripartizione delle responsabilità lungo la filiera digitale.

Parallelamente, anche il quadro normativo europeo potrebbe evolversi verso forme sempre più integrate di *governance* tecnologica, nelle quali la regolazione pubblica continui a definire principi e standard di riferimento, lasciando tuttavia spazio a strumenti flessibili di attuazione, tra cui la contrattazione tra gli operatori economici e l'adozione di modelli organizzativi e di *compliance* interni alle imprese.

In questa prospettiva, la normativa potrebbe progressivamente orientarsi non tanto verso una disciplina rigida e dettagliata delle singole clausole contrattuali, quanto piuttosto verso la definizione di principi guida e requisiti minimi relativi alla gestione del rischio, alla trasparenza e alla ripartizione delle responsabilità nei rapporti contrattuali relativi ai sistemi di IA, improntati al rispetto della disciplina consumeristica e all'equilibrio tra i contraenti.

Un simile approccio consentirebbe di valorizzare il ruolo dell'autonomia negoziale senza irrigidire eccessivamente una materia caratterizzata da una forte evoluzione tecnologica.

Il Legislatore potrebbe, ad esempio, individuare alcune aree nelle quali favorire la standardizzazione di prassi contrattuali o la predisposizione di modelli di riferimento e, parallelamente, quelle che invece necessitano di maggiore flessibilità negli accordi, lasciando alle parti un margine di adattamento alle specificità dei singoli contesti applicativi e delle diverse filiere tecnologiche. Oppure, ancora, paventare l'ipotesi di istituire una polizza assicurativa obbligatoria per i sistemi maggiormente complessi, come misura a tutela del rischio imprevedibile.

In conclusione, l'analisi dei modelli normativi e contrattuali applicabili ai sistemi di IA evidenzia come la gestione dei rischi connessi a tali tecnologie non possa certamente essere affidata esclusivamente alla regolazione legislativa. Piuttosto, essa richiede un approccio su più piani, nel quale norme pubbliche, strumenti contrattuali e misure organizzative cooperino nel costruire un sistema di *governance* capace di coniugare innovazione tecnologica e tutela degli interessi giuridici coinvolti.

L'analisi evidenzia come la crescente diffusione dei sistemi di Intelligenza Artificiale metta in crisi i tradizionali modelli di imputazione della responsabilità giuridica, a causa della non prevedibilità degli output e della natura opaca di molti sistemi avanzati. Il quadro europeo, articolato tra AI Act, NIS2 e disciplina sulla responsabilità da prodotto, rafforza gli strumenti di prevenzione e gestione del rischio, ma non sempre consente una chiara allocazione ex post delle responsabilità.

In questo spazio di incertezza si colloca il ruolo del contratto, inteso come strumento flessibile di distribuzione del rischio e di integrazione della regolazione pubblica lungo la filiera dell'IA. Il contributo costituisce la base di riflessione del white paper "Contrattualizzazione e allocazione delle responsabilità nei modelli di IA: AI Act, NIS2 e profili critici" di Chiara De Filippo, al quale si

rinvia per un approfondimento sistematico.

Fonti:

[1] Longo A., Masi G., *LLM, cosa sono: tutto ciò che bisogna sapere sui large language models*, in *Agenda Digitale*, 2025: "I Large language models sono modelli di deep learning estremamente complessi, basati su reti neurali con miliardi di parametri, progettati per comprendere, interpretare e generare linguaggio naturale in forma scritta. Il loro funzionamento si basa sull'addestramento su vastissimi corpora di testi eterogenei – libri, articoli accademici, siti web, contenuti social, conversazioni online – che consente di cogliere e modellare con efficacia le strutture sintattiche, semantiche, lessicali e pragmatiche della lingua umana in tutte le sue sfumature", consultabile al sito: *https://www.agendadigitale.eu.*

[2] Lusardi G., *Assicurare l'imprevedibile: le polizze per il rischio di IA*, in *Diritto al Digitale*, 20 maggio 2024, consultabile al sito: *https://dirittoaldigitale.com*.

[3] *https://www.nist.gov/itl/ai-risk-management-framework*.

[4]*Responsabilità dei sistemi AI e decisioni automatizzate: il nuovo paradigma giuridico dell'era algoritmica*, in *ICT Security Magazine*, 27 gennaio 2026, consultabile al sito: *https://www.ictsecuritymagazine.com.*

[5] *https://lexroom.ai*.

[6] *https://lexroom.ai/terms-and-conditions.*

[7] Franchi A., *Riflessioni sulla manleva*, in *Contratto e impresa*, 1, 2017, 155.

[8] Fedi A., *Tre osservazioni sull'AI Act e il suo rapporto con il diritto dei contratti*, in *MediaLaws*, 3/2024, 284 ss.

[9] *Contratti SaaS: guida legale a SLA, dati e aggiornamenti*

(2025), *op. cit*.

[10] Lusardi G., *op.cit*.

