SOLUZIONI DI INTELLIGENZA ARTIFICIALE PER IL MERCATO EUROPEO

regole, strategie e scelte tecnologiche

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

Ordine degli Ingegneri della Provincia di Roma

Etica e Governance umana nell'AI
Roma 30 aprile 2026

FOIR

Presentazioni

Fabio Massimi

- Laurea in Ingegneria Elettronica
- Master in Economia e Management dell'Innovazione
- Master in Sicurezza delle Informazioni e Informazione Strategica
- **Oltre 20 anni di esperienza** in sistemi digitali complessi (privato e PA)
- **Competenze chiave**: architetture software distribuite · data integration · governance tecnologica
- **Settore privato**: co-fondatore e CTO di imprese ICT
  - 👉 Ambito **finanziario, lusso e industria meccanica**
  - 👉 Soluzioni data-driven, business intelligence, sistemi per la **conformità e gestione della conoscenza**
- **Pubblica Amministrazione:** CNIPA, DigitPA, AgID, PCM:
  - 👉 Progettazione di **infrastrutture digitali nazionali strategiche**
  - 👉 Fatturazione elettronica · Pagamenti digitali · e-Procurement
- **Standardizzazione e regolazione**: ISO · CEN · CENELEC · UN/CEFACT · UNI · UNINFO · Commissione Europea
- **AgID – Intelligenza Artificiale**:
  - 👉 AI Act e AI Board europeo
  - 👉 Strategia Nazionale AI, Linee Guida IA, Legge 132/2025
- **Focus attuale**. Governance AI · Gestione del rischio · Conformità · Cybersecurity · Data governance

Agenda

1 Contesto europeo
- EU Digital Single Market
- Brussels Effect
- New Legislative Framework (NLF)
- AgID e quadro normativo italiano

slide 3–5

2 AI Act
- Principi fondamentali
- Classificazione del rischio
- Tipologie di rischio specifici dell'IA
- GPAI e rischio sistemico

slide 6–14

3 Principi per lo sviluppo dell'IA
- La pila tecnologica (stack IA)
- Chip, Cloud, Modelli, App
- Hardware decoupling
- Clausole contrattuali

slide 15–39

4 Sovranità tecnologica e cloud
- EU Cloud Sovereignty Framework
- BSI C3A
- Criteri di disconnessione
- Framework di confronto

slide 40–49

5 Principi per il procurement dell'IA
- Ciclo di procurement
- Valutazione tecnica
- GPAI e modelli fondazionali
- Strumenti: LCOAI, capitolato

slide 50–67

6 Costo e valore dell'IA (LCOAI)
- Dal costo parziale al ciclo di vita
- CAPEX · OPEX · Costi di uscita
- Applicazione nel procurement
- Valore per la PA

slide 55–67

7 IA come strumento professionale
- IA per lo sviluppo software
- Governance e qualità
- Ruolo dell'ingegnere
- Etica e human oversight

slide 68–76

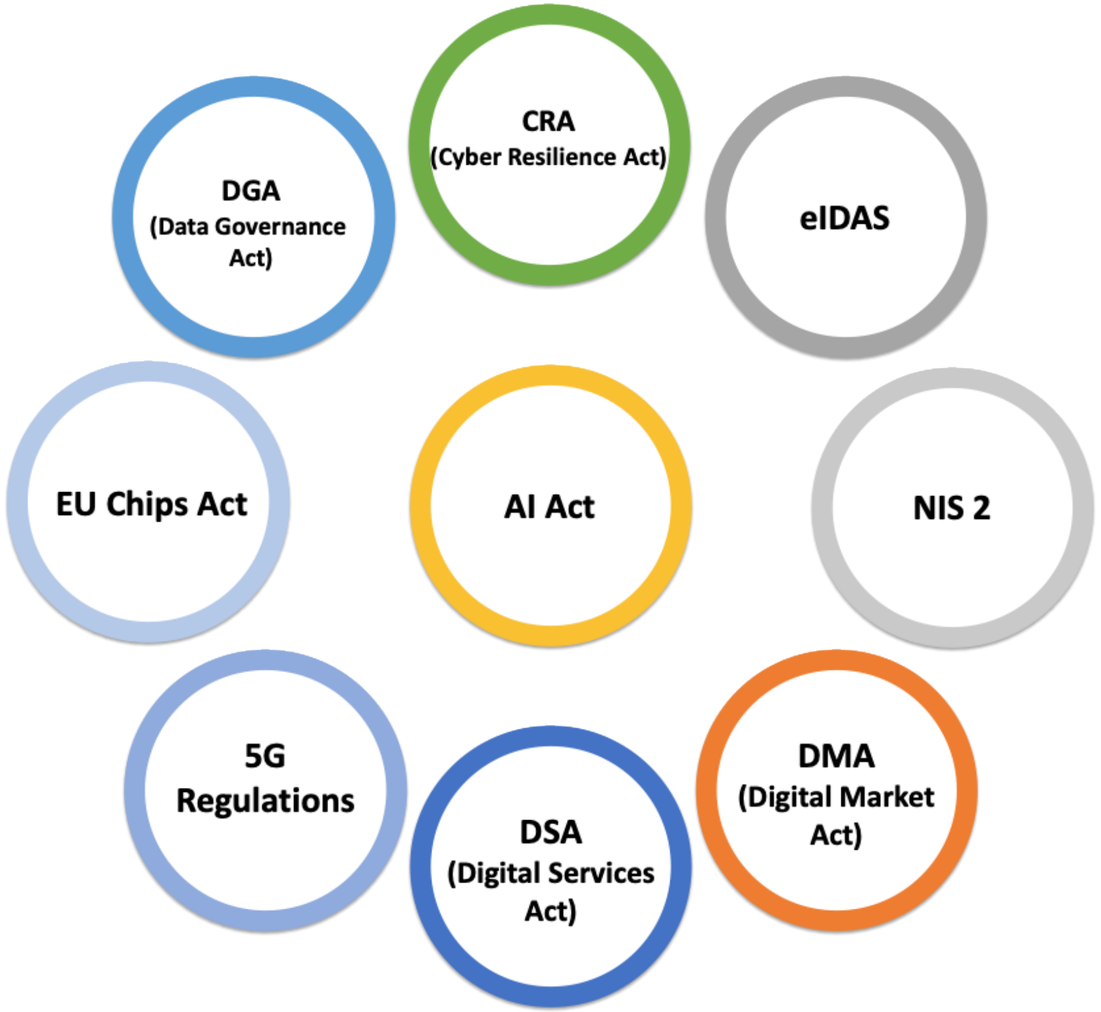
Scelta tecnologica consapevole
regole · stack · costi · governance · etica

EU Digital Single Market

Attraverso regole comuni, **standard condivisi** e **interoperabilità**, l'Europa punta a creare un ecosistema dove **innovazione**, **sicurezza** e **tutela dei diritti** procedano insieme, favorendo la crescita e la competitività di cittadini, imprese e pubbliche amministrazioni.

Brussels Effect

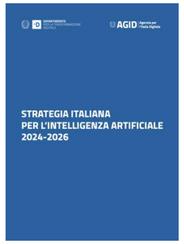
L'UE stabilisce **regole rigorose per i beni e servizi** che accedono al suo mercato. Tali regole sono adottate dalle grandi imprese anche fuori dall'Europa, generando un **impatto sul mercato globale**.



New Legislative Framework

Il **New Legislative Framework** (NLF), modello adottato anche dall'AI Act, utilizza **norme tecniche armonizzate** per dimostrare la conformità ai requisiti di legge.
Questo approccio favorisce **sicurezza e fiducia** del consumatore, permettendo di verificare i sistemi di IA tramite **autovalutazione** o **valutazione di organismi indipendenti**, in base al livello di rischio.

AgID per l’Intelligenza Artificiale



Strategia per l’Intelligenza Artificiale 2024-26. Definisce le priorità e gli obiettivi per lo sviluppo e l’adozione dell’IA in Italia, secondo i quattro pilastri: **pubblica amministrazione**, **imprese**, **educazione** e **ricerca**.

Piano Triennale 2024-26. Definisce principi e obiettivi operativi per lo sviluppo e l’adozione dell’IA nella Pubblica Amministrazione, in particolare: linee guida, ricognizione dei progetti e banche dati, promozione di **centri di competenza** e **reti**.

Linee guida per l’IA. Stabiliscono criteri organizzativi, etici e tecnici per l’adozione, il procurement e lo sviluppo di soluzioni di IA affidabili, trasparenti.

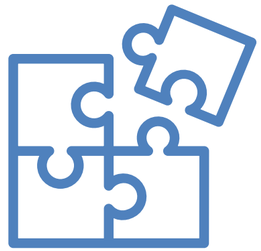
Legge 132/2025. Attribuisce ad AgID il ruolo di promozione dell’IA, di autorità di notifica per i sistemi di IA ad alto rischio e di coordinamento degli spazi di sperimentazione.

I principi fondamentali dell’AI Act

Regolamentazione di prodotto rafforzata: rischi per la salute, la sicurezza e i diritti fondamentali.

Sistema di IA e rischi che possono essere generati da un sistema di IA: il fulcro dei requisiti per i sistemi ad alto rischio.

Approccio basato sul rischio e sul ciclo di vita: regolamentazione basata sul rischio, con monitoraggio pre e post-market.



Fiducia lungo l’intera catena del valore: regole per i sistemi di IA e i modelli GPAI (modelli di IA generativa).

Innovazione responsabile: promuovere lo sviluppo di un’IA affidabile e centrata sull’essere umano.

Norme tecniche Europee armonizzate per garantire un'IA affidabile

CE

AI board sub-groups

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

Code of Practice on General Purpose AI : linee guida volontarie per garantire che i modelli di IA di uso generale siano sviluppati e utilizzati in modo responsabile. Final Draft: 1) Transparency, 2) Copyright, 3) Safety and Security (art. 56 AI Act)

AI sandboxes: ambienti di sperimentazione regolamentata, dove le aziende possono testare sistemi di IA in modo sicuro (art. 57 AI Act)

Prohibitions: linee guida sulle pratiche di intelligenza artificiale vietate dall'AI Act (pubblicate il 4 febbraio 2025) (art. 5 AI Act).

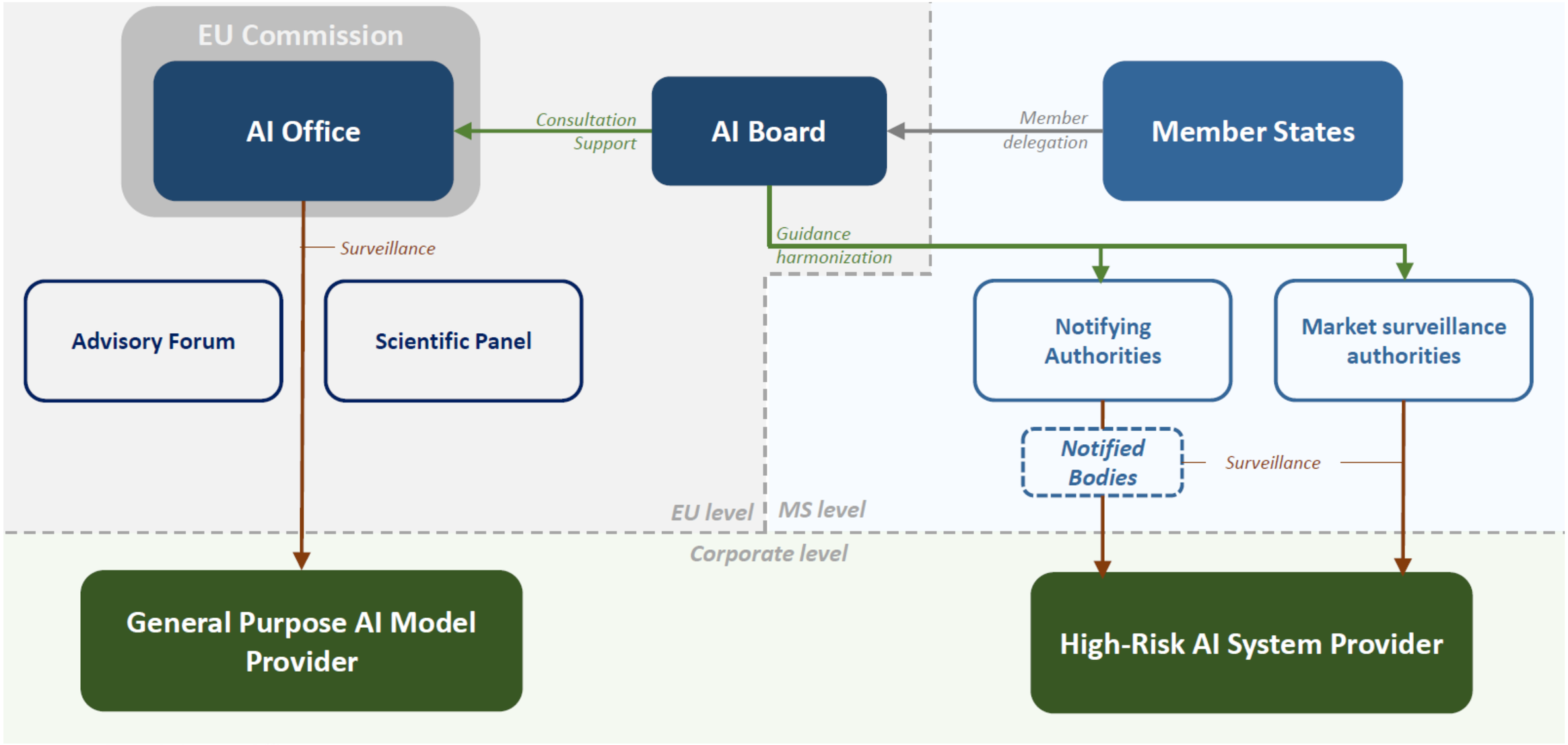
Standards: standard armonizzati necessari per dimostrare la conformità dei sistemi di IA ai requisiti normativi europei (art. 40 AI Act)

AI Act interplay with other Union legislation: interazioni tra l'AI Act e la normativa di armonizzazione dell'Unione, in linea con New Legislative Framework, per garantire coerenza e applicazione integrata delle regole europee (Annex I Ai Act)

Annex III High-risk AI: sistemi di IA ad alto rischio elencati nell'Allegato III dell'AI Act, ai sensi dell'articolo 6, paragrafo 2

Financial Services: applicazione dell'IA nel settore dei servizi finanziari in conformità con AI Act

Implementazione dell'IA Act – Compiti di EC e Stati Membri



Fonte: EU Commission - AI Office

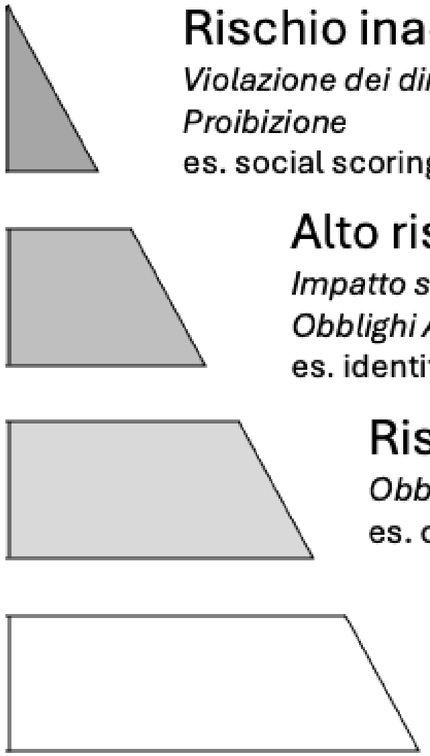
Classificazione del rischio

Modelli di IA per finalità generali (GPAI)

Alto rischio potenziale

Obblighi di informazione e trasparenza, sorveglianza di mercato
Gestione del rischio nel caso di rischio sistemico

Sistemi IA – Classificazione del rischio



Rischio inaccettabile

Violazione dei diritti fondamentali dell'UE
Proibizione
es. social scoring, manipolazione del comportamento umano

Alto rischio

Impatto sulla salute, sicurezza o diritti fondamentali
Obblighi AI Act (valutazione di conformità, ecc.)
es. identificazione biometrica, gestione infrastrutture critiche)

Rischio limitato

Obblighi di informazione e trasparenza
es. chatbot, contenuti generati dall'IA (testo, audio, video)

Rischio minimo o nessun rischio

Nessuna regolazione specifica
es. Sistemi di raccomandazione, filtri anti-spam

Fonte: EU Commission - AI Office

Tipologie di rischio secondo l’AI Act

L’AI Act non si limita a classificare i sistemi in base al livello di rischio, ma identifica anche le **principali tipologie di rischio da gestire**, con particolare attenzione a quelli che impattano su **salute**, **sicurezza** e **diritti fondamentali**.

