AI strategica: quando l’intelligenza artificiale diventa potere

L’**AI strategica** non è una proiezione futura: è già la cornice entro cui si ridefiniscono sovranità, competizione geopolitica e architetture di potere. Comprendere questa trasformazione significa rileggere il ruolo dell’intelligenza artificiale non come strumento, ma come infrastruttura critica dell’interesse nazionale.

Dall’innovazione al potere: la nuova dimensione dell’AI strategica

Negli ultimi anni con grande enfasi l’**intelligenza artificiale** è stata raccontata come **tecnologia abilitante**, parlando di **efficienza produttiva**, **automazione**, **ottimizzazione dei processi**, **analisi predittiva**. Oggi con una grandissima accelerazione, l’AI sta progressivamente abbandonando la sola dimensione dell’innovazione per entrare con prepotenza in

quella dell'**interesse nazionale**.

Il punto di svolta che sicuramente riguarda l'avanzamento tecnico dei **modelli generativi** o dei **sistemi di apprendimento automatico**, coinvolge in realtà la loro integrazione nei **processi decisionali pubblici**, nella **pianificazione industriale**, nella **sicurezza nazionale** e nelle **dinamiche geopolitiche**. L'AI assume le caratteristiche di un'**infrastruttura strategica**, comparabile alle reti energetiche, ai sistemi di telecomunicazione o alle piattaforme satellitari.

Quando una tecnologia diventa infrastruttura, il suo controllo oltre ad essere una questione di mercato, diventa soprattutto una questione di **potere**.

Modelli fondazionali e concentrazione di capacità

L'emergere dei **modelli fondazionali** (*foundation models*, ovvero modelli di intelligenza artificiale addestrati su grandi quantità di dati generali, riutilizzabili come base per molte applicazioni diverse), ha modificato la struttura dell'**ecosistema AI**. Questi sistemi, addestrati su quantità massive di dati rappresentano un **livello infrastrutturale** dell'intelligenza artificiale.

Il loro sviluppo richiede tre **risorse critiche** che possiamo così specificare: accesso a grandi volumi di **dati**, **capacità computazionale** avanzata e **competenze altamente specializzate**. Evidente che la conseguenza della concentrazione di tali risorse in un numero ristretto di attori globali, produce una nuova forma di **asimmetria tecnologica**.

Chi controlla i modelli controlla l'innovazione

Chi controlla **modelli di base**, **dataset strategici** e **infrastrutture di calcolo** ad alte prestazioni

influenza la direzione dell'innovazione, la disponibilità di strumenti per terzi e la configurazione degli **ecosistemi digitali nazionali**. La capacità computazionale, misurata in termini di potenza di calcolo e accesso a **chip avanzati**, assume inoltre una valenza geopolitica comparabile al controllo delle **materie prime energetiche**.

AI Act e high-risk systems: la regolazione come strumento di potere

L'adozione dell'**AI Act** da parte dell'Unione Europea ha sicuramente segnato un passaggio rilevante perché la regolazione dell'intelligenza artificiale viene oggi configurata come **architettura di governance**. La classificazione dei **sistemi ad alto rischio**, gli obblighi di **trasparenza**, i requisiti di **gestione del rischio** e le responsabilità per i fornitori incidono sulla struttura del mercato e sulla configurazione degli investimenti.

La regolazione non opera esclusivamente come strumento di tutela dei **diritti fondamentali** sia chiaro, ma contribuisce a definire **standard globali**. E vivendo all'interno di un contesto di **competizione tecnologica** tra Stati Uniti, Unione Europea e Cina, la capacità di fissare le regole del gioco assume indubbiamente un valore strategico.

Il controllo normativo dei sistemi ad alto rischio, inclusi quelli impiegati in ambito sanitario, finanziario, giudiziario e di **sicurezza pubblica**, delimita le modalità attraverso cui l'AI può incidere sulle **decisioni collettive**. Da questo ne deriva che la **governance dell'AI** diventa così governance del **potere tecnologico**.

