Sovereign AI Report

Come le organizzazioni italiane possono riprendere il controllo sull'AI che usano

Rational AI

Executive Summary

L'AI è già al lavoro nelle organizzazioni italiane, spesso più di quanto i loro responsabili pensino. Sistemi di screening del personale, algoritmi di pricing, strumenti di analisi del rischio, assistenti integrati nei software gestionali: l'AI è entrata nei processi aziendali attraverso mille porte diverse, non sempre con la consapevolezza di chi ne è responsabile.

Questo crea un'esposizione che diventa urgente nel 2026, per tre ragioni convergenti.

La prima è normativa. Il 2 agosto 2026, l'EU AI Act entra in piena applicazione per i sistemi ad alto rischio. Le organizzazioni che usano sistemi AI per decisioni che riguardano persone (selezione del personale, accesso ai servizi, gestione delle infrastrutture) devono essere conformi: documentazione tecnica, valutazione di conformità, tracciabilità degli output, supervisione umana. Il rischio di una svista o di un'imprecisione si traduce in sanzioni fino a 35 milioni di euro o al 7% del fatturato globale per le pratiche vietate.

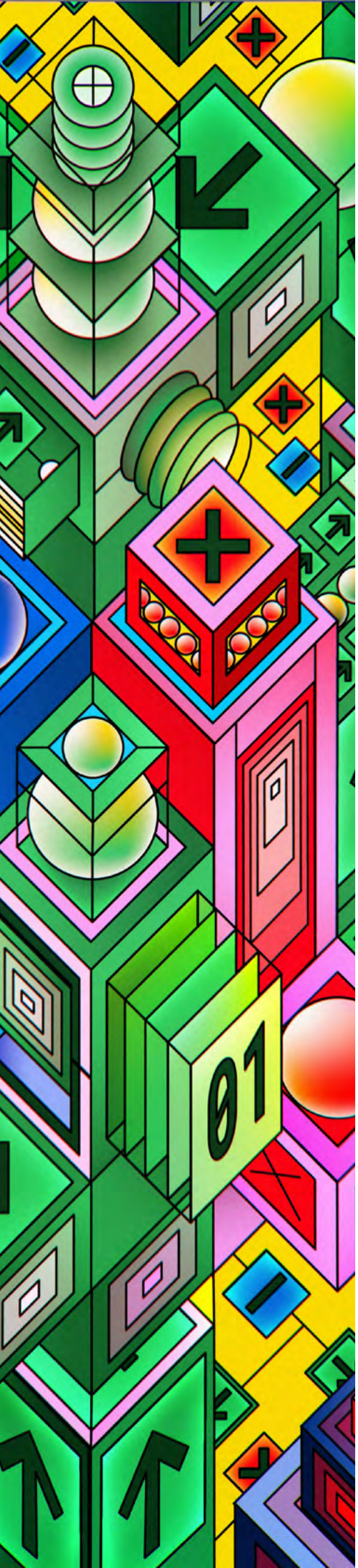
La seconda è geopolitica. L'Europa controlla meno del 5% della capacità computazionale AI globale. Gli hyperscaler americani dominano oltre il 70% del mercato cloud europeo. Il CLOUD Act americano consente alle autorità statunitensi di accedere ai dati di provider USA indipendentemente da dove sono fisicamente archiviati. Scegliere la "EU region" di AWS o Azure non è una questione di sovranità ma di data residency, che è una cosa diversa.

La terza è strategica. Le organizzazioni che dipendono interamente da modelli e infrastrutture esterne per i propri processi critici hanno trasferito una parte significativa del proprio potere decisionale a soggetti su cui non hanno leva. Se il vendor cambia i prezzi, modifica i termini d'uso o subisce un'interruzione, l'organizzazione ne subisce le conseguenze senza poter intervenire.

AI sovrana non significa costruire modelli fondazionali nazionali o infrastrutture da miliardi di euro. Significa, per ogni organizzazione, una cosa più concreta: sapere cosa sta succedendo ai propri dati, ai propri modelli e ai propri processi decisionali quando si adotta l'intelligenza artificiale, e mantenere il controllo su tutto questo nel tempo.