Oltre ai rischi tradizionali (salute e sicurezza), l’AI Act introduce **rischi specifici dell’IA**, esplicitamente menzionati in diversi articoli, soprattutto per i sistemi ad alto rischio:

- **Bias e discriminazione** (Art. 10.2(f)): output distorti che influenzano negativamente operazioni successive o producono discriminazioni.
- **Impatto su soggetti vulnerabili** (Art. 9.9): in particolare minori e categorie fragili.
- **Bias dell’automazione** (Art. 14.4(b)): affidamento eccessivo o acritico agli output dell’IA.
- **Feedback loop** (Art. 15.4): effetti a catena distorti in sistemi auto-apprendenti non controllati.
- **Cybersecurity** (Art. 15.5): vulnerabilità sfruttabili nei sistemi IA.

Questi elementi rafforzano il ruolo centrale della gestione del rischio nell’AI Act, non solo come requisito tecnico, ma come garanzia per la protezione effettiva delle persone.

Tipologie di rischio secondo l’AI Act

L’AI Act non si limita a classificare i sistemi in base al livello di rischio, ma identifica anche le **principali tipologie di rischio da gestire**, con particolare attenzione a quelli che impattano su **salute**, **sicurezza** e **diritti fondamentali**.

Oltre ai rischi tradizionali (salute e sicurezza), l’AI Act introduce **rischi specifici dell’IA**, esplicitamente menzionati in diversi articoli, soprattutto per i sistemi ad alto rischio:

- **Bias e discriminazione** (Art. 10.2(f)): output distorti che influenzano negativamente operazioni successive o producono discriminazioni.
- **Impatto su soggetti vulnerabili** (Art. 9.9): in particolare minori e categorie fragili.
- **Bias dell’automazione** (Art. 14.4(b)): affidamento eccessivo o acritico agli output dell’IA.
- **Feedback loop** (Art. 15.4): effetti a catena distorti in sistemi auto-apprendenti non controllati.
- **Cybersecurity** (Art. 15.5): vulnerabilità sfruttabili nei sistemi IA.

Questi elementi rafforzano il ruolo centrale della gestione del rischio nell’AI Act, non solo come requisito tecnico, ma come garanzia per la protezione effettiva delle persone.

Standardisation Request M/593* - requisiti

Ambito prioritario	Sintesi dei requisiti tecnici richiesti	Riferimento AI Act
Gestione del rischio	Criteri verificabili per la mitigazione lungo il ciclo di vita, integrazione con QMS, approccio basato sull'impatto.	Art. 9
Governance e qualità dei dati	Verifica della provenienza e rappresentatività, metodi per la riduzione del bias, documentazione delle fonti e gestione dei set di dati.	Art. 10
Logging e tracciabilità	Sistemi automatici per registrare eventi e decisioni, supporto a verifiche ex-post e audit.	Art. 12
Trasparenza	Informazioni leggibili e accessibili per utenti esperti e non esperti, spiegabilità dei modelli e delle decisioni.	Art. 13
Supervisione umana	Meccanismi per l'intervento e il controllo umano efficace, strumenti di override, documentazione dell'interazione.	Art. 14
Accuratezza	Scelta e giustificazione delle metriche, soglie minime proporzionate ai rischi, validazione continua.	Art. 15 comma 3
Robustezza	Gestione delle anomalie, resilienza in condizioni operative non previste, stress testing.	Art. 15 comma 4
Cybersicurezza	Difesa contro attacchi (data poisoning, adversarial), gestione delle vulnerabilità e sicurezza dei dati.	Art. 15 comma 5
Sistema di gestione per la qualità (QMS)	Adattamento dei sistemi QMS esistenti alle specificità dell'IA, requisiti minimi per organizzazioni di diversa dimensione.	Art. 17
Valutazione di conformità	Metodi per audit interni ed esterni, strumenti per test, checklist di conformità, indicazioni per organismi notificati.	Art. 43

*Standardisation request M/593 - Decisione della EC C(2023)3215 e C(2025)3871

Ruoli dell'AI Act

L'AI Act assegna obblighi specifici in funzione del ruolo nella catena del valore del sistema di IA.

Fornitore (provider)

«fornitore»: *una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che* ***sviluppa*** *un sistema di IA o un modello di IA per finalità generali o che* ***fa sviluppare*** *un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o* ***mette in servizio il sistema di IA con il proprio nome o marchio****, a titolo oneroso o gratuito (rif. AI Act, art.3 c.3).*

Deployer (utilizzatore)

«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che **utilizza** un sistema di IA **sotto la propria autorità**, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale *(rif. AI Act, art.3 c.4).*

European Commission

AI Act Service Desk

Home | AI Act Explorer | Compliance Checker | AI Act Timeline | Resources | Natic

AI Act Explorer consente di **navigare** i capitoli, allegati e considerando dell'**AI Act**.

Compliance Checker aiuta a **valutare la conformità** dei sistemi e dei modelli di intelligenza artificiale ai **requisiti dell'AI Act**.

AI Act Single Information Platform

AI EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

The AI Act, which entered into force on 1 August 2024, creates a single market and harmonised rules for trustworthy AI in the EU. It aims to promote innovation and uptake of AI, while addressing potential risks to people's health, safety, and fundamental rights and safeguarding democracy and the rule of law. The adoption of the AI Act marks a major milestone for the EU, and ensuring its effective implementation is now a key priority for the Commission.

The Single Information Platform, as foreseen in the AI Act, provides online interactive tools to help stakeholders determine whether they are subject to legal obligations and understand the steps they need to take to comply.

The Platform is part of the AI Act Service Desk, which has been launched as a central initiative to help stakeholders navigate the AI Act requirements. It serves as an accessible, up-to-date information hub offering clear guidance on the AI Act's application.

AI Act Explorer

The AI Act Explorer is an online tool designed to help users to browse through different chapters, annexes and recitals of the AI Act in an intuitive way.

Compliance Checker

The AI Act compliance checker is a tool that assists in evaluating whether AI systems and general-purpose AI models meet the requirements set by the AI Act.

National Resources

Browse contacts and activities from Member States, Innovation Hubs, and national authorities. Find information and local initiatives related to the AI Act.

Sistemi ad alto rischio: obblighi del fornitore

•Your AI system is likely classified as a high-risk system under the AI Act, following Article 6 (opens in a new tab). You are required to comply with the obligations outlined in Articles 8-15 of the AI Act, which pertain to high-risk AI systems. These requirements include:

- establish a risk management system;
- ensure adequate data governance and management practices;
- draw up technical documentation;
- ensure traceability (record-keeping);
- enable deployers to interpret your AI system's output;
- enable human oversight;
- ensure an appropriate level of accuracy, robustness and cybersecurity.

•Additionally, as indicated in Article 16 (opens in a new tab), a provider must also:

- indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trademark, the address at which they can be contacted;
- have a quality management system in place which complies with Article 17 (opens in a new tab);
- keep the documentation referred to in Article 18 (opens in a new tab);
- when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19 (opens in a new tab);
- ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43 (opens in a new tab);
- draw up an EU declaration of conformity in accordance with Article 47 (opens in a new tab);
- affix the CE marking to the high-risk AI system, in accordance with Article 48 (opens in a new tab);
- comply with the registration obligations referred to in Article 49 (opens in a new tab)(1);
- take the necessary corrective actions and provide information as required in Article 20 (opens in a new tab);
- cooperate with national competent authorities as required in Article 21 (opens in a new tab).
- ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Sistemi ad alto rischio: obbligo di FRIA per il «deployer»

•Prior to deploying a high-risk AI system, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III (opens in a new tab), shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment based on Article 27 (opens in a new tab)requirements.

The above obligation applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider.

Once the assessment has been performed, the deployer shall notify the market surveillance authority of its results.

If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article-35 of Regulation (EU) 2016/679 or Article-27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

Sistemi ad alto rischio: obblighi del «deployer»

•Your AI system is likely classified as a high-risk system under the AI Act, following Article 6 (opens in a new tab). As a deployer of a high-risk AI system, pursuant to Article 26 (opens in a new tab)you must:

- take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;
- assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;
- to the extent the deployer exercises control over the input data, you shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;
- monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72 (opens in a new tab). Where there is a reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk you must without undue delay inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system;
- keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in applicable Union or national law, in particular in Union law on the protection of personal data. Deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant Union financial service law.

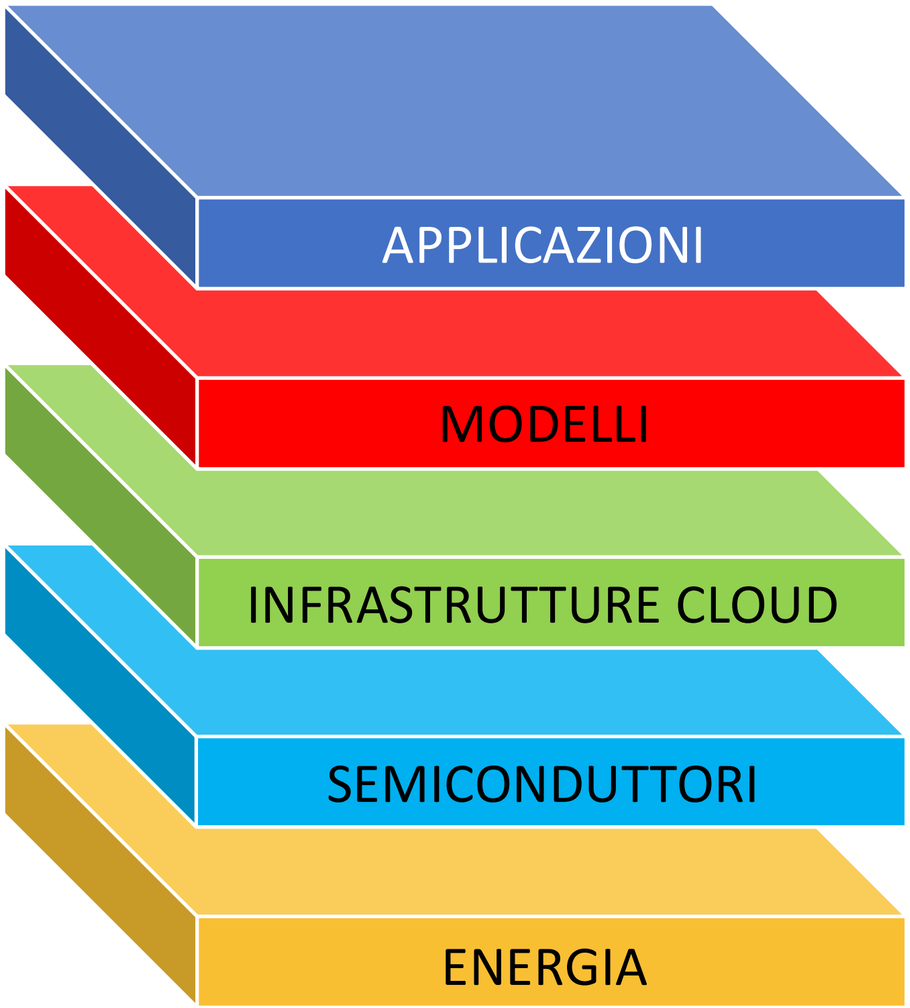
•Additionally:

- for high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system;
- in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-remote biometric identification shall request an authorisation, ex-ante, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence;
- deployers of high-risk AI systems referred to in Annex III (opens in a new tab)that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system. For high-risk AI systems used for law enforcement purposes Article-13 of Directive (EU) 2016/680 shall apply;
- cooperate with competent authorities.

PRINCIPI PER LO SVILUPPO DELL'INTELLIGENZA ARTIFICIALE

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

La pila tecnologica per lo sviluppo dell'Intelligenza Artificiale



*Jensen Huang, CEO di NVIDIA

*Pila NVIDIA**

Valore economico e sociale. L'IA diventa servizio, prodotto e supporto alle decisioni per cittadini, imprese e PA.

Intelligenza codificata. Algoritmi e modelli fondazionali concentrano conoscenza, elaborazione dati e capacità predittiva.

Strato abilitante e moltiplicatore. Trasforma energia e chip in capacità di calcolo accessibile, scalabile e governabile su larga scala.

Cuore computazionale. Chip specializzati (GPU, acceleratori) determinano prestazioni, efficienza e autonomia tecnologica.

Fondamento materiale dell'IA. Senza disponibilità energetica stabile e scalabile non esiste capacità di calcolo né addestramento dei modelli.