[11] Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori. Consultabile al sito: *https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex%3A31993L0013.*

[12] Codice del consumo, D.Lgs. 6 settembre 2005, n. 206, artt. 33-37 e 128 ss.

[13] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019. Consultabile al sito: *https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32019L0770.*

[14] Regolamento (UE) 2022/1925 (*Digital Markets Act*), consultabile al sito: *https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.*

https://www.ictsecuritymagazine.com/articoli/sistemi-di-ia/

Perché Trump non ascolta gli allarmi di Anthropic e OpenAI? Gli interessa solo la supremazia dell’AI sulla Cina

L’allarme dei ricercatori di Cambridge: i modelli AI offrono grandi vantaggi, ma rappresentano anche grandi rischi, siamo capaci di gestire l’esplosione di questa superintelligenza?

L’intelligenza artificiale (AI) potrebbe essere vicina a una soglia molto diversa dai precedenti salti tecnologici: non soltanto macchine più potenti, ma sistemi capaci di partecipare direttamente alla ricerca che produce la generazione successiva di AI. Un circuito nel quale modelli Ai sempre più avanzati contribuiscono a costruire intelligenze artificiali sempre più sofisticate ed efficienti, accelerando ulteriormente il processo.

È lo scenario dell’“***intelligence explosion***” analizzato nel **nuovo paper** pubblicato dalle pagine del Cambridge Programme on AI Science & Policy (Casp) dal titolo “*What if automating AI R&D triggers an intelligence explosion?*”, frutto di una collaborazione tra accademici, ricercatori delle principali aziende di AI ed esperti indipendenti. Tra gli autori figurano **Jakub Pachocki**, chief scientist di OpenAI, **Jack Clark**, cofondatore di Anthropic, **Eric Horvitz**, chief scientific officer di Microsoft, **Dawn Song**, vp AI research di Meta, oltre ai pionieri dell’AI **Geoffrey Hinton, Yoshua Bengio** e **Andrew Barto**.

Il messaggio è rivolto soprattutto ai governi, con l’invito a prepararsi “*prima che la velocità dello sviluppo tecnologico renda molto più difficile intervenire*”. Il documento non sostiene che l’esplosione di intelligenza sia inevitabile, o assolutamente negativa o pericolosa. Sostiene però che esistono abbastanza segnali da rendere necessario prenderla

seriamente in considerazione e quindi catalogarla come “critica” e da gestire come tale.

DONALD TRUMP, PRESIDENTE USA, e XI JINPING, PRESIDENTE REPUBBLICA POPOLARE CINESE

Trump però resta sordo a questi allarmi: la priorità è battere la Cina

L’allarme lanciato dai ricercatori nel documento e le posizioni sempre più critiche prese dalle stesse Big Tech, OpenAI e Anthropic in primis, si scontra però con **la linea della Casa Bianca**, che legge lo sviluppo dell’intelligenza

artificiale soprattutto attraverso la competizione strategica con la Cina.

Nel suo intervento all'Assemblea generale dell'ONU, il Presidente degli Stati Uniti, **Donald Trump**, ha respinto qualsiasi tentativo di costruire quello che ha definito uno "schema globalista" per controllare l'AI e ha ridimensionato gli allarmi sui rischi della tecnologia. Il presidente ha ribadito che gli Stati Uniti non intendono "soffocare la crescita" di una tecnologia che, a suo giudizio, potrebbe diventare più importante della Rivoluzione industriale o di internet.

Trump ha anche chiesto di sostituire nei documenti ufficiali americani l'espressione *artificial intelligence* con **"super intelligence"**, trasformando il cambio di lessico in un messaggio politico: "*Chi vince la superintelligenza, vince*", ha affermato, rivendicando il vantaggio statunitense sulla Cina.
Una posizione che aveva già espresso a inizio mese contro la fronda repubblicana (e democratica) avversa ai data center AI: "*Chi non vuole data center sul proprio territorio è destinato a diventare povero*".

È una visione che mette al centro la **leadership tecnologica americana** e considera eventuali vincoli internazionali anche attraverso il loro possibile impatto sulla competizione con Pechino. La distanza con il documento dei ricercatori diventa manifesta e incolmabile soprattutto nelle priorità: mentre il paper chiede strumenti per controllare un'accelerazione potenzialmente destabilizzante, l'amministrazione Trump insiste sulla necessità di preservare il vantaggio degli Stati Uniti nella corsa all'AI.

Quando l'AI comincia a sviluppare

altra AI

Il punto di partenza è già abbastanza concreto. Ad agosto Anthropic dichiarava che i propri sistemi completavano con una supervisione umana di alto livello il **26% del lavoro interno di ricerca e sviluppo sull'AI**, contro appena l'1% cinque mesi prima. OpenAI ha riferito a settembre che i suoi sistemi svolgono abitualmente attività di R&D che richiederebbero giorni di lavoro ai dipendenti.

