L’illusione del controllo nell’era dell’AI

*Rubrica settimanale **SosTech**, frutto della collaborazione tra **Key4biz** e **SosTariffe**. Per consultare gli articoli precedenti, **clicca qui**..*

Un concetto che si sente ripetere spesso, da qualche anno, è quello di **sovranità digitale**. Ora questo concetto guida una nuova corsa globale agli investimenti nell’intelligenza artificiale, presentata come una forma di emancipazione dalla dipendenza tecnologica verso gli Stati Uniti.

I governi di mezzo mondo (dall’Asia di Giappone e Cina al Medio Oriente, fino all’Europa) stanno costruendo ogni giorno nuovi **data center**, per i quali sono necessari programmi di formazione per le competenze. Vengono messi da parte miliardi per le infrastrutture nazionali, con l’obiettivo dichiarato di trattenere sul territorio il valore creato dai dati dei cittadini.

Oltre alla sovranità digitale, si parla di **decolonizzazione** (sempre digitale, s’intende), definitacome il processo che permette ai vari Paesi di gestire autonomamente la propria trasformazione digitale invece di esportare dati grezzi per poi riacquistarli sotto forma di servizi di AI forniti da poche corporation americane.

Ma dietro questo scenario che vorrebbe essere di autodeterminazione tecnologica si nasconde un paradosso strutturale: per diventare indipendenti dalle **big tech** statunitensi, gli stati come l’Indonesia, l’India, l’Arabia Saudita o la Francia sono costretti a rivolgersi proprio a **Nvidia**, **Google** e **Amazon** per chip, i server, i servizi cloud,

visto che, come sa chiunque abbia dato un’occhiata al mercato negli ultimi mesi, Nvidia controlla circa il 90% del mercato dei semiconduttori per AI, e AMD e i grandi fornitori di hardware sono americani.

Perfino quando le aziende nazionali promettenti ci sono (come **Mistral** in Francia) la loro crescita è legata a doppio filo alle partnership strategiche con i fornitori statunitensi.

Di chi è davvero la nuvola?

Un contraddizione, è chiaro. Difficile da risolvere. E che diventa ancora più evidente quando entrano in gioco le cosiddette soluzioni di **cloud sovrano**, che sulla carta promettono infrastrutture localizzate e maggior controllo sui dati, tutto grazie a una governance più trasparente; e tuttavia restano comunque vincolate alla giurisdizione americana, visto che il **CLOUD Act** consente alle autorità USA di accedere ai dati detenuti da aziende statunitensi ovunque nel mondo.

Nel frattempo, la complessità contrattuale e la natura proprietaria di molte tecnologie trasformano i progetti pubblici in costose **vetrine per le tecnologie private**, difficili da verificare in modo indipendente ma soprattutto impossibili da sostituire senza affrontare costi enormi.

Per questa ragione, alcuni analisti parlano di “**sovereignty as a service**”: una mera illusione di controllo che maschera un nuovo tipo di dipendenza, meno visibile di quella tradizionale ma potenzialmente più profonda perché radicata nelle infrastrutture digitali essenziali di un paese.

Per gli esperti, la vera sovranità non consiste nel possedere data center perfetti per le brochure ma nella capacità di cambiare fornitore e certificare autonomamente la sicurezza dei sistemi.

Il paradosso dell’indipendenza che alimenta il mercato

Tutto quello che riguarda la tecnologia pubblica ha un’immediata ricaduta sulle strategie commerciali, tenendo conto che il vero asset, la vera posto in gioco, è sempre la stessa, cioè **l’accesso a capacità di calcolo su larga scala**; una risorsa che è distribuita tutt’altro che in modo uniforme, ma che è invece concentrata nelle mani di pochissimi attori privati a livello globale.