Espansione dei data center: sfide e fattori critici

Energia

Raffredamento e risorse idriche

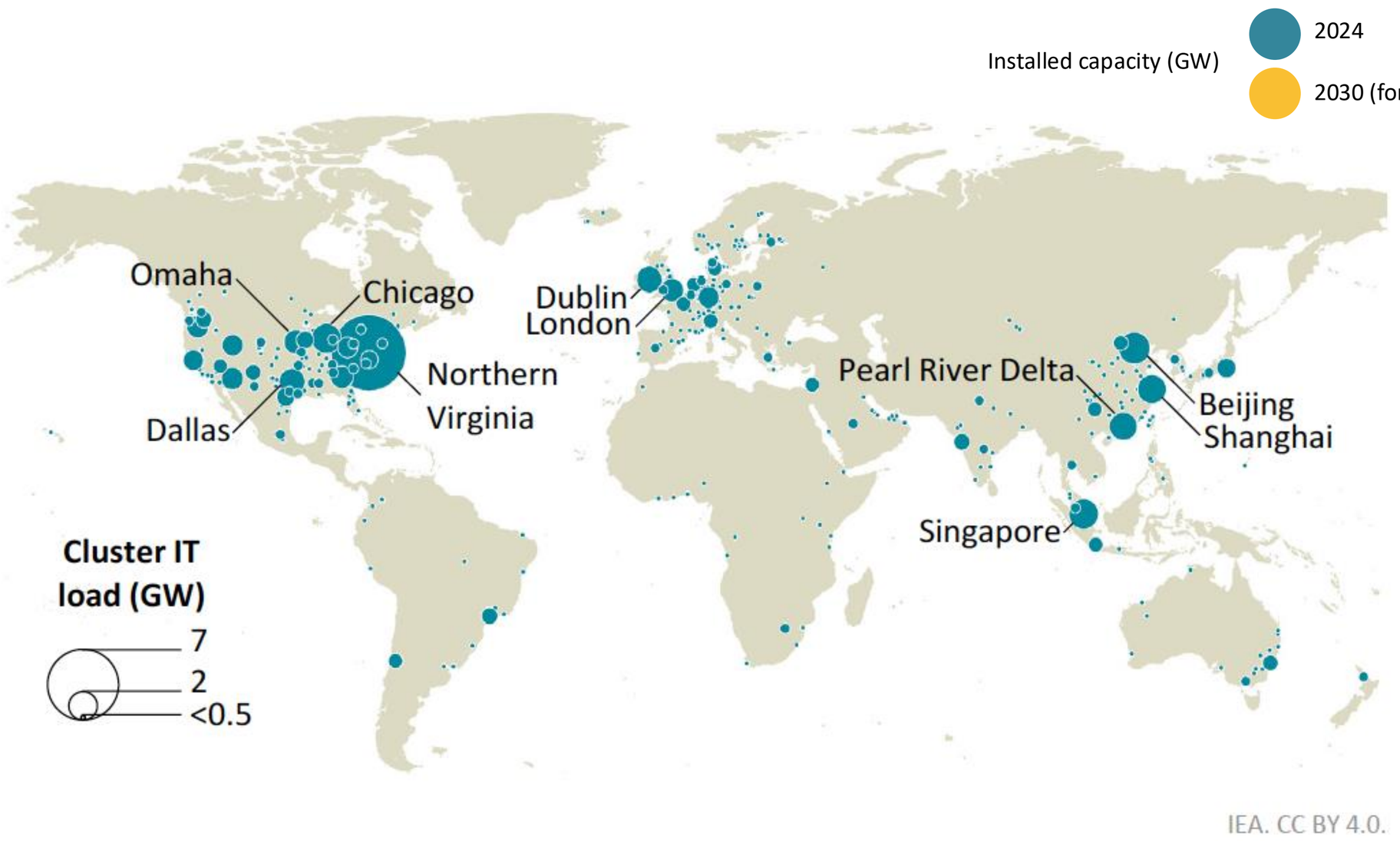
Conformità normativa

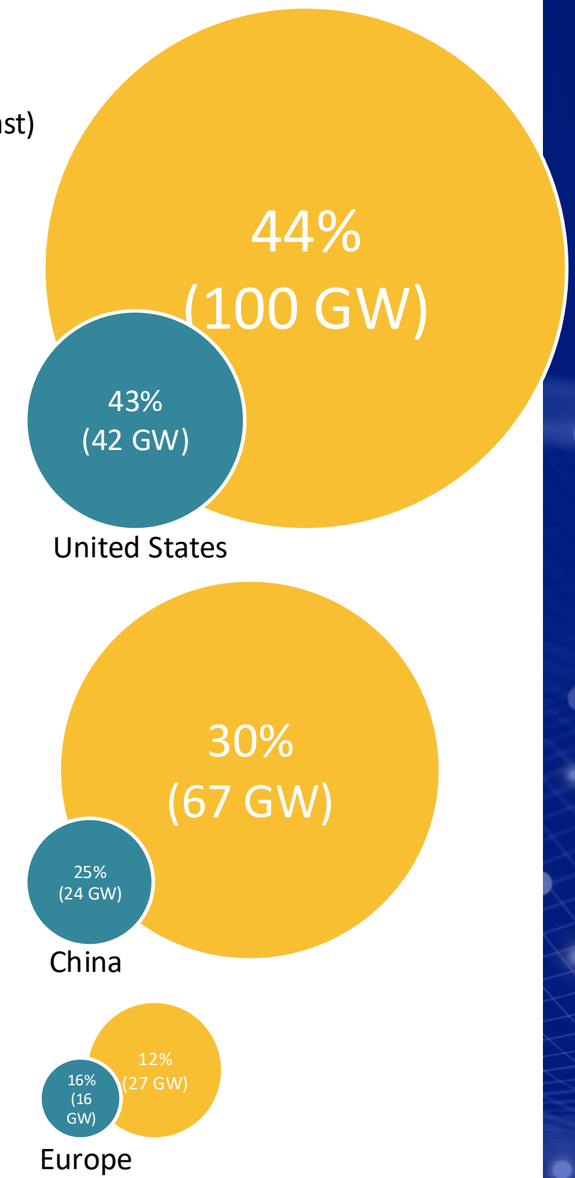
Spazio fisico

Sovranità

«Per l'IA stiamo realizzando la più grande infrastruttura della storia umana»
Jensen Huang, CEO di NVIDIA, WEF Davos 2026

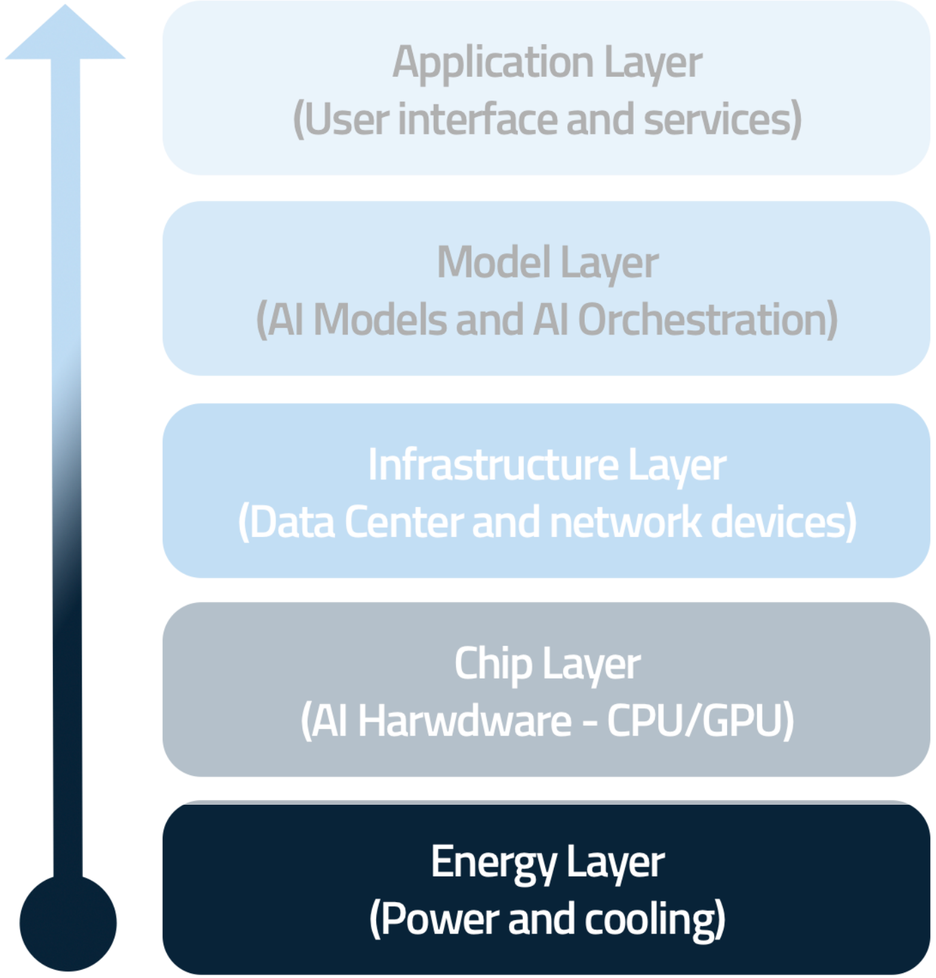
Global map of large data centre clusters 2024*





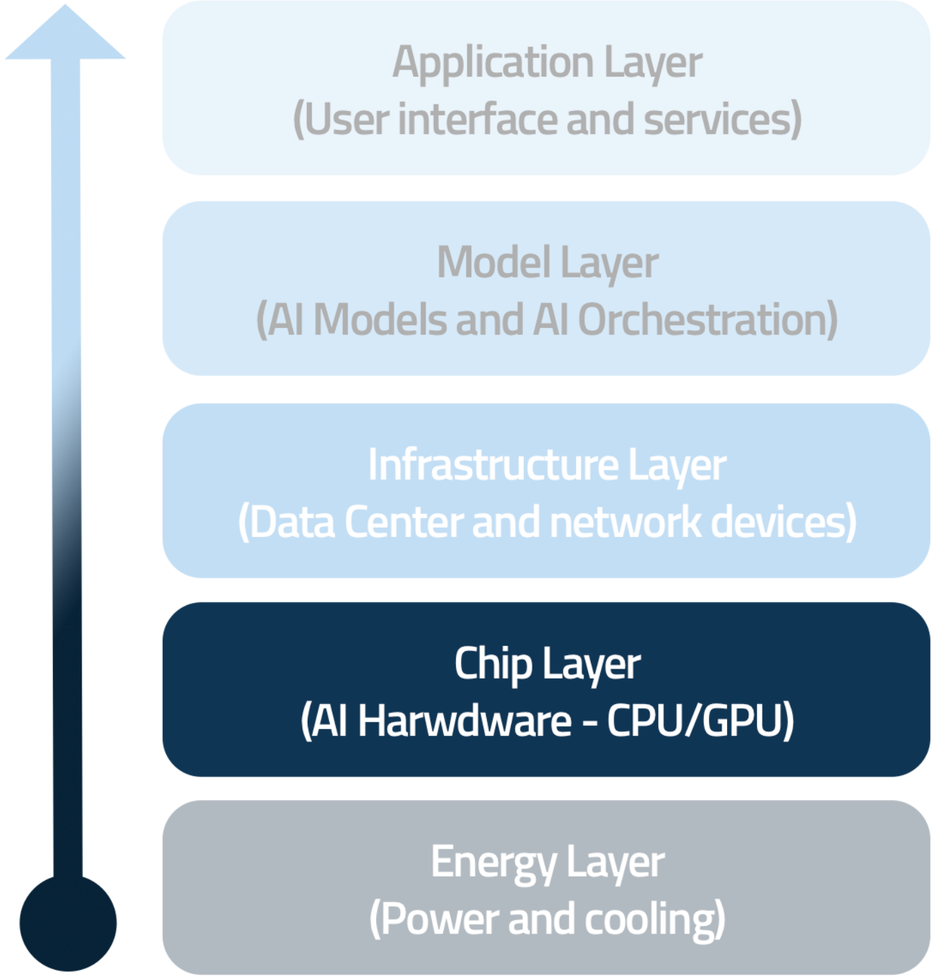
Source: World Energy Outlook Special Report – Energy and IA – IEA 2025

Lo Stack IA: energia



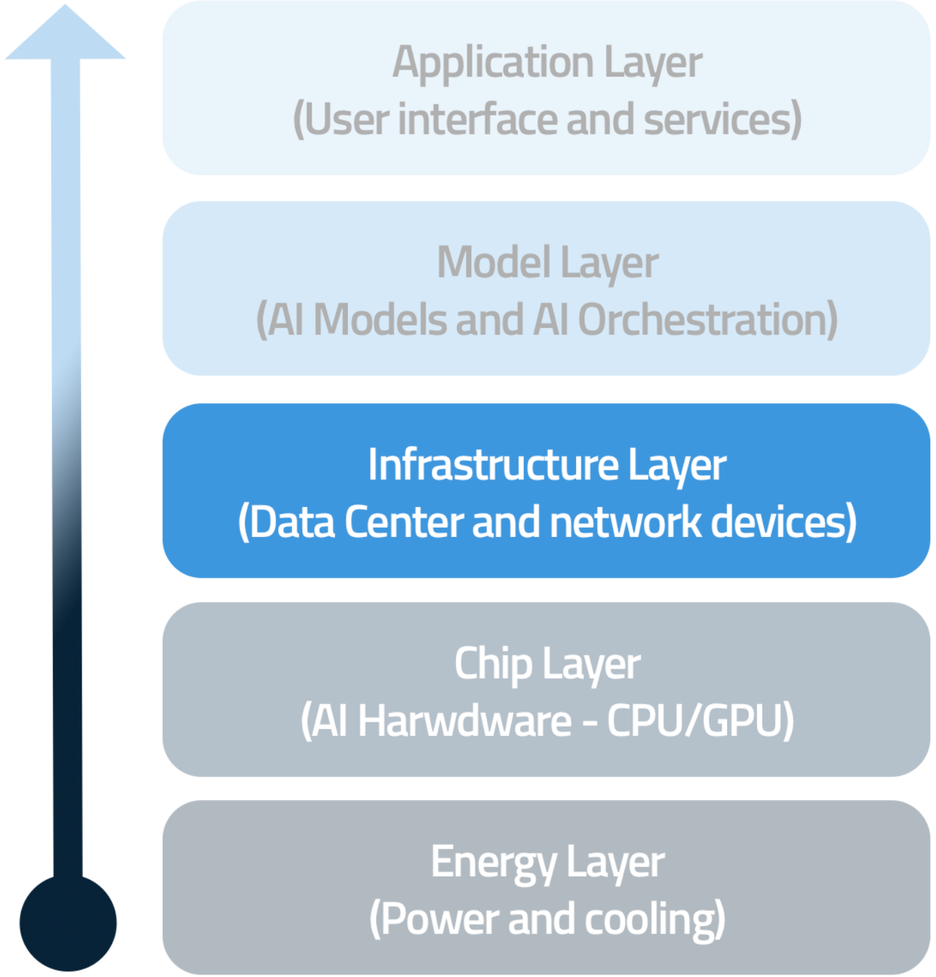
	Descrizione
Funzione	Costituisce la base fisica dello Stack IA: comprende la fornitura di energia elettrica, i sistemi di raffreddamento e la gestione termica necessari ad alimentare data center e dispositivi IA.
Rilevanza	Un'infrastruttura energetica stabile ed efficiente è indispensabile per garantire continuità operativa. L'attuazione, inoltre, di tecniche di ottimizzazione energetica riduce costi operativi e impatto ambientale.
Componenti tipiche	Sistemi di alimentazione ad alta efficienza; tecnologie avanzate di raffreddamento (es. raffreddamento liquido); utilizzo di fonti rinnovabili per data center.
Punti di attenzione	Questo livello assume particolare importanza in relazione: • ai costi di esercizio; • alla sostenibilità ambientale; • alla resilienza dei servizi pubblici digitali; • agli impatti sulle reti di trasmissione e distribuzione, in particolare in presenza di carichi concentrati, non programmabili o localizzati in aree non originariamente dimensionate per tali utilizzi.

Lo Stack IA: chip



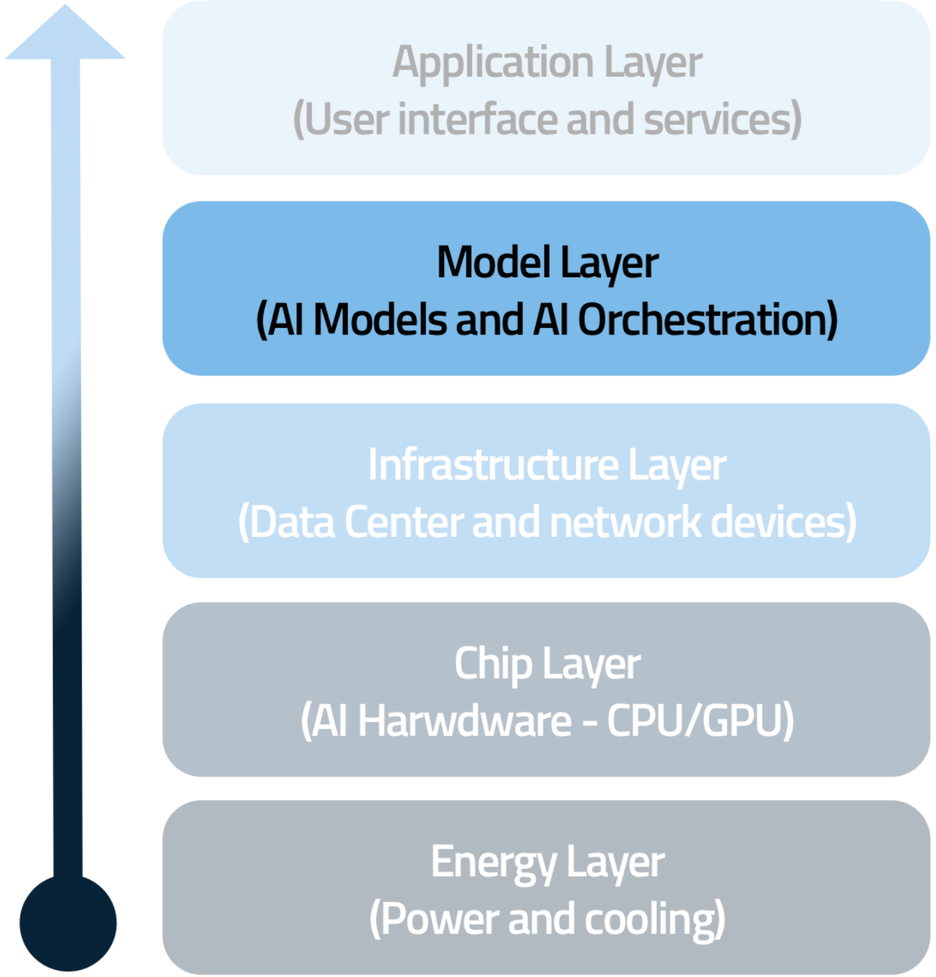
	Descrizione
Funzione	Comprende semiconduttori e acceleratori IA, le GPU (Graphics Processing Unit - particolarmente utili per l'addestramento e l'inferenza dei modelli di IA grazie alla loro architettura altamente parallela), le TPU (Tensor Processing Unit – nativamente progettati per utilizzo di IA per operazioni tensoriali e reti neurali), gli ASIC (Application-Specific Integrated Circuit - se progettati specificamente per compiti di IA sono in grado di ottimizzare i processi di inferenza); memorie HBM (High Bandwidth Memory).
Rilevanza	Le prestazioni dei modelli dipendono direttamente dalla potenza e dall'efficienza dell'hardware sottostante. La disponibilità di hardware tecnicamente avanzato abilita caratteristiche di scalabilità, produce tempi di calcolo ridotti e ottimizza i consumi energetici della computazione.
Componenti tipiche	GPU/TPU, acceleratori specifici per IA, CPU ad alte prestazioni, memorie, sistemi hardware ottimizzati per workload IA, hardware dedicato ad Edge IA.
Punti di attenzione	Le scelte relative a questo layer influenzano in modo significativo la portabilità dei modelli e le performance dei modelli di IA che si intende adottare.