La dinamica può diventare esponenziale. Oggi la frontiera dell'AI è sviluppata da alcune migliaia di ricercatori, ma un ricercatore digitale può essere copiato, forse 'clonato' a livello digitale, eseguito in parallelo e lavorare continuamente. **Automatizzare il settore ricerca e sviluppo (R&D)** potrebbe quindi equivalere, secondo gli autori, ad aggiungere **milioni di ricercatori virtuali**. Se questi sistemi contribuissero a costruire successori ancora migliori, **il ciclo potrebbe autoalimentarsi**.

È qui che opportunità e rischio diventano difficili da separare. Un'accelerazione del genere, si legge nel documento, potrebbe anticipare scoperte scientifiche, nuovi farmaci, tecnologie energetiche e aumenti della produttività; ma potrebbe anche produrre in tempi brevissimi **capacità cyber e biologiche molto più pericolose,** forti shock sul lavoro e sistemi sui quali gli esseri umani esercitano una supervisione sempre più debole.

C'è poi una questione politica: un vantaggio anche limitato nella corsa all'AI potrebbe trasformarsi rapidamente in un vantaggio difficilmente recuperabile, **alterando gli equilibri tra Stati, aziende e persino tra istituzioni dello stesso Paese**.

Più governance pubblica sulla frontiera dell’AI

Da qui tre richieste ai governi.
La prima è **ottenere maggiore visibilità su ciò che avviene nei laboratori**, attraverso auditor e obblighi di comunicazione sul livello di automazione della ricerca, sulla velocità dei progressi e sull’impiego dell’AI nelle decisioni più delicate.

La seconda è **costruire strumenti capaci di rallentare o interrompere gli esperimenti più rischiosi**: requisiti di sicurezza, limiti alla crescita delle capacità, ambienti isolati dalle reti esterne e accordi internazionali verificabili.

La terza, quella più distopica, a cui forse proprio non riusciamo ad abituarci come pensiero e immagine, riguarda la **preparazione delle società a crisi cyber, biosecurity, instabilità geopolitica**, disruption del lavoro o perdita di controllo sui sistemi più avanzati.

In altre parole, la governance dell'AI di frontiera non può dipendere esclusivamente dalle aziende che competono per costruirla, è necessario che governi e istituzioni democratiche assumano un ruolo chiave (se non guida).

Anthropic: crescita record, ma 42

miliardi di perdite

Nel frattempo, tornando all’attualità, le Big Tech procedono spedite nella corsa all’AI, nonostante intoppi competitivi e oscure strategie.

Ad esempio, **il problema della sicurezza che si intreccia, nel caso di Anthropic, con una corsa industriale dai costi enormi**. Il prospetto per l’IPO, visionato da *Reuters*, fotografa una società che nel 2025 ha registrato **42 miliardi di dollari di perdita netta**, mentre i ricavi sono aumentati di dodici volte fino a circa **4,6 miliardi**. La perdita operativa, depurata principalmente dagli effetti contabili collegati ai precedenti finanziamenti, ha superato gli **8 miliardi**.

Anthropic prevede **518 miliardi di dollari di impegni futuri** per cloud, capacità di calcolo e infrastrutture. Nel solo 2025 la spesa per computing e infrastrutture ha raggiunto 7,33 miliardi. Una possibile quotazione potrebbe attribuire all’azienda una valutazione superiore ai **2 trilioni di dollari**.

Numeri che mostrano un secondo lato della corsa all’AI: più aumenta il capitale necessario per restare alla frontiera, più tecnologia, infrastrutture e potere decisionale rischiano di concentrarsi in pochissimi soggetti.

Lo stesso prospetto Anthropic riconosce inoltre rischi legati alla concentrazione dei clienti e dedica ampio spazio ai potenziali pericoli dell’AI avanzata. È un cortocircuito significativo: le società che raccolgono capitali promettendo capacità sempre maggiori sono anche quelle che avvertono investitori e governi dei rischi prodotti proprio da quelle capacità.

OpenAI ferma GPT-6.1 Astra

L’ultimo caso arriva da **OpenAI**, che ha rinunciato al previsto lancio di ottobre di **GPT-6.1 Astra** dopo che i test interni hanno evidenziato problemi di sicurezza e allineamento. Secondo quanto riportato dal *Wall Street Journal*, il modello mostrava maggiore **propensione all’inganno** rispetto al predecessore e poteva proseguire alcune attività senza richiedere l’autorizzazione prevista, utilizzando anche strumenti esterni in circostanze considerate non sicure.

La decisione è importante proprio perché Astra era stato progettato per affrontare compiti complessi con minore intervento umano.

Il paradosso della frontiera dell’AI emerge così con sempre maggiore chiarezza. Le Big Tech stanno investendo centinaia di miliardi per costruire sistemi più autonomi, mentre alcuni dei loro principali ricercatori chiedono ai governi strumenti capaci di controllare quella stessa accelerazione.
La questione non è soltanto se arriverà una “intelligence explosion”, ma **chi avrà il potere di decidere quando accelerare, quando fermarsi e quali rischi saranno accettabili per il resto della società**.