Le decisioni politiche sui data center nazionali rischiano di alimentare la polarizzazione del mercato, anche perché bisogna stabilire chi allenerà i nuovi modelli, e le grandi aziende di intelligenza artificiale si fanno concorrenza – oltre che per fornire un prodotto migliore degli altri – per garantirsi **posizioni preferenziali**. Ad esempio per le cruciali catene di approvvigionamento dei chip, ma anche sugli accordi energetici e sul cloud, tutti elementi che nessun Paese può sognarsi di controllare davvero.

Così sono proprio le strategie governative a rischiare di accelerare la stessa competizione che vorrebbero mitigare, e gli stati diventano di fatto finanziatori e acquirenti privilegiati di una bolla sempre più gonfiata e che rischia di esplodere con conseguenze potenzialmente disastrose.

Quando si parla delle aziende che dominano il mercato dell’AI, bisogna sempre più rendersi conto di quanto siano in grado di spostare a livello politico.

Ma il controllo non è in mano nemmeno alle big tech

La pressione competitiva è sempre più insostenibile anche dove si riescono a costruire infrastrutture e a gestire al meglio

la dipendenza tecnologica, perché non va dimenticato che anche le aziende che forniscono chip e servizi cloud ai governi stanno vivendo un momento di **allarme interno**.

Tra gli ultimi allarmi, quello interno ad OpenAI lanciato da Sam Altman, un “codice rosso” per **ChatGPT** che ha imposto di spostare risorse e priorità verso miglioramenti immediati dell’esperienza quotidiana degli utenti, visto che c’è un concorrente che emerge con sempre maggior prepotenza: **Google**, che dopo aver incorporato **Gemini** direttamente nella sua piattaforma di ricerca riesce a offrire a un immenso bacino di utenti una distribuzione quasi istantanea della sua tecnologia.

E c’è pure **Anthropic** con **Claude**, preferito sempre da più persone grazie alle sue spiccate doti in attività complesse come il ragionamento strutturato e il coding.

Non è in discussione il primato, ovviamente, visto che solo ChatGPT (per ora) può contare su 800 milioni di utenti settimanali, che si collegano da PC o da smartphone (utilizzando le sempre più convenienti offerte di **Internet mobile** con alta dotazione mensile di giga, come quelle che si possono trovare sul comparatore di **SOSTariffe.it**).

Ma c’è un rischio strategico più su larga scala, visto che chi controlla l’infrastruttura globale di ricerca e cloud controlla anche l’evoluzione culturale, linguistica e cognitiva dei modelli.

Il problema della sicurezza

È quando si parla di controllo e sicurezza che il quadro si fa davvero preoccupante, visto che un tale potere deve essere regolato con la massima cura per evitare danni globali, e molto spesso non lo è.

Il più recente **AI Safety Index** del **Future of Life Institute**

mostra che le principali aziende del settore stanno dirigendosi dritti dritti verso sistemi potenzialmente superumani, masenza adeguati meccanismi di controllo.

Otto compagnie sono state valutate e nessuna sembra avere un piano convincente per prevenire gli scenari di perdita del controllo: **Google DeepMind**, **OpenAI** e **Anthropic** guidano la classifica della sicurezza, ma ottengono comunque voti bassini, tra C e C+, mentre per quanto riguarda la variabile "**existential safety**" (la capacità di evitare eventi catastrofici o irreversibili) tutte le aziende hanno preso tra D o F, da insufficiente a gravemenete insufficiente.

Le aziende riconoscono il rischio (non possono farne a meno), ma continuano a non presentare strategie tecniche e regolatorie concrete per ridurlo.

E anche nella gestione dei danni già visibili, come **i modelli che forniscono consigli suicidi** o producono effetti psicologici documentati fin troppo bene dagli articoli che leggiamo ogni giorno sui giornali, i sistemi mostrano fragilità diffus.

Senza trasparenza e metriche verificabili l'investimento pubblico nella sovranità digitale rischia di costruire cattedrali senza fondamenta; aspirare al controllo nazionale dell'IA ha senso solo se, contemporaneamente, si sviluppano capacità reali per dominarne i rischi.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/lillusione-del-controllo-nellera-dellai/558418/