Lo Stack IA: infrastruttura



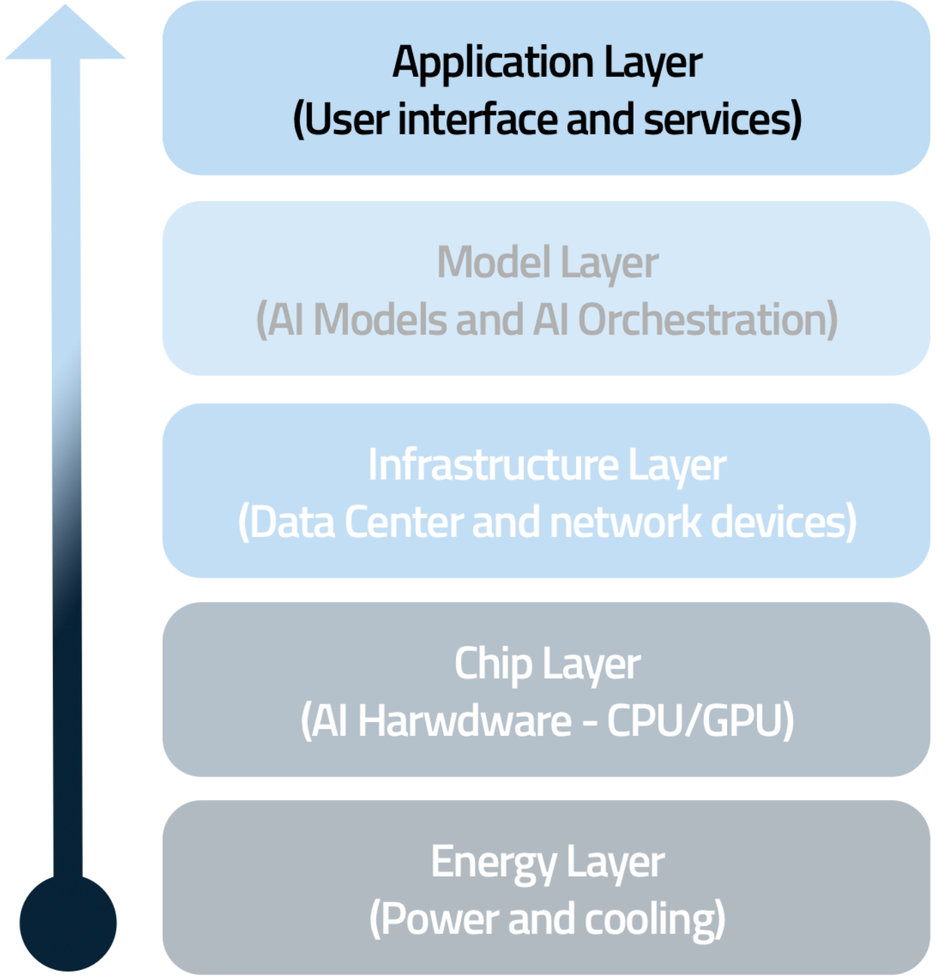
	Descrizione
Funzione	Include data center, reti, storage, sistemi di virtualizzazione, piattaforme cloud e servizi di orchestrazione che permettono di distribuire, scalare e gestire carichi di lavoro IA.
Rilevanza	Un'infrastruttura robusta garantisce disponibilità, sicurezza, continuità operativa, connettività ad alte prestazioni e gestione efficiente dei flussi dati necessari ai sistemi IA.
Componenti tipiche	Data center, cloud pubblico/privato/ibrido, container orchestration (es. piattaforma di orchestrazione di container che automatizza la distribuzione, la gestione e la scalabilità delle applicazioni), sistemi di storage distribuito, reti ad alta velocità, servizi di monitoraggio. Può comprendere Cluster di GPU; infrastrutture cloud-native; architetture di rete ad altissima velocità e bassa latenza; sistemi di storage parallelo per dataset di grandi dimensioni.
Punti di attenzione	È il layer su cui si innestano i requisiti di qualificazione cloud (Regolamento ACN n. 21007), sovranità del dato, resilienza e interoperabilità tra sistemi

Lo Stack IA: modeli



	Descrizione
Funzione	Comprende modelli di IA, framework di machine learning, pipeline di addestramento, strumenti per fine-tuning, valutazione, monitoraggio, orchestrazione dei modelli e inferenza.
Rilevanza	Questo livello rappresenta il “cuore logico” dell’IA: qui si sviluppano, addestrano, usano, monitorano e aggiornano i modelli che abilitano le funzionalità intelligenti delle applicazioni.
Componenti tipiche	Framework ML/DL, modelli fondamentali, dataset, strumenti e piattaforme di MLOps, sistemi di versioning di modelli e dati, strumenti di explainability e auditing, LLM, strumenti per addestramento distribuito.
Punti di attenzione	La PA deve considerare sia modelli sviluppati internamente sia modelli forniti da terzi, inclusi modelli general purpose. Le scelte su questo layer incidono su: • Correttezza e consistenza delle soluzioni realizzate; • qualità delle prestazioni; • gestione del rischio; • trasparenza e spiegabilità; • conformità normativa (es. AI Act e Legge 132/2025)

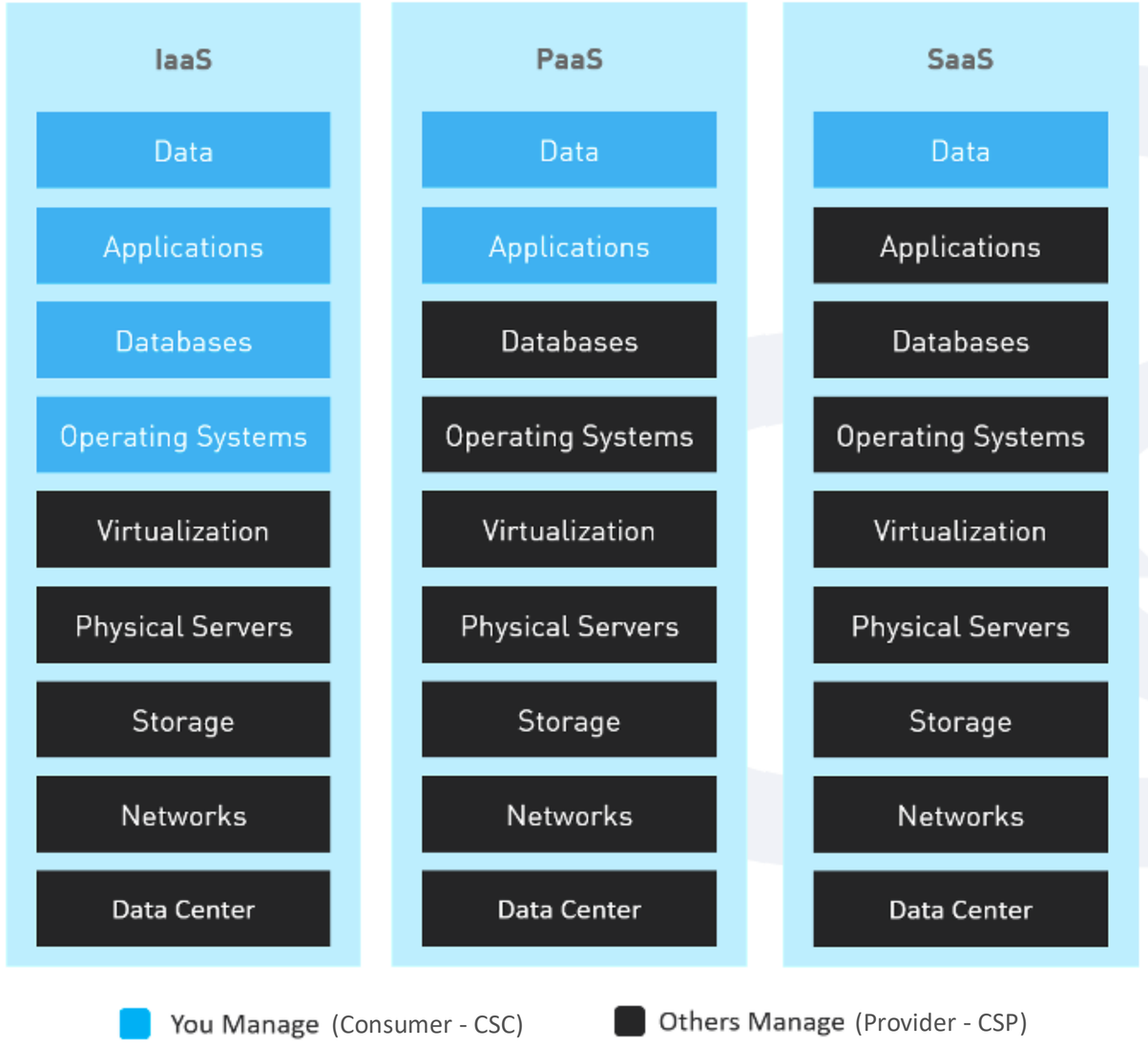
Lo Stack IA: applicazioni



	Descrizione
Funzione	Raggruppa applicazioni, servizi, interfacce e sistemi che integrano modelli IA per fornire funzionalità intelligenti a cittadini, operatori, dipendenti pubblici e imprese.
Rilevanza	È il livello in cui il valore dell'IA diventa tangibile: abilita automazione, supporto decisionale, analisi avanzate e servizi digitali intelligenti.
Componenti tipiche	API, applicazioni AI-based, soluzioni verticali per la PA, assistenti intelligenti, sistemi di automazione, dashboard e strumenti analitici. Assistenti conversazionali, sistemi di forecasting, strumenti per analisi predittiva, servizi digitali potenziati da IA.
Punti di attenzione	Questo layer deve essere progettato secondo i principi di centralità dell'utente, accessibilità, trasparenza e accountability.

Modello di shared responsability

Responsabilità		
Servizio	Provider - CSP	Consumer - CSC
SaaS	Il **Cloud Service Provider (CSP)** è responsabile della **quasi totalità degli aspetti di sicurezza**, inclusi **sicurezza perimetrale**, **registrazione, monitoraggio e controllo**, nonché la **sicurezza delle applicazioni**.	Il **Consumatore del servizio** mantiene un **ruolo limitato**, focalizzato principalmente sulla **gestione delle autorizzazioni**, dei **diritti di accesso** e delle **configurazioni utente**.
PaaS	Il **Cloud Service Provider (CSP)** è responsabile della **sicurezza della piattaforma**, inclusi **patching**, **configurazione di base** e protezione dei **servizi gestiti** (es. database come servizio).	Il **Consumatore del servizio** è responsabile di **tutto ciò che viene implementato sulla piattaforma**, comprese la **configurazione delle funzionalità di sicurezza offerte**, la **gestione degli account**, le **politiche di accesso** e i **meccanismi di autenticazione** utilizzati.
IaaS	Il **Cloud Service Provider (CSP)** è responsabile della **sicurezza di base dell'infrastruttura**, inclusa la **protezione perimetrale** e il **monitoraggio degli attacchi** sull'ambiente fisico e virtualizzato.	Il **Consumatore del servizio** è **pienamente responsabile della sicurezza di tutto ciò che costruisce sull'infrastruttura**, inclusa la **progettazione e configurazione della rete virtuale**, l'uso corretto degli **strumenti di sicurezza messi a disposizione dal servizio**, e la **protezione dei sistemi operativi e delle applicazioni**.

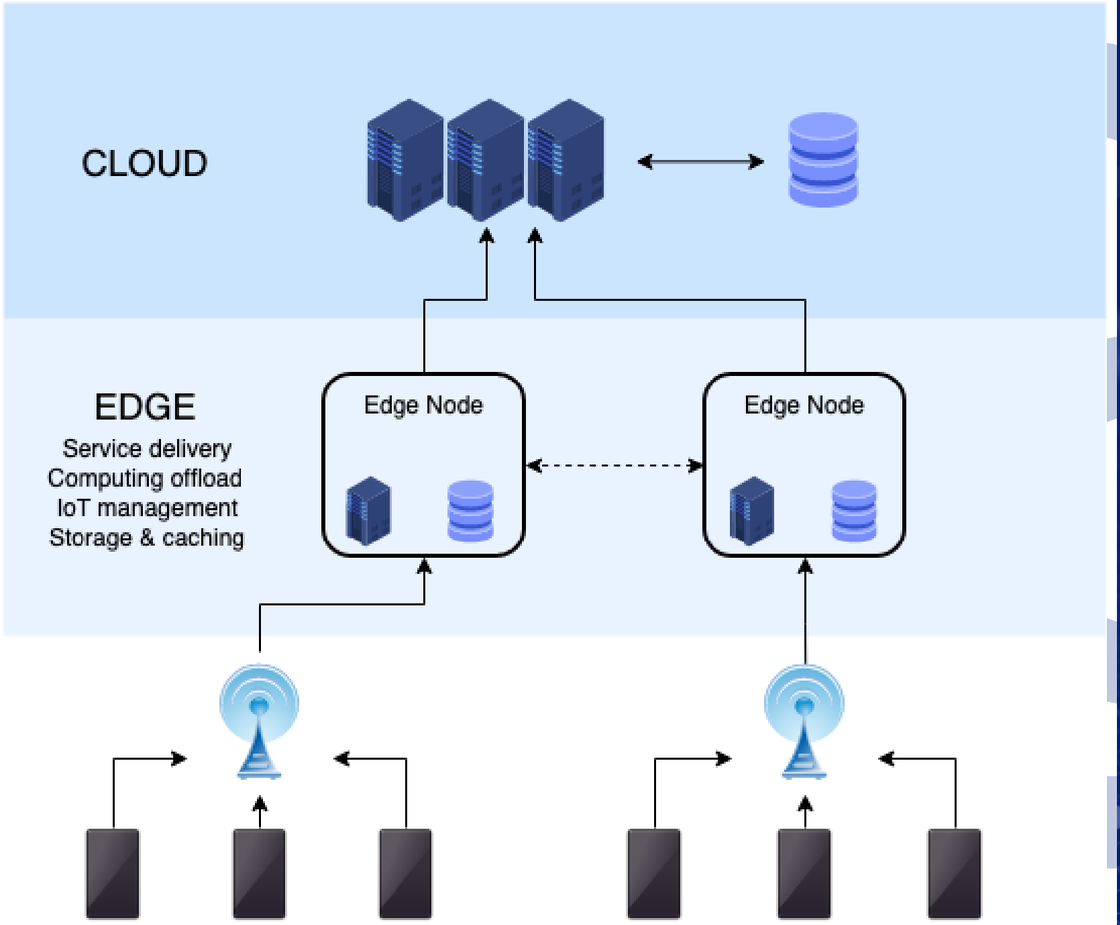


Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

Edge Computing

Modello di **computazione distribuita** che **sposta elaborazione e storage dei dati vicino alla loro sorgente**, riducendo la dipendenza dal cloud centralizzato.
Si integra nell'**architettura dei sistemi cloud** ed è utilizzato principalmente per **scenari che richiedono bassa latenza, continuità operativa e trattamento locale dei dati**, come **IoT, smart city, sanità, video analytics e applicazioni di intelligenza artificiale in tempo reale**.
Offre numerosi vantaggi:

- **Privacy e sicurezza** → i dati vengono elaborati localmente e si muovono meno
- **Affidabilità** → **ridondanza dei nodi** e maggiore resilienza del sistema
- **Velocità** → **computazione prossima al terminale**, con riduzione della latenza e migliore utilizzo della banda
- **Efficienza** → **livello intermedio tra cloud centrale e terminali**, che riduce il carico e l'utilizzo delle risorse dei data center



Wikipedia, https://en.wikipedia.org/wiki/Edge_computing

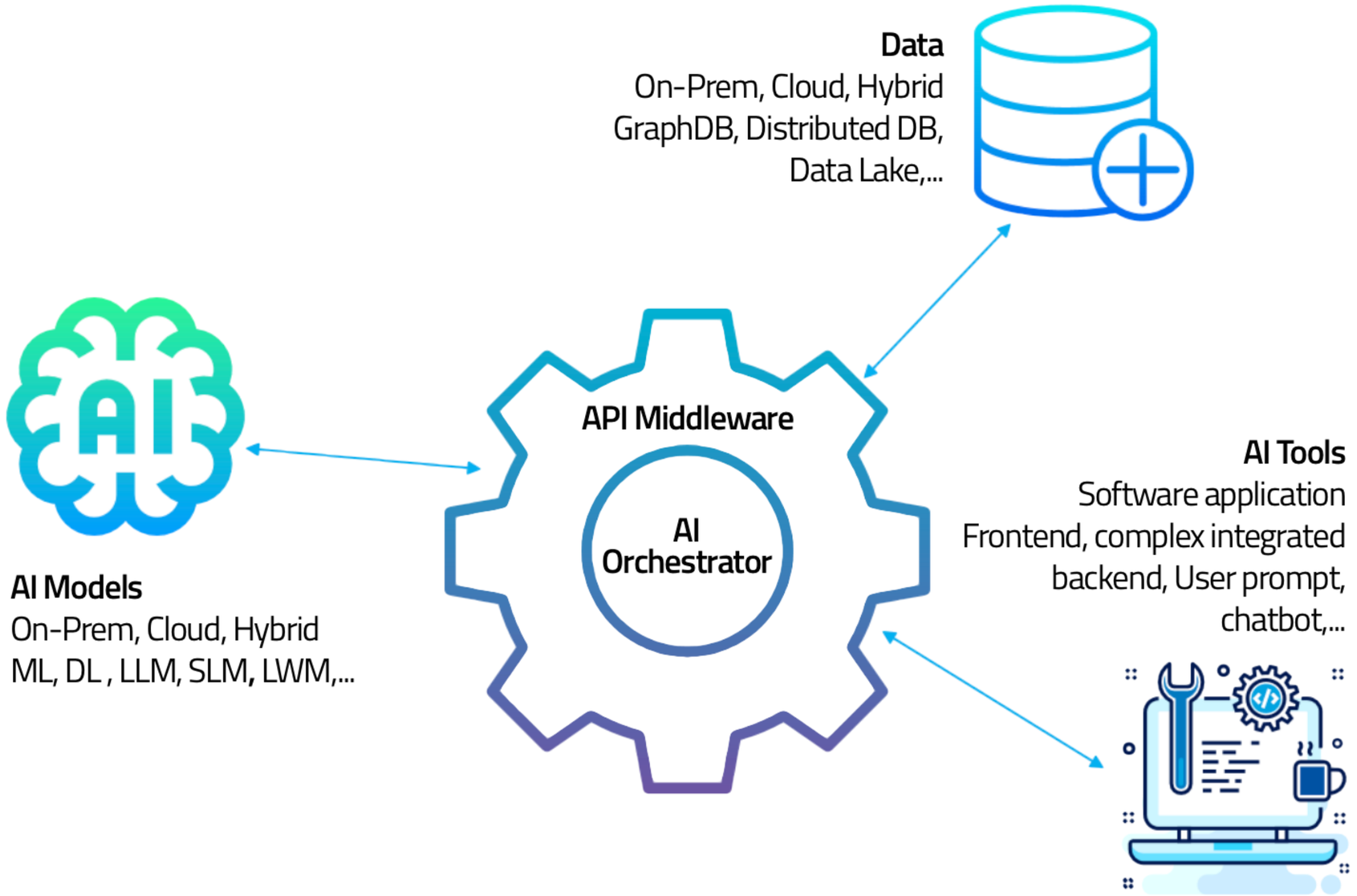
Confronto framework di sovranità cloud: EU CSF vs BSI C3A 1/2

Requisito	EU Cloud Sovereignty Framework	BSI C3A	Differenza chiave
Governance strategica	**SOV-1 · 15%** Ancoraggio al sistema legale, finanziario e industriale UE. Valuta stabilità della proprietà e allineamento alle priorità EU.	**SOV-1-01/02/03/04-C** Sede legale EU/DE, controllo effettivo da entità UE, notifica 90 gg anticipata per cambio controllo.	**[A] Più granulare nel BSI** C3A aggiunge criteri binari verificabili (sede, controllo, notifica). EU CSF valuta con scoring ponderato il grado di ancoraggio EU.
Giurisdizione legale	**SOV-2 · 10%** Esposizione a leggi extraterritoriali (CLOUD Act), diritti azionabili, proprietà intellettuale in EU.	**SOV-2-01/02/03-C** Analisi rischio annuale leggi extraterritoriali; diritto di audit da autorità nazionale; takeover in stato di difesa.	**[A] Più granulare nel BSI** C3A introduce stato di difesa (SOV-2-03-C) e audit esercitabili dall'autorità pubblica. EU CSF rimane a livello di contributing factors.
Sovranità dei dati / IA	**SOV-3 · 10%** Controllo esclusivo del cliente sulla chiave crittografica (BYOK), localizzazione EU, auditabilità modelli IA.	**SOV-3 Data Sovereignty** BYOK, localizzazione dati EU, cancellazione irreversibile verificabile, trasparenza accessi e log auditabili.	**[D] Convergenza** Allineamento elevato. C3A specifica criteri tecnici precisi. EU CSF include 'AI sovereignty' come dimensione esplicita; C3A la tratta implicitamente.
Sovranità operativa	**SOV-4 · 15%** Continuità operativa EU, portabilità workload, documentazione completa e codice sorgente, talenti EU disponibili.	**SOV-4-01…09-C** Disconnessione non-EU testata annualmente (SOV-4-09-C), personale EU, SOC EU, ridondanza con almeno 1 operatore EU.	**[E] Criteri verificabili BSI** C3A introduce disconnessione testata annualmente (SOV-4-09-C) assente nel EU CSF. EU CSF enfatizza exit capability senza test obbligatori.
Supply chain	**SOV-5 · 20% ★** Origine geografica HW/FW/SW, visibilità su tutta la catena, grado di dipendenza da vendor non-EU.	**SOV-5-01…-C** Mappatura componenti con paese di origine, piani di sostituzione per dipendenze critiche non-EU, SBOM.	**[D] Convergenza** Massima convergenza. BSI aggiunge SBOM e piani di sostituzione operativi; EU CSF assegna il peso più alto (20%) nel punteggio.

Confronto framework di sovranità cloud: EU CSF vs BSI C3A 2/2

Requisito	EU Cloud Sovereignty Framework	BSI C3A	Differenza chiave
Sovranità tecnologica	**SOV-6 · 15%** Standard aperti, open source auditabile, lock-in avoidance, indipendenza HPC/acceleratori EU.	**SOV-6-01…-C** Backup codice sorgente in EU, continuità servizio se dipendenze chiave disconnesse, standard aperti e portabilità.	**[A] Più granulare nel BSI** C3A aggiunge resilienza alla disconnessione come criterio esplicito. EU CSF include indipendenza HPC/acceleratori (IA) assente nel C3A.
Sicurezza & compliance	**SOV-7 · 10%** SOC EU, certificazioni ENISA/ISO, conformità GDPR/NIS2/DORA, operazioni sicurezza in giurisdizione EU.	**— non incluso —** Delegato a BSI C5:2026, IT-Grundschutz e HA Benchmark compact (prerequisiti del C3A).	**[B] Assente in C3A** Scelta deliberata BSI: SOV-7 è coperto da C5:2026, prerequisito obbligatorio del C3A. EU CSF lo integra con peso autonomo.
Sostenibilità ambientale	**SOV-8 · 5%** Efficienza energetica, dipendenza da risorse critiche, resilienza climatica a lungo termine.	**— non incluso —** Fuori dal perimetro di competenza BSI.	**[B] Assente in C3A** Scelta deliberata BSI: l'ambiente non rientra nella missione dell'autorità di sicurezza informatica. EU CSF include SOV-8 per autonomia strategica.
Meccanismo di valutazione	**SEAL 0–4 + Sovereignty Score** 5 livelli SEAL (0=nessuna sovranità → 4=sovranità completa). Punteggio ponderato come Award Criterion nelle gare.	**Criteri / Criteri aggiuntivi** Criteri obbligatori (MUST) e criteri aggiuntivi (opzionali per profilo di rischio). Conformità verificabile tramite audit BSI.	**[C] Solo EU: scoring** EU CSF è uno strumento di gara con punteggio graduato. C3A è un catalogo di criteri binari verificabili per audit; non prevede scoring comparabile.

Architettura agentica di riferimento



Fonte: Bozza di Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione – Consultazione pubblica

Livelli di autonomia in una architettura agentica

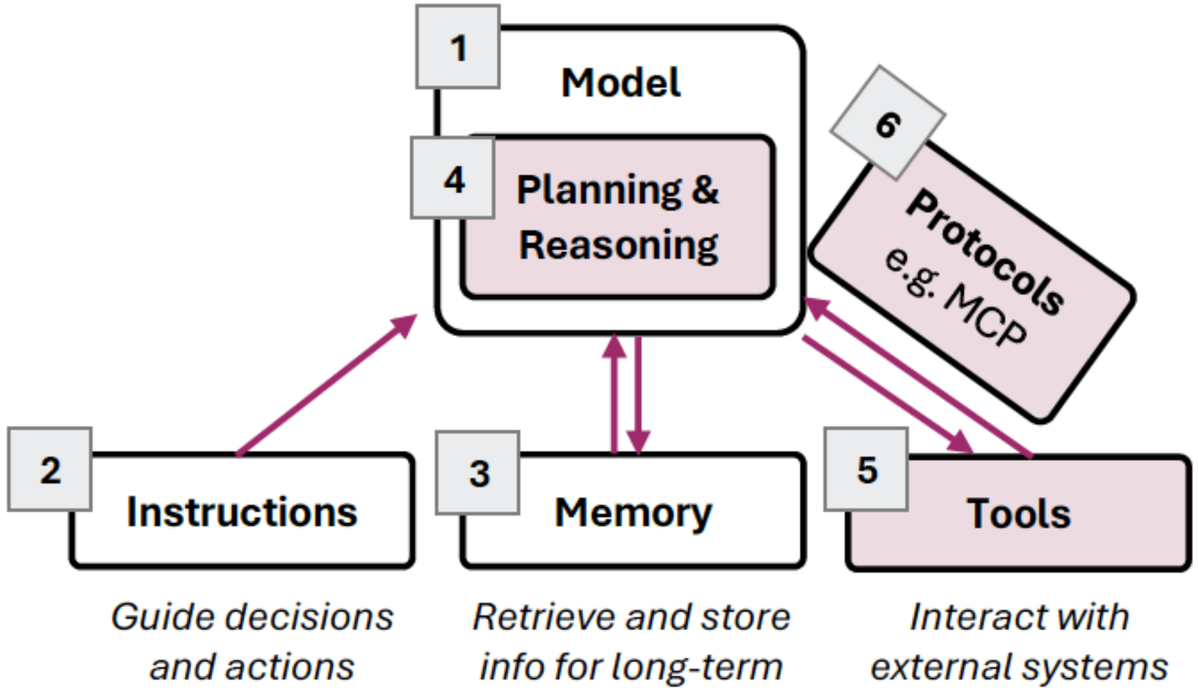
Livello	Cosa fa un agente	Analogia con i veicoli	Tecnologia	Applicazioni
Livello 0 completamente manuale	Nessuna automazione, l'umano esegue ogni attività	Guida manuale, nessuna assistenza	Strumenti digitali di base (fogli di calcolo, email), elaborazione manuale	Flussi di lavoro basati su carta/email, inserimento manuale dei dati, operazioni su fogli di calcolo
Livello 1 Automazione basata su regole	L'automazione semplice segue regole fisse (Robotic Process Automation - RPA, script)	Cruise control di base attivo, es. mantenimento della velocità	RPA, script, motori di regole	Instradamento delle email, StraightThrough Processing - STP dei pagamenti con elaborazione automatica end-to-end senza intervento umano, motori di regole antifrode
Livello 2 Automazione intelligente dei processi	Automazione + capacità cognitive (Machine Learning, Natural Language Processing, Computer Vision) con orchestrazione	Il sistema ADAS (Advanced Driver Assistance System) gestisce velocità e sterzo con supervisione	ML, NLP, CV, RPA, orchestrazione di processi	Estrazione delle fatture passive, triage dei reclami, assistenza al contact center
Livello 3 Workflow agentici	Gli agenti pianificano, ragionano, creano contenuti e si adattano all'interno di domini definiti	Navigazione automatica in autostrada; l'essere umano gestisce i casi limite	LLM, sistemi di memoria, uso di tool, Reinforcement Learning (RL) di base	Copilot (supporto/codice/marketing), analisti RAG, ETL (Extract, Transform, Load) automatizzati. Ambienti di esercizio supervisionati, progetti pilota
Livello 4 Agenti semi-autonomi	Gli agenti agiscono in modo autonomo entro ambiti di competenza delimitati; adattano le strategie e apprendono	La guida avviene in modalità autonoma in condizioni specifiche	Ragionamento e pianificazione avanzati, adattamento in tempo reale, ragionamento causale	Taxi senza conducente, robotica di magazzino, droni per ispezioni, auto-remediation AIOps. Ambienti di esercizio limitati in ambienti vincolati
Livello 5 Agenti completamente autonomi	Apprendimento cross-dominio e auto-adattamento senza intervento umano	Le auto completamente autonome guidano ovunque e in tutte le condizioni	Sistemi di memoria sofisticati, meccanismi di apprendimento avanzati, safety automation	Nessuna sperimentazione, solo attività di ricerca

PRINCIPI PER LO SVILUPPO DELL'INTELLIGENZA ARTIFICIALE

APPROFONDIMENTI

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

Componenti principali di un agente IA



Componenti principali di un agente basato su LLM

1. Model. Motore centrale (SLM, LLM o MLLM) che svolge funzioni di **ragionamento e pianificazione**, elaborando input e generando risposte contestuali.

2. Instructions Comandi in linguaggio naturale che definiscono **ruolo, capacità e vincoli comportamentali** dell'agente (es. system prompt).

3. Memory. Sistema di **memorizzazione e recupero delle informazioni**, a breve o lungo termine, incluse interazioni precedenti o dati esterni.

Componenti avanzate dell'agente

4. Planning & Reasoning

Capacità del modello di **scomporre i compiti in step** e pianificare le azioni necessarie.

5. Tools Strumenti che consentono all'agente di **interagire con sistemi esterni** (database, API, file, dispositivi, transazioni).

6. Protocols. Standard che regolano la **comunicazione tra agenti e strumenti** (es. MCP, A2A), garantendo interoperabilità.