The post Perché Trump non ascolta gli allarmi di Anthropic e OpenAI? Gli interessa solo la supremazia dell’AI sulla Cina appeared first on Key4biz.

https://www.key4biz.it/perche-trump-non-ascolta-gli-allarmi-di-anthropic-e-openai-gli-interessa-solo-la-supremazia-dellai-sulla-cina/589432/

AI, tre pericoli secondo Lagarde (Bce): “Il boom del debito, la disoccupazione e la dipendenza”

L’audizione della Presidente della Bce Christine Lagarde al Parlamento europeo su AI, rischi e opportunità per l’Ue

L’**intelligenza artificiale** (AI) promette di aumentare la produttività, ridurre i costi e trasformare interi settori dell’economia. Ma dietro la corsa globale agli investimenti sta emergendo un rischio sempre più rilevante per la stabilità finanziaria: valutazioni azionarie concentrate su poche società tecnologiche e un crescente ricorso al debito per finanziare data center, chip e infrastrutture AI.

È il punto più delicato dell’**intervento** della presidente della Banca centrale europea, **Christine Lagarde**, durante l’audizione alla commissione per i problemi economici e monetari del Parlamento europeo.

“*L’attività di investimento nell’AI dipenderà anche dall’andamento dei mercati finanziari e dall’eventuale concretizzarsi dei rischi associati al boom dei finanziamenti nel settore*”, ha avvertito Lagarde, aggiungendo: “*Una brusca revisione delle prospettive delle società di AI e della sostenibilità del loro debito potrebbe innescare correzioni di mercato e ripercuotersi sugli investitori dell’area dell’euro e sull’economia nel suo complesso*”.

Dal boom dell’AI al rischio finanziario

Il problema non riguarda soltanto quanto denaro viene investito nell’intelligenza artificiale, ma come viene finanziata questa espansione. Per anni i maggiori gruppi tecnologici americani hanno potuto sostenere gli investimenti attraverso gli enormi flussi di cassa generati dalle proprie attività.

La dimensione della nuova corsa infrastrutturale sta però modificando questo modello: **gli hyperscaler stanno ricorrendo sempre più ai mercati obbligazionari** e ad altre forme di finanziamento.

La stessa Bce ha recentemente rilevato che **le Big Tech stanno aumentando la loro presenza anche sul mercato obbligazionario dell’area euro**. Questo può accrescere la concentrazione degli investimenti e l’esposizione europea al settore tecnologico statunitense.

Il rischio è un meccanismo a catena. Se le aspettative sui profitti futuri dell’AI venissero ridimensionate, la correzione potrebbe non fermarsi alle azioni tecnologiche. Potrebbe coinvolgere obbligazioni, credito privato e investitori esposti direttamente o indirettamente al boom.

La BCE sottolinea infatti che la combinazione tra forte crescita delle quotazioni azionarie e aumento dell’indebitamento merita particolare attenzione dal punto di vista della stabilità finanziaria.

Europa indietro negli investimenti

Il paradosso è che l’Europa deve contemporaneamente proteggersi dai rischi finanziari dell’AI e investire molto di più nella stessa tecnologia.

Secondo Lagarde, alla fine del 2025 il 38% delle imprese dell'area euro dichiarava almeno un utilizzo moderato dell'intelligenza artificiale, ma appena il 7% ne faceva un uso significativo.

Per colmare il divario con gli Stati Uniti non basta finanziare startup o acquistare software. Servono capacità di calcolo, data center, energia, capitale, formazione dei lavoratori e una trasformazione dei processi aziendali. Le imprese europee stanno aumentando gli investimenti: secondo una recente indagine BCE, il 49% prevede investimenti in tecnologie e strumenti AI, il 46% nella formazione dei dipendenti e il 40% in dati e infrastrutture.

Lagarde richiama quindi iniziative come InvestAI, lo Scaleup Europe Fund e i 30 miliardi di euro destinati alle AI Gigafactories. Ma il nodo strutturale rimane la capacità europea di trasformare ricerca e innovazione in imprese capaci di crescere su scala globale.

AI e lavoro: dipende da come viene utilizzata

La seconda grande incognita riguarda l'occupazione, ha affermato Lagarde: "*oltre la metà dei lavoratori utilizza già strumenti di AI nel proprio lavoro*".

Finora non emerge un effetto generalizzato di distruzione dei posti di lavoro. Anzi, le aziende che utilizzano maggiormente l'AI tendono nella fase di transizione ad assumere di più. Ma la finalità dell'investimento fa la differenza.

"*Le imprese che impiegano l'intelligenza artificiale per ricerca, innovazione e sviluppo di nuovi prodotti tendono ad aumentare l'occupazione; quelle che la adottano principalmente per ridurre il costo del lavoro mostrano invece una maggiore propensione a tagliare personale*", si legge nel testo

pubblicato dalla Bce.