Dati, infrastrutture computazionali e sovranità digitale

Un punto fermo da cui partire sempre quando si parla di AI è

quello che i **dati** costituiscono la **materia prima** dell'intelligenza artificiale. La loro disponibilità, qualità e **interoperabilità** determinano la performance dei modelli. La **politica dei dati**, inclusi *data spaces* europei, strategie nazionali e normative sulla condivisione, si intreccia con la questione della **sovranità digitale**.

Parallelamente, la capacità computazionale avanzata dipende da **infrastrutture fisiche**, pensiamo ai **data center**, ai sistemi di **high performance computing (HPC),** alle catene di approvvigionamento di **semiconduttori**. E le restrizioni all'export di chip avanzati, adottate in contesti geopolitici specifici, dimostrano come il controllo della capacità di calcolo venga percepito come una **leva strategica**.

Il triangolo infrastrutturale: dati, modelli e potenza di calcolo

Il nesso tra dati, modelli e potenza di calcolo definisce un **triangolo infrastrutturale**. La sua configurazione incide sulle traiettorie decisionali future, poiché sistemi di AI integrati nei processi pubblici e privati contribuiscono a orientare scelte economiche, allocazione di risorse e **valutazioni di rischio**.

AI come moltiplicatore decisionale: quando l'algoritmo delimita le scelte

Altra riflessione necessaria è che l'intelligenza artificiale interviene sempre più nella fase di **pre-decisione**, attraverso **analisi predittiva**, **scoring**, **profilazione**, ottimizzazione di scenari. Questo significa che anche quando la decisione finale resta umana, il perimetro delle opzioni viene delimitato da **modelli algoritmici**.

La questione assume un rilievo anche in questo caso strategico quando tali modelli sono sviluppati, addestrati e controllati da attori esterni al perimetro nazionale. La **dipendenza**

tecnologica può tradursi in **dipendenza cognitiva**, poiché le categorie interpretative incorporate nei sistemi influenzano la valutazione delle alternative.

L'**AI strategica** si colloca quindi nell'intersezione tra tecnologia, **sicurezza nazionale** e **politica industriale**. La capacità di sviluppare modelli autonomi, proteggere dataset sensibili e garantire infrastrutture computazionali resilienti diventa componente della sicurezza complessiva.

Verso una dottrina dell'AI strategica

L'AI come **infrastruttura di potere** richiede come diretta conseguenza una **dottrina integrata** e pertanto politiche industriali, investimenti in ricerca, formazione specialistica e cooperazione internazionale devono convergere in una visione coerente.

L'**interesse nazionale** non si esaurisce nella produzione di applicazioni innovative, ma anzi, oggi deve includere la capacità di definire standard, proteggere **asset critici** e ridurre **dipendenze strutturali**. In questo nuovo paradigma, l'AI Act, le strategie nazionali sull'intelligenza artificiale e i programmi europei per l'**high performance computing** rappresentano nuovi strumenti di **architettura strategica**.

La transizione dall'AI come tecnologia abilitante all'AI come infrastruttura di potere caratterizza come anticipato un **mutamento di paradigma**. Il controllo di modelli, dati e capacità computazionale influenza la configurazione delle scelte future e la **sovranità tecnologica** assume una dimensione concreta e misurabile, in cui regolazione, innovazione e sicurezza inevitabilmente convergono.

Bibliografia

European High-Performance Computing Joint Undertaking (EuroHPC JU), *Official Documentation*, 2023–2024.

European Parliament and Council, *Artificial Intelligence Act*, Regulation (EU) 2024/… (testo definitivo approvato 2024).

OECD, *OECD AI Principles*, 2019.

Stanford University, *AI Index Report 2024*, Stanford Institute for Human-Centered AI.

European Commission, *Coordinated Plan on Artificial Intelligence*, 2021 Update.

Brundage, M. et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018.

National Security Commission on Artificial Intelligence (NSCAI), *Final Report*, 2021.

Executive Office of the President (USA), *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 2023.