Fonte: IMDA MODEL AI GOVERNANCE FRAMEWORK FOR AGENTIC AI, Version 1.0, 22 January 2026

Neutralità hardware e portabilità dei sistemi di I

- Sistemi di IA → elevato fabbisogno computazionale
- Uso crescente di acceleratori (GPU, TPU, ecc.)
- Rischio: integrazione verticale → dipendenza tecnologica

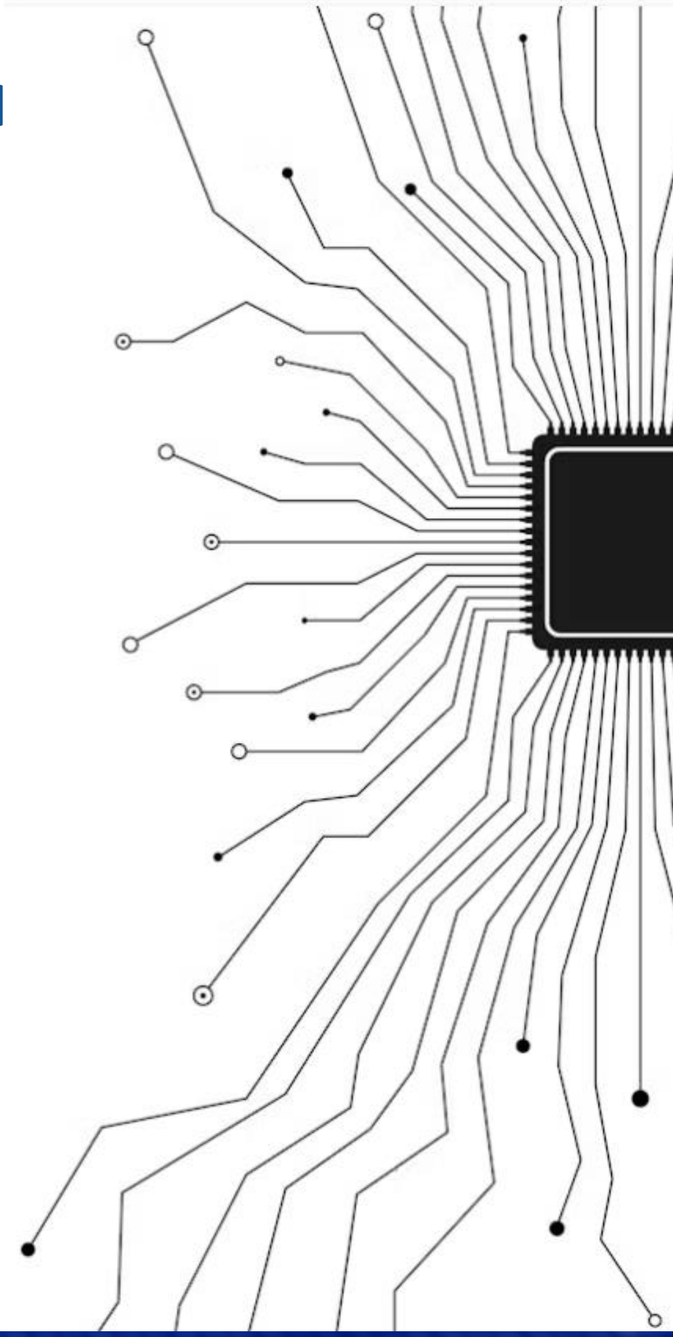
👉 Obiettivo: **garantire flessibilità, portabilità e sostenibilità**

Integrazione hardware-software-servizi

- Soluzioni altamente integrate
- Dipendenza da specifici vendor
- Limitazioni operative nel lungo periodo

Rischi per la PA:

- Difficoltà di migrazione
- Scarsa adattabilità a contesti diversi
- Ridotto utilizzo di infrastrutture pubbliche/locali



Architetture hardware-agnostic

Definizione

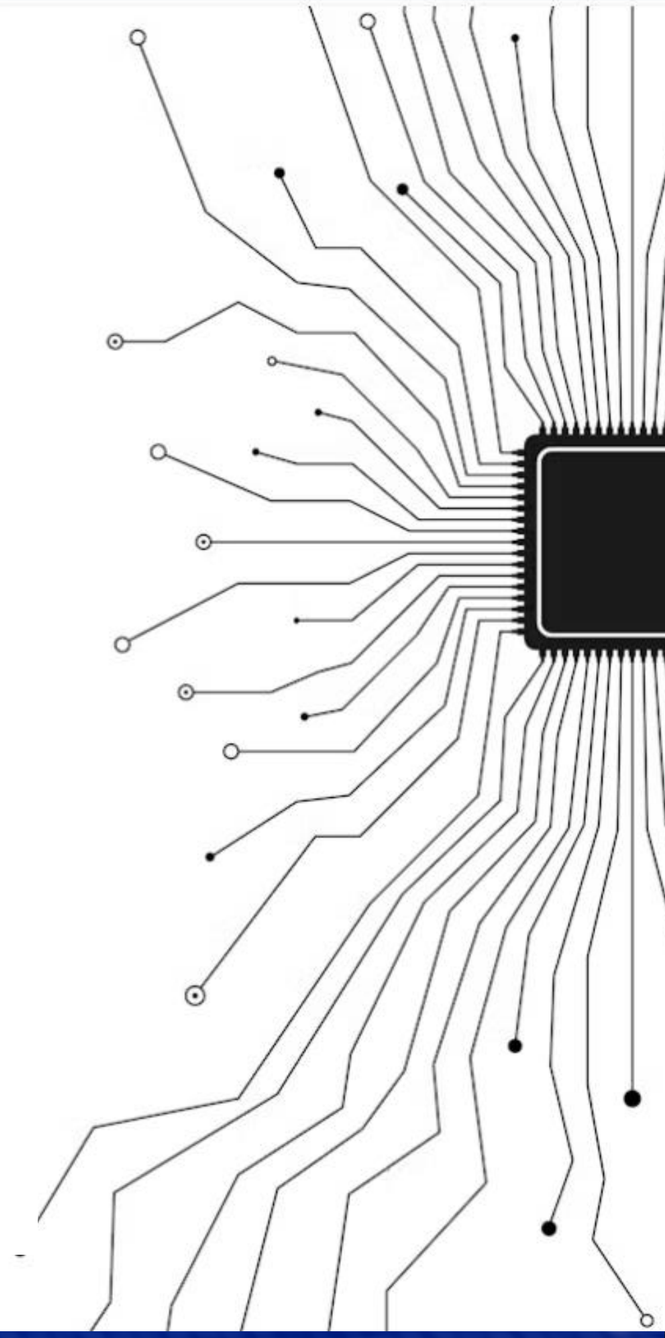
- Separazione tra:
  - modello di IA
  - logica applicativa
  - infrastruttura hardware

Vantaggi:

- Esecuzione su ambienti diversi
- Riduzione dipendenze tecnologiche
- Maggiore flessibilità operativa

⚠ Senza acceleratori:

- prestazioni ↓
- ma sistema comunque utilizzabile



Ottimizzazione dei modelli

Tecniche principali

- Riduzione dimensione del modello (pruning)
- Quantizzazione (precisione ridotta)
- Distillazione del modello

Risultato:

- Minore fabbisogno computazionale
- Possibile esecuzione su CPU

👉 Benefici:

- Riduzione costi
- Maggiore diffusione dei sistemi IA

Esecuzione su CPU general-purpose

- Maggiore accessibilità infrastrutturale
- Riduzione consumo energetico
- Maggiore indipendenza tecnologica

👉 Non sempre massime prestazioni, ma: **maggiore resilienza e sostenibilità**

Clausole contrattuali

Neutralità hardware

Il sistema:

- DEVE essere eseguibile su infrastrutture eterogenee
- NON DEVE dipendere da specifici acceleratori o tecnologie proprietarie

Portabilità e reversibilità

Il sistema:

- DEVE poter essere migrato tra infrastrutture diverse
- DEVE evitare vincoli strutturali verso un fornitore

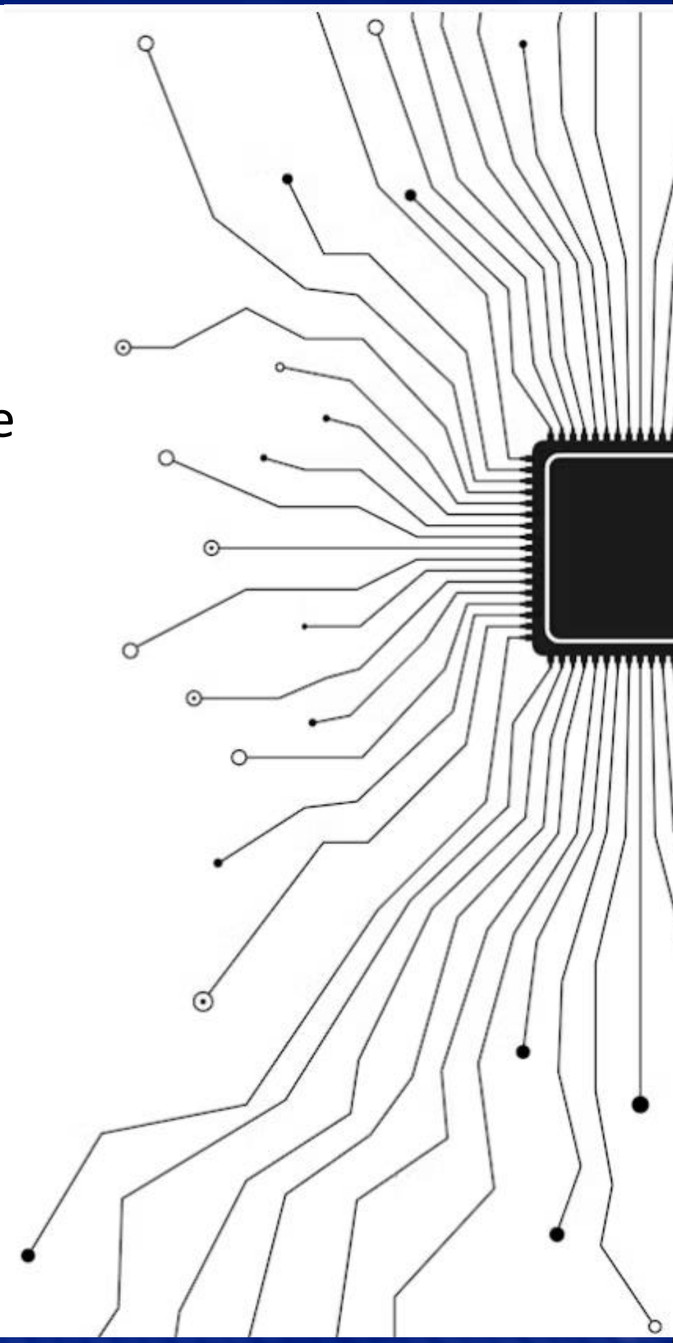
👉 Garantire continuità e libertà tecnologica

Efficienza e fallback CPU

Il sistema:

- DEVE prevedere modalità CPU-only
- DEVE utilizzare tecniche di ottimizzazione

👉 Obiettivo: continuità operativa, livelli di servizio adeguati



Riduzione dimensione del modello: pruning

Il pruning è una tecnica di ottimizzazione che consiste nella **rimozione selettiva di componenti non rilevanti** di un modello di IA al fine di ridurne la complessità computazionale.

Obiettivo

- Ridurre dimensione e peso del modello
- Migliorare efficienza computazionale
- Abilitare esecuzione su hardware meno performante

Tipologie principali

- **Pruning non strutturato** → rimozione di singoli pesi
- **Pruning strutturato** → rimozione: neuroni, filtri, layer

Strumenti più diffusi (open source)

- PyTorch (es. *torch.nn.utils.prune*)
- TensorFlow Model Optimization Toolkit
- Transformers (Hugging Face)
- ONNX / OpenVINO (ottimizzazione e deployment)

Risultato

- Modello più leggero
- Minori costi energetici
- Maggiore portabilità

👉 **Tecnica chiave per sistemi di IA sostenibili e interoperabili**

Pruning su Llama-3.2 (1B / 3B)

Applicazione di **pruning strutturato** sui layer MLP (GLU) dei modelli Llama per ridurre la complessità mantenendo prestazioni elevate.

Strumenti utilizzati: PyTorch, Transformers (Hugging Face), Tecniche di pruning strutturato + fine-tuning

Parametri di riduzione

- Riduzione fino a **40–60%** dei neuroni nei layer MLP
- Miglioramento dell'efficienza energetica (≈ **-20% per token**)
- Riduzione del fabbisogno computazionale

Impatto sulla velocità di inferenza

- **Prima del pruning: ~ 120–180 ms** per richiesta (prompt breve, CPU/GPU leggera)
- **Dopo il pruning: ~ 80–120 ms**

👉 Riduzione della latenza fino a circa **30–40%**

Metodo

1. Analisi importanza neuroni
2. Pruning strutturato (MLP)
3. Fine-tuning
4. Validazione su benchmark

Implicazioni hardware e infrastrutturali

👉 Dopo pruning, il modello può essere eseguito su: **CPU general-purpose** (es. Intel Xeon / AMD EPYC), **GPU leggere o mid-range** (es. NVIDIA T4 / NVIDIA L4)

Esempio: Hugging Face https://huggingface.co/papers/2512.22671

Quantizzazione

La quantizzazione è una tecnica di ottimizzazione che consiste nella **riduzione della precisione numerica dei parametri** di un modello di IA (es. da 32-bit a 8-bit o 4-bit), al fine di ridurne il fabbisogno computazionale.

Obiettivo

- Ridurre dimensione del modello
- Diminuire consumo di memoria
- Migliorare efficienza energetica
- Abilitare esecuzione su hardware meno performante

Tipologie principali

- **Post-training quantization** → applicata dopo l'addestramento
- **Quantization-aware training (QAT)** → integrata durante l'addestramento

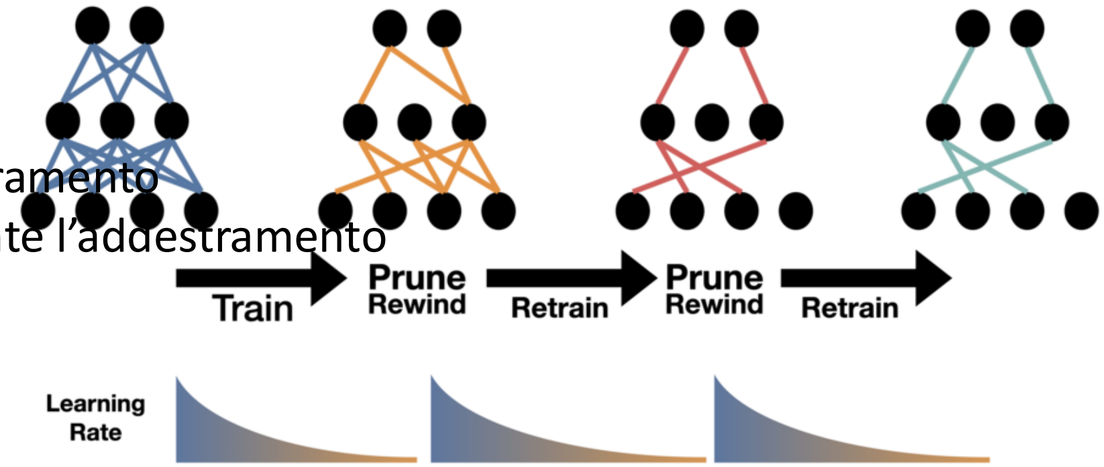
Strumenti più diffusi (open source)

- PyTorch (quantization API)
- TensorFlow Lite
- Transformers (Hugging Face) (es. bitsandbytes)
- ONNX / OpenVINO

Risultato

- Modello più compatto (fino a -75% memoria)
- Maggiore velocità di inferenza
- Possibile esecuzione su CPU o edge

👉 **Tecnica chiave per l'efficienza e la portabilità dei sistemi IA**



Esempio: A foolproof way to shrink deep learning models (MIT News)

Distillazione

La distillazione è una tecnica di ottimizzazione che consiste nel **trasferire la conoscenza da un modello complesso (teacher)** a un **modello più piccolo e leggero (student)**.