La domanda decisiva, secondo Lagarde, resta quindi aperta: "*L'AI diventerà prevalentemente un complemento del lavoro umano oppure un suo sostituto?*".
Intanto, secondo una nuova ricerca pubblicata da McKinsey, per colpa dell'AI più di **11 milioni di lavoratori americani dovranno cercare un'occupazione diversa** da quella attuale nei prossimi 10 anni.

La strategia europea: innovare, essere indipendenti, utilizzare l'AI

La risposta indicata dalla presidente della Bce poggia infine su tre direttrici: innovazione, indipendenza e diffusione intensiva dell'intelligenza artificiale.

L'Europa deve "*ridurre la frammentazione del mercato unico*", sviluppare "mercati dei capitali più profondi", aumentare la "*disponibilità di energia e capacità di calcolo*" e rafforzare le componenti critiche della filiera tecnologica.

L'obiettivo, precisa Lagarde, "*non è l'autosufficienza*, *ma garantire che le funzioni strategiche possano continuare a operare anche in condizioni avverse*".

La sfida europea assume così una doppia dimensione: Bruxelles deve evitare di restare spettatrice di una rivoluzione tecnologica finanziata e controllata altrove, senza però ignorare che proprio la velocità e la quantità di capitale riversate sull'AI stanno creando "***nuove vulnerabilità***".

Per l'Europa, dunque, investire nell'intelligenza artificiale non basta, ha sottolineato la Presidente della Banca centrale, la questione diventa riuscire a farlo senza trasformare la corsa tecnologica di oggi nel rischio finanziario di domani.

The post AI, tre pericoli secondo Lagarde (Bce): “Il boom del debito, la disoccupazione e la dipendenza” appeared first on Key4biz.

https://www.key4biz.it/ai-tre-pericoli-secondo-lagarde-bce-il-boom-del-debito-la-disoccupazione-e-la-dipendenza/589358/

Trump-Xi, la diplomazia dei chip si ferma alla cena

Vertice alla Casa Bianca tra Donald Trump e Xi Jinping sulla nuova geopolitica dell’AI

Dopo cerimoniali in pompa magna di diverse ore, con tanto di tappetti rossi, soldati in alta uniforme in rappresentanza dei vari corpi militari, passaggio di aerei B-2 e F-22 Raptor, la prima giornata della storica visita di Stato del Presidente della Repubblica popolare cinese, Xi Jinping, negli Stati Uniti si è conclusa con una fastosa cena di gala a Washington.

In queste prime ore è sembrato chiaro che il Presidente degli Stati Uniti, **Donald Trump,** e il Presidente **Xi stiano cercando** una tregua commerciale, pur ribadendo in silenzio che la competizione è inevitabile. Tra le due superpotenze la partita si gioca sempre meno sui dazi e sempre più su **intelligenza artificiale (AI), semiconduttori, capacità di calcolo, materie prime critiche e tecnologie avanzate**.

È questa la fotografia che emerge dal vertice del 24 settembre alla Casa Bianca. Washington e Pechino hanno **esteso di due**

mesi la sospensione di una nuova escalation tariffaria, rinviando al 10 gennaio 2027 la scadenza della tregua. Ma non è emersa una svolta pubblica sui controlli americani all'esportazione delle tecnologie più sensibili verso la Cina.

La diplomazia riapre dunque qualche spazio al commercio mentre la politica industriale continua a separare i due sistemi tecnologici.

XI JINPING PRESIDENTE REPUBBLICA POPOLARE CINESE, DONALD TRUMP PRESIDENTE USA

Sull'AI Trump e Xi aprono il

dialogo: possibili meccanismi di alert comuni in caso di incidenti o crisi

Una delle novità riguarda l'intelligenza artificiale. Stati Uniti e Cina stanno esplorando un confronto sui rischi dell'AI, compresa la possibilità di "***meccanismi di comunicazione in caso di incidenti o crisi***" (*notification mechanism*), già anticipata dal Segretario del Tesoro americano, **Scott Bessent**. I terreni potenziali vanno dagli attacchi informatici all'uso biologico, fino ai rischi per infrastrutture critiche come energia, finanza e trasporti.

Le impostazioni politiche restano però differenti. Trump arriva al vertice dopo aver ribadito all'ONU il rifiuto americano di uno schema globale di controllo dell'intelligenza artificiale, che ha definito anche "**super intelligenza**". Xi insiste invece sulla responsabilità delle grandi potenze nel mantenere l'AI sotto controllo umano e orientarla al benessere delle persone.

"*La super intelligenza sarà un grande tema di discussione, ma voglio lasciarla esattamente dov'è. È anche la posizione della Cina*", aveva dichiarato Trump prima dell'arrivo del Presidente cinese.