Questo documento descrive come farlo, per tre tipologie di organizzazioni diverse (PMI, grandi aziende e Pubblica Amministrazione) con un metodo in quattro fasi e uno strumento di autovalutazione che ogni organizzazione può usare subito.

Il punto di partenza è una questione di inventariato: sapere cosa si ha, prima di decidere cosa costruire.



Il contesto: perché adesso

La domanda che molte organizzazioni si pongono, di fronte al tema della sovranità AI, è legittima: perché adesso? L'AI esiste da decenni, la dipendenza tecnologica da vendor americani anche. Cosa è cambiato?

Tre forze stanno convergendo simultaneamente, e la loro combinazione rende il 2026 un momento diverso da tutti i precedenti.

Il quadro geopolitico

L'Europa produce meno del 5% della capacità computazionale AI globale. Gli hyperscaler americani controllano oltre il 70% del mercato cloud europeo. Tale concentrazione è il prodotto di due decenni di investimenti privati americani in assenza di una risposta europea coordinata.

Le conseguenze sono diventate visibili negli ultimi anni in modo sempre più netto. Quando nel 2025 l'amministrazione americana ha inasprito i controlli sulle esportazioni di tecnologie AI verso alcuni paesi, molte organizzazioni europee hanno scoperto di dipendere, per i propri sistemi critici, da infrastrutture su cui non hanno alcuna leva negoziale. Quando OpenAI ha modificato i termini d'uso dei propri modelli, chi aveva costruito processi aziendali intorno a quelle API si è trovato a dover scegliere tra accettare le nuove condizioni o affrontare una migrazione costosa.

I tre scenari

La sovranità AI non è uguale per tutti. Un comune di diecimila abitanti, una manifattura da duecento dipendenti e una banca con operazioni in più paesi europei hanno esposizioni diverse, risorse diverse e priorità diverse.

	PMI	Grandi Aziende	PA
Problema	Adozione inconsapevole, zero governance	AI frammentata, nessuna visione d'insieme	Decisioni pubbliche non tracciabili
Rischio	Sistemi Annex III in produzione senza documentazione	Vendor lock-in su processi critici	Output non spiegabili su decisioni che riguardano cittadini
Approccio	Assessment leggero, compliance prima	Inventario sistemi, architettura ibrida	Compliance-first, governance centralizzata

PMI

Il problema

La maggior parte delle PMI italiane che usano AI non sa di usarla nel senso rilevante per questo documento. Sa che usa ChatGPT per scrivere testi, o che il proprio CRM ha una funzione di “suggerimento intelligente”, o che il software HR incorpora un algoritmo di screening dei candidati. Non sa (perché nessuno gliel’ha mai chiesto) se questi strumenti trattano dati personali dei dipendenti o dei clienti, se i dati migrano su server americani, se i modelli sottostanti vengono aggiornati da terze parti senza notifica.

Valuta il tuo livello di sovranità AI

Le dieci domande che seguono coprono i quattro livelli dello stack: infrastruttura, modelli, applicazioni e governance. Per ciascuna, la risposta è sì (1 punto) o no (0 punti). Non esistono risposte parzialmente corrette: o un inventario esiste, o non esiste.

Rational AI

Rational AI nasce per risolvere uno dei principali ostacoli all'adozione dell'AI in ambito enterprise e pubblico: la mancanza di controllo su dati, modelli e decisioni. La piattaforma offre un'infrastruttura modulare e open-source che consente di portare l'AI in produzione senza cedere la proprietà dei dati a terzi, senza lock-in tecnologico e con strumenti nativi di governance, audit e supervisione umana. Progettata per integrarsi con i sistemi esistenti, ERP, CRM e archivi documentali, trasforma l'AI da strumento sperimentale a infrastruttura aziendale governabile.

Rational AI srl è una società soggetta all'attività di direzione e coordinamento di Geckosoft Group s.r.l.
Società a socio unico.

Maggio 2026