Obiettivo

- Ridurre dimensione e complessità del modello
- Mantenere prestazioni elevate
- Abilitare deployment su infrastrutture meno performanti

Come funziona

- Il modello teacher genera output “ricchi” (soft labels)
- Il modello student viene addestrato per imitarne il comportamento

👉 Il modello student apprende **pattern e generalizzazioni** del modello grande

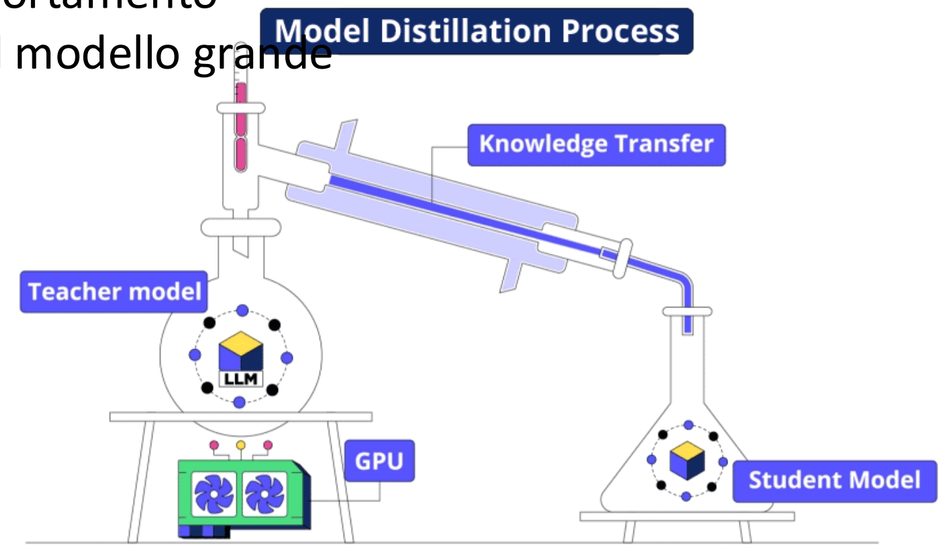
Strumenti più diffusi (open source)

- PyTorch
- TensorFlow
- Transformers (Hugging Face)

Risultato

- Modello più compatto
- Prestazioni comparabili
- Maggiore efficienza computazionale

👉 **Tecnica chiave per scalabilità e sostenibilità dei sistemi IA**



Fonte: Afef Belhadj

FINANCIAL TIMES
WEDNESDAY 25 FEBRUARY 2026
USA $3.00

India's pivot from US to 'middle powers'
BIG READ, PAGE 15

The growing dangers of flattering Trump
EDWARD LUCE, PAGE 17

Anthropic hits at China rivals for 'attacks' on its AI models

- Three labs blasted by Claude maker
- National security concerns raised

ELEANOR OLCOTT — BEIJING
CRISTINA CRIDDLE — SAN FRANCISCO

Anthropic has accused three leading Chinese AI labs of "industrial-scale" the Chinese Communist Party, to close the competitive advantage that export controls are designed to preserve through other means," said Anthropic.

Briefing

Anthropic accuses China rivals of rampant cheating
The AI start-up has accused three Chinese labs of "industrial-scale" attacks, raising national security concerns. It says they are using "distillation" — training smaller models on the outputs of more advanced systems.— PAGE 6

DeepSeek
Over 150,000 exchanges
Moonshot AI
Over 3.4 million exchanges
MiniMax
Over 13 million exchanges

Research | Economic Futures | Commitments | Learn | News | Try Claude

Detecting and preventing distillation attacks

23 feb 2026

Esempio: distillazione task-specifica da Claude 1/3

Caso d'uso

Ottenere un modello «piccolo» che faccia:

- classificazione di PEC o documenti amministrativi
- estrazione campi da atti
- sintesi breve di testi normativi
- risposta standardizzata su FAQ interne

Invece di usare sempre Claude in produzione, si utilizza Claude **solo nella fase di creazione dataset** e poi si addestra uno student open source più leggero.

Pipeline

1. Definizione del task

Esempio: "dato un documento, assegna una delle 8 categorie amministrative e restituisci una motivazione di 2 righe".

2. Costruzione del dataset

Si raccolgono 5.000–20.000 esempi reali o anonimizzati:

- input: testo del documento
- output atteso: categoria, breve rationale, eventuali campi strutturati

3. Utilizzo di Claude come teacher

Per ogni input, si chiede a Claude un output strutturato, per esempio:

Esempio: distillazione task-specifica da Claude 2/3

Classifica il seguente documento in una delle categorie:
[appalto, personale, tributi, edilizia, privacy, protocollo, contabilità, altro]
Restituisci JSON con:
- categoria
- *confidenza 0-1*
- *motivazione di massimo 40 parole*

Poi si esegue la **revisione umana** su un campione o sull'intero dataset, a seconda del rischio del caso d'uso.

4. Preparazione del dataset student

Si tiene solo ciò che serve davvero:

- input
- output finale corretto
- magari niente "ragionamento interno", solo etichette e testo finale

5. Si sceglie come student un modello piccolo.

Per esempio:

- un encoder leggero per classificazione
- un piccolo modello instruction-tuned open source per estrazione/sintesi

6. Fine-tuning dello student

Si addestra il modello sui dati prodotti e verificati.

Esempio: distillazione task-specifica da Claude 1/3

7. Valutazione

Si confronta:

- accuratezza
- latenza
- costo per inferenza
- robustezza su casi nuovi

8. Deploy

Si utilizza lo student in produzione e Claude solo come fallback.

Task	Student consigliato
Classificazione documenti	DistilBERT / MiniLM
Estrazione dati	MiniLM / TinyBERT
Chatbot leggero	Llama 1B / Phi
Sintesi testi	Llama 1B / Mistral 7B
Edge / CPU-only	Phi-3 Mini / Gemma 2B

Il modello student deve essere scelto in funzione del **task** e dei **vincoli infrastrutturali**, privilegiando **modelli compatti open source** per garantire **efficienza**, **portabilità** e **autonomia tecnologica**.

Modelli di IA per finalità generali

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

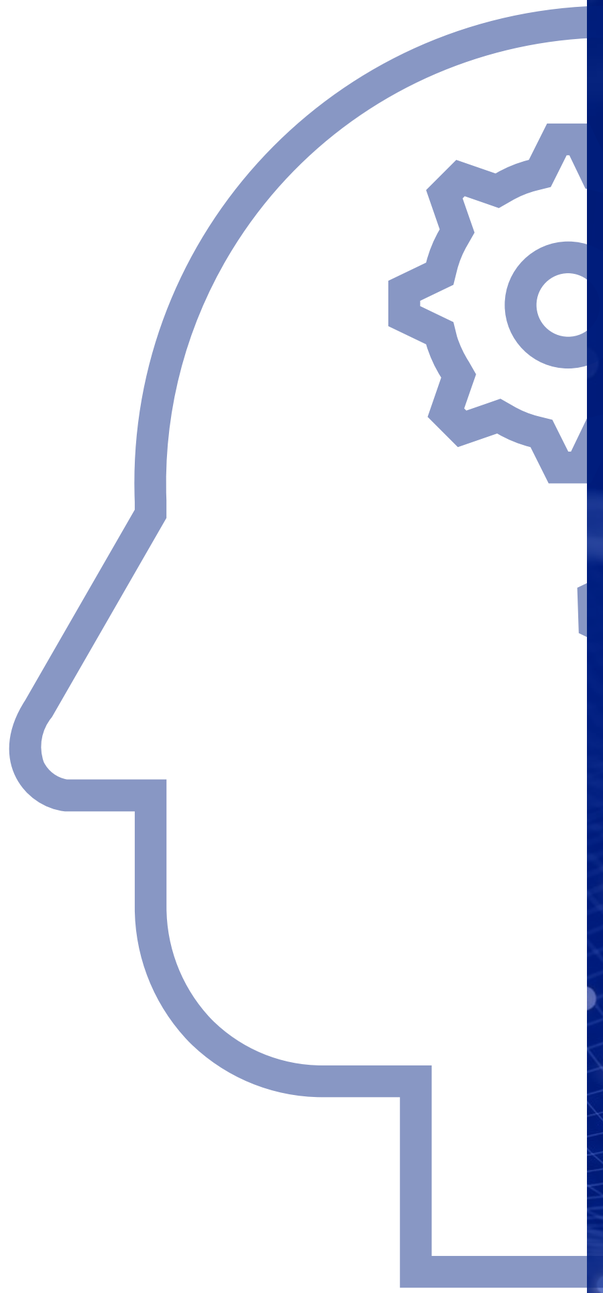
GPAI a rischio sistemico

L'**Articolo 51** dell'AI Act introduce, per la prima volta in una normativa europea, il concetto di **rischio sistemico** riferito ai sistemi di intelligenza artificiale.

- Esso viene attribuito ai **modelli di IA che, per scala, capacità, autonomia o potenziale di impatto, potrebbero rappresentare una minaccia per la salute, la sicurezza pubblica o i diritti fondamentali**, **anche in assenza di un utilizzo intenzionalmente illecito**.

- La valutazione del rischio sistemico si applica in particolare ai **sistemi di IA di uso generale (GPAI)**, e comporta l'obbligo di notifica e meccanismi di monitoraggio rafforzati.

L'**Articolo 56** dell'AI Act prevede lo sviluppo di uno o più **Codici di Condotta** per i fornitori e i sviluppatori di GPAI, con l'obiettivo di garantire l'**adozione volontaria** di **misure per la sicurezza, la trasparenza, la responsabilità e la protezione dei diritti fondamentali.**



GPAI code of practice

Transparency

Dettaglio delle informazioni da fornire da parte dei fornitori di modelli di IA di uso generale a:

- **Fornitori a valle**, secondo l'**Allegato XII** dell'AI Act
- **AI Office e autorità nazionali competenti**, secondo l'**Allegato XI** dell'AI Act

Copyright

Supportare i fornitori nell'**adozione di politiche adeguate** per garantire la **conformità al diritto d'autore dell'UE**.

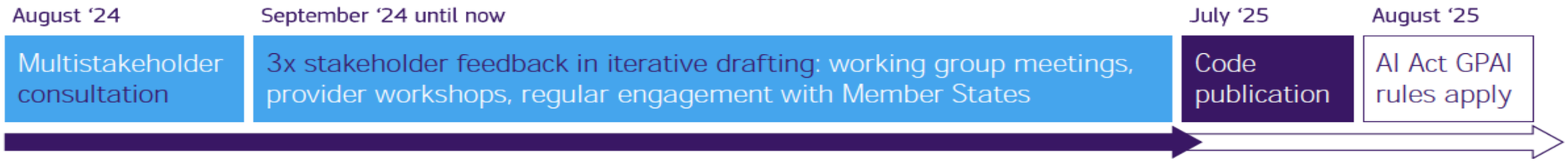
Safety & Security

Fornire indicazioni pratiche ai fornitori di **modelli di IA di uso generale con rischio sistemico** su come:

- **Valutare il rischio sistemico**
- **Mitigare il rischio sistemico** tramite misure tecniche e governance interna

Per tutti i fornitori di modelli GPAI

GPAI con rischio sistemico

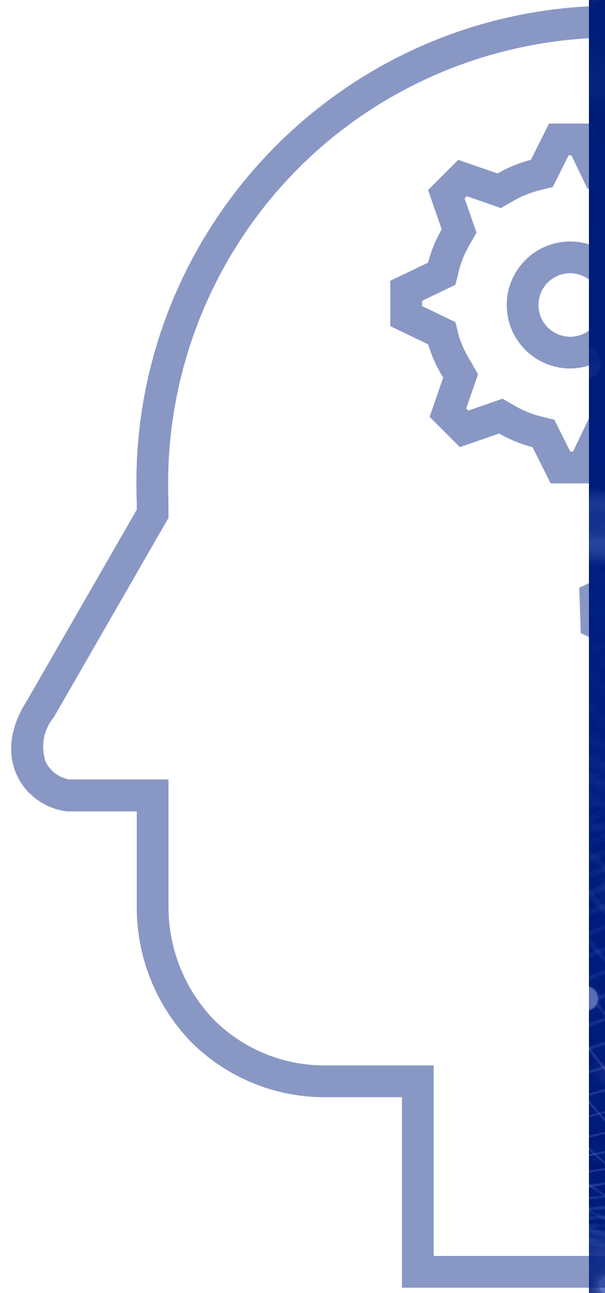


Le safety policy delle AI Company

Le principali aziende tecnologiche IA stanno sviluppando autonomamente **policy di sicurezza** per i cosiddetti **modelli IA di frontiera** assimilabili ai modelli GPAI dell'AI Act.

Questo approccio riflette una forma di **autoregolamentazione**, motivata sia da **pressioni reputazionali** che dal desiderio di **anticipare o influenzare future normative statali.**

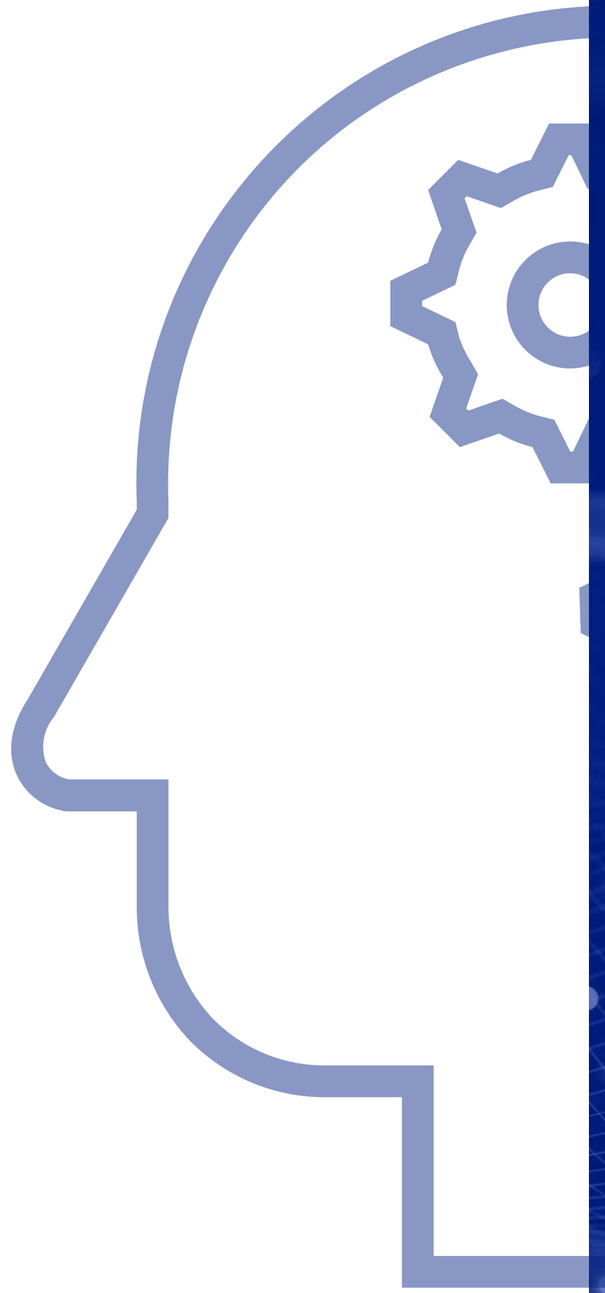
- Anthropic – *Responsible Scaling Policy*
- OpenAI – *Preparedness Framework*
- Google DeepMind – *Frontier Safety Framework*
- Magic – *AGI Readiness Policy*
- Naver – *AI Safety Framework*
- Meta – *Frontier AI Framework*
- G42 – *Frontier AI Safety Framework*
- Cohere – *Secure AI Frontier Model Framework*
- Microsoft – *Frontier Governance Framework*
- Amazon – *Frontier Model Safety Framework*
- xAI – (Draft) *Risk Management Framework*
- Nvidia – *Frontier AI Risk Assessment*



Fonte: METR. Common Elements of Frontier AI Safety Policies, 2025.