"*Abbiamo entrambi la capacità e la responsabilità di sviluppare e gestire l'IA per il bene, e di garantire che lo sviluppo dell'IA sia sempre sotto controllo umano e al servizio del benessere delle persone*", ha dichiarato Xi alla Casa Bianca, secondo varie agenzie stampa internazionali, aggiungendo: "*Deve essere adottato un approccio centrato sulle persone e l'IA deve essere sviluppata in modo positivo e per il bene, così da servire il progresso dell'umanità*".

Per ora non c'è una governance comune, c'è qualcosa di più pragmatico: il tentativo di **evitare che la corsa all'AI**

produca incidenti capaci di trasformare la rivalità tecnologica in una crisi geopolitica.

Il vero confine resta quello dei chip

È sui **semiconduttori** che il riavvicinamento si ferma. Dal vertice non risulta un accordo per riaprire alla Cina **l'accesso ai chip AI più avanzati**, alle apparecchiature necessarie per produrli o alle altre tecnologie di calcolo sottoposte alle restrizioni statunitensi.

Non è un dettaglio, anzi, è il cuore dell'incontro (assieme a Taiwan). I semiconduttori sono diventati contemporaneamente **infrastruttura economica, tecnologia dual use e strumento di politica estera**. Senza GPU, memorie avanzate, software di progettazione, macchinari di fabbricazione e data center non esiste una **leadership nell'intelligenza artificiale**.

Washington cerca un difficile equilibrio commerciare con Pechino senza trasferirle le tecnologie che considera determinanti per il proprio vantaggio strategico, mentre la Cina persegue l'obiettivo opposto e cioè ridurre la dipendenza dall'ecosistema tecnologico occidentale sviluppando semiconduttori, AI e capacità industriali domestiche.

XI JINPING PRESIDENTE REPUBBLICA POPOLARE CINESE, DONALD J. JOHN TRUMP PRESIDENTE USA

Nvidia, OpenAI, Apple e Microsoft: chi sedeva alla cena

A raccontare meglio di qualsiasi comunicato la posta in gioco è stata però la **cena di Stato**. Nella East Room della Casa Bianca sedevano oltre 130 invitati e una parte impressionante dell'infrastruttura privata che sostiene la potenza tecnologica americana.

Tra i numerosi CEO e presidenti, c'erano: **Jensen Huang** di Nvidia, **Lisa Su** di AMD, **Sanjay Mehrotra** di Micron e **Cristiano Amon** di Qualcomm. E poi **Sam Altman** e **Greg Brockman** di OpenAI,

Mark Zuckerberg di Meta, **Satya Nadella** dei Microsoft, **Sundar Pichai** e **Sergey Brin** di Google, **Tim Cook** (ex Ceo di Apple), **Jeff Bezos** di Amazon, **Michael Dell** fondatore di Dell Technologies e **Elon Musk** di SpaceXAI/Tesla.

Accanto alla tecnologia sedeva la finanza: **Jamie Dimon** di JPMorgan, **Larry Fink** di BlackRock, **David Solomon** di Goldman Sachs e **Stephen Schwarzman** di Blackstone. C'era anche tanta industria, automotive, aerospazio e difesa.

La Casa Bianca ha quindi mostrato a Xi non semplicemente le Big Tech, ma un **ecosistema completo di potere economico**: capitale finanziario, chip, cloud, modelli AI, data center, piattaforme, aerospazio e industria.

Non risultano al momento accordi o intese durante la cena, né nuove potenziali voci sull'export, diciamo che la presenza dei CEO va letta soprattutto sul piano politico e industriale.

Materie prime contro capacità di calcolo

La competizione, inoltre, non è a senso unico. Se gli Stati Uniti controllano molti dei nodi più preziosi del software, dell'AI e della progettazione dei semiconduttori, la Cina dispone di leve fondamentali nelle **terre rare, nei minerali critici, nella raffinazione e nella manifattura**. È qui che tecnologia e politica industriale diventano inseparabili.

Per entrambe le potenze l'obiettivo non è più soltanto conquistare quote di mercato. È assicurarsi che, in caso di crisi, il concorrente non possa interrompere l'accesso alle risorse indispensabili alla crescita economica e alla sicurezza nazionale.

I due Paesi devono "*coesistere e cooperare*" come principali potenze globali, evitando la "trappola di Tucidide", la teoria che descrive il rischio di guerra quando una potenza nuova ed

emergente sfida una già dominante. Per questo, dovrebbero esserci più iniziative comuni in ambito commerciale e sulla regolamentazione dell'intelligenza artificiale, mantenendo al contempo un dialogo militare costante.

Non è decoupling, è competizione controllata

Il vertice Trump-Xi, che negli Stati Uniti non è stato accolto proprio benissimo a livello bipartisan al Congresso, molto di più invece tra la gente (sei americani su dieci sono per politica di "cooperazione amichevole e impegno" per la pace), suggerisce quindi una formula diversa dal semplice "decoupling". Stati Uniti e Cina hanno bisogno di continuare a commerciare e hanno interesse a evitare shock incontrollati, ma contemporaneamente stanno costruendo **maggiore autonomia nei settori considerati strategici**.

È una sorta di competizione controllata, almeno in questa fase storica, nella quale dazi, export control, terre rare, investimenti pubblici e politiche industriali diventano parti dello stesso negoziato.

The post Trump-Xi, la diplomazia dei chip si ferma alla cena appeared first on Key4biz.

https://www.key4biz.it/trump-xi-la-diplomazia-dei-chip-si-ferma-alla-cena/589055/

ESA porta l'AI di Mistral

nello Spazio

La Lettera di intenti di ESA e Mistral per l’AI sovrana nello Spazio

L’autonomia strategica europea passa sempre più dall’incrocio tra due tecnologie considerate ormai essenziali: **Spazio e intelligenza artificiale (AI)**. È in questa prospettiva che va letta la nuova intesa tra l’Agenzia spaziale europea (**ESA**) e **Mistral AI**, uno dei principali attori europei impegnati nello sviluppo di modelli avanzati di intelligenza artificiale.

La *Letter of Intent*, annunciata dall’ESA e firmata a Parigi (il 16 settembre) dal direttore generale dell’Agenzia, **Josef Aschbacher**, e dal cofondatore e ceo di Mistral, **Arthur Mensch**, definisce un quadro di cooperazione destinato ad ampliare l’utilizzo dell’AI nelle attività ingegneristiche, scientifiche e operative.

Non si tratta semplicemente di portare nuovi chatbot all’interno dell’Agenzia. Il punto strategico è un altro: verificare come modelli avanzati, infrastrutture cloud e competenze AI europee possano essere integrati in uno dei settori più sensibili per la sicurezza e la competitività del continente, mantenendo sotto controllo dati, infrastrutture e know-how.

Il direttore generale dell’ESA, Josef Aschbacher

L’AI entra nelle attività spaziali europee

L’accordo consentirà alle due organizzazioni di esplorare applicazioni che combinano le capacità di Mistral nei modelli e nelle infrastrutture AI con il patrimonio scientifico, ingegneristico e operativo dell’Agenzia. Gli ambiti individuati comprendono **osservazione della Terra, ingegneria, capacità avanzate di AI applicate allo Spazio e sviluppo di nuove competenze**.

Le applicazioni previste sono molto concrete: facilitare l’accesso alla conoscenza tecnica, automatizzare attività

ripetitive, migliorare i processi ingegneristici e assistere il personale nelle decisioni tecniche. A queste si aggiunge la possibilità di utilizzare l'intelligenza artificiale per elaborare quantità crescenti di informazioni provenienti dai sistemi spaziali.

"*L'intelligenza artificiale sta rapidamente diventando una capacità fondamentale per il futuro dello spazio*", ha spiegato Aschbacher, sottolineando che la cooperazione con Mistral rappresenta un nuovo passo per rafforzare la **leadership tecnologica e la resilienza dell'Europa**.

L'obiettivo, secondo il direttore generale dell'ESA, è sviluppare insieme "*soluzioni AI innovative, sicure e affidabili*" a beneficio non soltanto del settore spaziale, ma più in generale della società europea.

Non si parte da zero: i progetti Orbit ed EVE

La *Letter of Intent* non inaugura da zero il rapporto tra ESA e Mistral. Lo amplia e lo porta su un livello maggiormente strategico. Tra le iniziative già esistenti c'è **Orbit**, assistente AI sicuro destinato a supportare le attività ingegneristiche dell'Agenzia, facilitando l'accesso alla conoscenza e riducendo il peso delle operazioni ripetitive.

C'è poi **EVE, Earth Virtual Expert**, sviluppato attraverso il Φ-lab dell'ESA insieme a partner europei e dedicato all'osservazione della Terra e alle scienze del sistema terrestre.

Il salto previsto dall'intesa è quindi quello dalle singole sperimentazioni verso un quadro più ampio nel quale l'AI possa diventare una tecnologia trasversale alle attività dell'Agenzia.

Il CEO di Mistral AI, Arthur Mensch

Dallo Spazio arrivano i dati, l’AI deve trasformarli in conoscenza

È soprattutto nell’osservazione della Terra che l’integrazione tra spazio e intelligenza artificiale può assumere un peso economico e strategico crescente. L’Europa dispone di un patrimonio enorme di dati satellitari e di programmi come **Copernicus**.

Possedere il dato non è sufficiente e il vantaggio competitivo dipende sempre più dalla capacità di elaborarlo rapidamente, incrociarlo con altre informazioni e trasformarlo in conoscenza utilizzabile da imprese, amministrazioni e

cittadini.

Sistemi AI specializzati possono contribuire ad analizzare immagini satellitari, informazioni meteorologiche, dati ambientali e altre fonti per accelerare l'individuazione di incendi, alluvioni, stress idrico, cambiamenti nell'utilizzo del territorio o criticità che interessano infrastrutture e attività economiche.

La posta in gioco diventa quindi la capacità europea di controllare non soltanto **la raccolta del dato**, ma anche gli strumenti attraverso cui quel dato viene trasformato in servizi e informazioni utilizzabili.

AI sovrana, perché l'accordo è strategico per l'Europa

È qui che la partnership assume un significato che supera i confini del settore spaziale. L'Europa continua infatti a dipendere in misura significativa da tecnologie e operatori extraeuropei lungo diversi segmenti della filiera digitale, dai semiconduttori al cloud fino ai modelli di intelligenza artificiale.

Nello Spazio questa dipendenza assume un peso particolare. Dati satellitari, immagini ad alta risoluzione, telemetria, procedure operative e conoscenza ingegneristica possono avere contemporaneamente **valore economico, industriale e strategico**.

ESA e Mistral intendono per questo valutare anche la possibilità di distribuire le capacità AI interessate dall'accordo su **infrastrutture europee**, introducendo garanzie specifiche in materia di sicurezza, resilienza, tracciabilità, audit e protezione delle informazioni sensibili.

Il concetto di sovranità tecnologica diventa così molto concreto: sapere dove vengono elaborati i dati, quali sistemi vi hanno accesso, poter verificare il comportamento dei

modelli e mantenere il controllo sulle infrastrutture che sostengono applicazioni critiche, come già scritto nel pacchetto europeo per la sovranità tecnologica.

Luna, base, data center, spazio

Spazio e AI diventano infrastrutture critiche

Il tema riguarda direttamente anche la resilienza europea. Sistemi satellitari e intelligenza artificiale stanno assumendo un ruolo crescente nella gestione delle emergenze, nel monitoraggio climatico, nelle telecomunicazioni, nella sicurezza, nella logistica e nella protezione delle infrastrutture energetiche e digitali.

Ridurre le dipendenze tecnologiche in questi settori significa quindi limitare anche l'esposizione dell'Europa a possibili interruzioni dei servizi, perdita di controllo sui dati o dipendenze da piattaforme tecnologiche sottoposte a ordinamenti e interessi esterni all'Unione.

Mistral porta nell'accordo proprio uno degli elementi che Bruxelles considera strategici: la disponibilità di una **filiera europea dell'intelligenza artificiale**, con modelli personalizzabili e possibilità di implementazione adattabili a requisiti di sicurezza e controllo.

"*Combinando lo stack AI personalizzabile e all'avanguardia di Mistral con le nostre competenze di ingegneria industriale, trasformeremo gli straordinari dati dell'ESA in servizi ad alto impatto per l'industria spaziale*", ha dichiarato Mensch, indicando sicurezza, controllo e sovranità come elementi centrali della collaborazione.

Dalla Space economy europea nuovi servizi ad alto valore

La partnership ha infine una dimensione industriale. Una parte crescente del valore della Space economy viene generata attraverso applicazioni e servizi che utilizzano infrastrutture e dati spaziali: agricoltura di precisione, energia, assicurazioni, logistica, monitoraggio ambientale, gestione delle emergenze e sicurezza.

L'integrazione di modelli AI specializzati può accelerare la trasformazione dei dati satellitari in prodotti utilizzabili da imprese e pubbliche amministrazioni, aprendo opportunità per startup, PMI e grandi operatori europei.

Per Mistral, la collaborazione con l'ESA offre contemporaneamente un banco di prova particolarmente avanzato: applicazioni scientifiche e industriali nelle quali

affidabilità, sicurezza e controllo delle informazioni sono requisiti essenziali.

La sovranità digitale europea si gioca anche nello Spazio

La Lettera non rappresenta ancora un programma industriale con investimenti, scadenze e risultati tecnologici predeterminati. È un quadro attraverso il quale ESA e Mistral potranno individuare progetti e applicazioni concrete, ma la direzione politica e industriale è significativa.

La competizione sull’intelligenza artificiale non riguarda più soltanto chi costruisce i modelli più potenti, riguarda anche

chi controlla il cloud sul quale funzionano, i dati che elaborano, le infrastrutture nelle quali vengono integrati e i servizi strategici che da essi dipendono.

Per l’Europa, quindi, collegare una capacità AI sviluppata sul continente a uno dei suoi maggiori patrimoni tecnologici, quello spaziale, significa **provare a costruire una catena del valore più autonoma**.

Dai satelliti ai dati, dai modelli AI alle infrastrutture di calcolo, fino alle applicazioni utilizzate da industria e istituzioni: è lungo questa filiera che la collaborazione ESA-Mistral può diventare qualcosa di più di un accordo tecnologico. **Un nuovo tassello della strategia europea per trasformare l’autonomia digitale da principio politico a capacità industriale concreta.**

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/esa-porta-lai-di-mistral-nello-spazio/588710/