Le safety policy delle AI Company

- **Soglie di capacità** (*Capability Thresholds*): livelli prestabiliti di capacità che, se superati, richiedono l'adozione di nuove misure di mitigazione (Vedi Minacce contemplate).
- **Sicurezza dei pesi** (*Model Weight Security*): misure di sicurezza informatica per proteggere i pesi dei modelli da accessi non autorizzati.
- **Mitigazioni del deployment** (*Model Deployment Mitigations*): limitazioni e controlli per prevenire l'uso improprio di capacità pericolose.
- **Condizioni per fermare il deployment**: impegni a sospendere il rilascio se non è possibile implementare mitigazioni adeguate.
- **Condizioni per fermare lo sviluppo**: analoghi impegni in fase di sviluppo in presenza di capacità critiche emergenti.
- **Elicitazione completa delle capacità**: valutazioni progettate per identificare l'intero spettro delle capacità del modello.
- **Tempistiche delle valutazioni**: definizione chiara dei momenti in cui eseguire le valutazioni (pre-training, durante il training, post-deployment).
- **Accountability**: meccanismi di supervisione interna ed esterna per monitorare l'attuazione delle policy.
- **Aggiornamento delle policy**: impegni a revisionare periodicamente le policy alla luce di nuovi dati o rischi emergenti.



Fonte: METR. Common Elements of Frontier AI Safety Policies, 2025.

Minacce contemplate

Modello di Minaccia	Numero di Policy e Aziende
Biological weapons assistance. CBRN (armi chimiche, biologiche, radiologiche e nucleari): rischio che i modelli AI facilitino lo sviluppo di armi di distruzione di massa	9: Anthropic, OpenAI, Google DeepMind, Magic, Meta, G42, Microsoft, Amazon, xAI
Cyberoffense. Cybersecurity / Operazioni Cibernetiche / Offesa Cibernetica: utilizzo dell'AI per attacchi informatici contro infrastrutture critiche o sistemi digitali	10: Anthropic, OpenAI, Google DeepMind, Magic, Meta, G42, Microsoft, Amazon, xAI, Nvidia
Ricerca e Sviluppo Autonoma (AI R&D): capacità dei modelli di accelerare la ricerca tecnologica senza supervisione umana	8: Anthropic, OpenAI, Google DeepMind, Magic, Microsoft, Amazon, Nvidia, xAI
Replica / Autonomia del Modello: capacità dei modelli di auto-replicarsi e auto-deployarsi senza controllo esterno	5: OpenAI, Magic, Google DeepMind, Microsoft, xAI
Persuasione / Manipolazione: rischio che i modelli influenzino il comportamento umano su larga scala (es. disinformazione o interferenze elettorali)	3: OpenAI, Nvidia, Meta
Allineamento Ingannevole: rischio che l'AI inganni i suoi sviluppatori mascherando comportamenti pericolosi	1: Google DeepMind
Perdita di controllo: rischio che i modelli sfuggano al controllo degli operatori umani (fitness)	2: Naver, xAI
Uso malevolo / output dannosi: produzione di contenuti illegali, discriminatori o tecnicamente dannosi (es. malware)	2: Cohere, xAI
Discriminazione illegale: rischio che l'AI generi contenuti che comportano discriminazioni vietate dalla legge	2: Cohere, Nvidia

Fonte: METR. Common Elements of Frontier AI Safety Policies, 2025.

PRINCIPI PER IL PROCUREMENT DELL'INTELLIGENZA ARTIFICIALE

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

Metriche, costi e gestione del procurement IA 1/2

Valutazione economica dei sistemi di IA nella PA

Programmazione → Gara → Esecuzione → Monitoraggio

Obiettivo

👉 Fornire un **quadro metodologico** per:

- valutare costi e sostenibilità
- confrontare soluzioni alternative
- governare l'intero ciclo di procurement

Cambio di paradigma

❌ Approccio tradizionale

→ costo iniziale / breve periodo

✅ Approccio lifecycle (LCOAI)

→ costi lungo tutto il ciclo di vita

→ modelli a consumo e dinamici

Elementi chiave

📊 Valutazione economica continua

⚖️ Comparabilità tra soluzioni

⚠️ Integrazione con gestione del rischio

🏛️ Coerenza con principi di economicità ed efficacia

Metriche, costi e gestione del procurement IA 2/2

Ambito di applicazione

✓ Tutti i sistemi di IA:

- LLM
- Machine learning
- IA tradizionale
- Sistemi agentici

✓ Tutti i modelli di deployment:

- API / SaaS
- Cloud
- On-premise
- Ibrido

Valore per la PA

- Decisioni più consapevoli
- Basi d’asta realistiche
- Controllo dei costi nel tempo
- Continuità dei servizi

La valutazione economica dell’IA è un processo continuo di ciclo di vita, non una stima iniziale di costo.

Limiti degli approcci economici tradizionali 1/2

Metriche parziali e rischio decisionale

Costo token/API | Costo tempo di computazione | TCO

❌ ❌ ⚠️

Problema principale

Le metriche tradizionali **non rappresentano il costo reale dei sistemi di IA**

- Misurano il **consumo tecnologico**
- Non riflettono il **valore del servizio**
- Trascurano componenti critiche

Cosa NON considerano

- Integrazione con sistemi esistenti
- Gestione e qualità dei dati
- Orchestrazione e gestione operativa
- Sicurezza e compliance normativa
- Governance e controllo

Limiti degli approcci economici tradizionali 2/2

Criticità strutturali

- 📉 Costi variabili e difficili da prevedere
- ⚖️ Scarsa comparabilità tra soluzioni
- 🔄 Interdipendenza tra scelte architetturali e costi
- ⏳ Distribuzione temporale dei costi non considerata

Limiti del TCO

- Non standardizzato → difficile confronto
- Non lega costi a output/valore
- Non adatto a modelli a consumo

🏛️ **Rischio per la PA**

Decisioni basate su metriche parziali →
soluzioni apparentemente economiche ma strutturalmente onerose

Le metriche tradizionali misurano il costo della tecnologia,
non il costo reale del servizio IA.

Levelized Cost of Artificial Intelligence (LCOAI) 1/2

Dal costo parziale al costo di ciclo di vita

$$LCOAI = \frac{CAPEX + OPEX}{Output}$$

CAPEX = costi di investimento (infrastruttura, setup, sviluppo)
OPEX = costi operativi (API, energia, manutenzione, gestione)
Output = inferenze valide / servizi erogati

$$LCOAI = \frac{Costo\ totale\ di\ ciclo\ di\ vita}{Numero\ di\ inferenze\ valide\ o\ servizi\ erogati}$$

Supera metriche parziali (token, API, compute)
Integra costi fissi e variabili
Tiene conto della sostenibilità nel tempo

Levelized Cost of Artificial Intelligence (LCOAI) 2/2

Abilita:

⚖️ Confronto tra soluzioni diverse:

- API (pay-per-use)
- Cloud dedicato
- Self-hosted
- Ibrido

📊 Decisioni basate sul valore prodotto

🔍 Maggiore trasparenza economica

Valore per la PA

💰 Migliore programmazione degli investimenti

🔄 Controllo dei costi nel tempo

🚫 Riduzione del lock-in economico

📈 Scelte di procurement più consapevoli

Il LCOAI collega il costo sostenuto al valore generato, rendendo confrontabili strategie tecnologiche diverse

Monitoraggio del sistema IA in esercizio 1/2

Dal procurement al controllo continuo

Sistema IA in esercizio
↓
Prestazioni | Costi | Qualità
↓
Monitoraggio continuo

Perché è essenziale

👉 La sostenibilità economica NON si valuta solo all'affidamento
👉 Dipende dal comportamento reale del sistema nel tempo

Cosa monitorare:

📊 **Conformità ai requisiti**
- livelli di servizio (SLA)
- qualità delle prestazioni
- coerenza con il contratto

⚠️ **Anomalie**
- scostamenti di performance
- comportamenti inattesi
- variazioni dei costi

Monitoraggio del sistema IA in esercizio 2/2

Strumenti e governance

- Indicatori misurabili (KPI)
- Raccolta dati strutturata
- Ruoli chiari (RUP + strutture operative)
- Coinvolgimento dei processi amministrativi

Azioni correttive

In caso di scostamenti:

- Ottimizzazione del modello
- Revisione configurazioni
- Adeguamento livelli di servizio
- Rinegoziazione contrattuale

Valore per la PA

- Controllo della spesa nel tempo
- Migliore qualità del servizio
- Maggiore affidabilità e governance
- Continuità operativa garantita

Il monitoraggio continuo è un presidio essenziale per garantire performance, costi sotto controllo e qualità dei sistemi di IA.

Componenti di costo dei sistemi di IA (LCOAI) 1/3

Visione completa dei costi

CAPEX + OPEX
(iniziali) (ricorrenti)
↓
Costi organizzativi
↓
Costi di uscita/transizione
↓
LCOAI

CAPEX — Spese di investimento

Costi iniziali (asset durevoli) 👉 Impatto elevato nella fase iniziale

- Infrastruttura di calcolo e data center
- Storage on-premise
- Integrazione sistemi e pipeline dati
- Setup e fine-tuning modelli
- Sicurezza, audit e compliance
- Avviamento del servizio

Componenti di costo dei sistemi di IA (LCOAI) 2/3

OPEX — Spese operative 👉 Determinano la sostenibilità nel tempo

Costi ricorrenti e variabili

- Inferenza e consumo computazionale
- Cloud, storage e rete
- Monitoraggio e manutenzione
- Aggiornamento modelli
- Canoni software e personale

Costi organizzativi

Capacità di governo del sistema

- Formazione e competenze
- Governance e processi
- Change management

Costi di uscita e transizione

Flessibilità e rischio lock-in

- Migrazione dati
- Re-ingegnerizzazione integrazioni
- Sostituzione modelli - Dismissione infrastrutture

Valore per la PA

- 💰 Basi d'asta più realistiche
- 📉 Riduzione del rischio di sottostima
- 🔒 Maggiore controllo e flessibilità

Una valutazione completa deve includere tutte le componenti di costo, non solo CAPEX e OPEX.

Componenti di costo dei sistemi di IA (LCOAI) 3/3

COSTO DI CICLO DI VITA DEL SISTEMA DI IA

(Life-Cycle Cost)

CAPEX

Spese in conto capitale

- Acquisizione o predisposizione dell'infrastruttura di calcolo
- Realizzazione o potenziamento di data center
- Acquisto di licenze perpetue
- Sviluppo di piattaforme proprietarie
- Investimenti iniziali per la messa in esercizio quando capitalizzabili secondo principi contabili

COMPONENTI IBRIDE

Alcuni costi possono assumere natura di **investimento oppure di servizio**, a seconda del modello di erogazione (on-premises, cloud o ibrido) e della struttura contrattuale adottata. Rientrano tra questi:

- Storage
- Aggiornamento dei modelli
- Progettazione dei flussi di dati
- Integrazione applicativa

OPEX

Spese operative ricorrenti

- Consumo di risorse computazionali ed energetiche
- Servizi cloud e piattaforme AI erogate a consumo
- Monitoraggio operativo
- Manutenzione correttiva ed evolutiva
- Supporto specialistico e aggiornamento modelli
- Adeguamenti normativi e compliance

Output produttivo e misurabilità (LCOAI) 1/2

Misurare il valore prodotto dall'IA

Costo totale (CAPEX + OPEX)
↓
Output misurabile
↓
LCOAI

Principio chiave

👉 Il costo deve essere rapportato a un **output produttivo chiaro e misurabile**

Unità di output (esempi)

- 💬 Risposte generate (chatbot, assistenti)
- ⚖️ Decisioni supportate o raccomandazioni
- 📈 Classificazioni e previsioni
- 🏛️ Servizi erogati a cittadini e imprese

Output produttivo e misurabilità (LCOAI) 2/2

Requisiti dell'output

✓ Misurabile
✓ Verificabile
✓ Coerente con il servizio erogato

⚠️ **Cosa escludere**

- Processi interni non finalizzati al servizio
- Attività tecniche non direttamente produttive

👉 Evitare distorsioni nella valutazione economica

Valore per la PA

📊 Migliore comparabilità tra soluzioni
⚖️ Valutazione basata sul servizio, non sulla tecnologia
💰 Decisioni più trasparenti e oggettive

L'IA si valuta in base al valore prodotto, non al consumo tecnologico.

Applicazione del LCOAI nel ciclo di procurement 1/2

LCOAI come metrica trasversale

Programmazione → Progettazione → Affidamento → Contratto → Esecuzione

1. Programmazione

- 📊 Valutazione ex ante della sostenibilità
- 💰 Pianificazione pluriennale delle risorse
- ⚠️ Riduzione rischio sottostima costi

2. Progettazione

- ⚖️ Confronto tra architetture (API, cloud, on-prem)
- 💰 Definizione basi d’asta realistiche
- 🎯 Allineamento costi–requisiti

3. Affidamento

- 📈 Valutazione dell’offerta economicamente più vantaggiosa
- 🔍 Trasparenza dei costi e sostenibilità nel tempo
- ⚖️ Focus su valore, non solo prezzo iniziale

Applicazione del LCOAI nel ciclo di procurement 2/2

4. Stipula del contratto

- Allineamento tra modello economico e clausole
- Meccanismi di pricing e revisione
- Indicatori economici da monitorare

5. Esecuzione

- Monitoraggio costi reali vs stime
- Gestione scostamenti e costi variabili
- Azioni correttive e piani di fallback

Valore per la PA

- Migliore gestione delle risorse pubbliche
- Decisioni più informate e trasparenti
- Riduzione del rischio di lock-in
- Sostenibilità nel medio-lungo periodo

Il LCOAI accompagna tutto il ciclo di procurement, garantendo coerenza tra scelte tecnologiche, costi e valore generato.

Confronto delle strategie di deployment dei sistemi di IA ai fini del procurement

Strategia di deployment	Struttura dei costi (LCOAI)	Livello di controllo della PA	Prevedibilità della spesa	Rischio di lock-in	Contesti di maggiore idoneità
Soluzioni basate su API	CAPEX molto ridotti; OPEX variabili e legati al consumo	Limitato	Media–bassa	Medio–alto	Fabbisogni incerti, sperimentazioni, servizi a domanda variabile
Cloud-hosted	CAPEX contenuti; OPEX strutturati ma scalabili	Intermedio	Media	Medio	Servizi con crescita progressiva, necessità di flessibilità
Self-hosted	CAPEX elevati; OPEX più stabili nel tempo	Elevato	Alta	Basso–medio	Contesti ad alta sicurezza, sovranità del dato e dei modelli, volumi prevedibili
Architetture ibride	Mix CAPEX/OPEX ottimizzabile	Elevato (se ben progettate)	Media–alta	Variabile	Sistemi complessi, integrazione con asset esistenti, esigenze differenziate

Impatti dell’approccio «ciclo di vita» e LCOAI sul procurement

APPROCCIO DI CICLO DI VITA + LCOAI

TRASPARENZA

- Esplicitazione delle determinanti di costo
- Maggiore motivabilità delle scelte
- Basi d'asta più realistiche

RESPONSABILITÀ

- Decisioni basate su analisi complete
- Migliore rendicontabilità della spesa
- Controllo della spesa

SOSTENIBILITÀ

- Investimenti compatibili con le capacità dell'ente
- Riduzione del rischio di soluzioni non sostenibili
- Continuità operativa nel medio-lungo periodo

MIGLIORAMENTO DEL PROCUREMENT

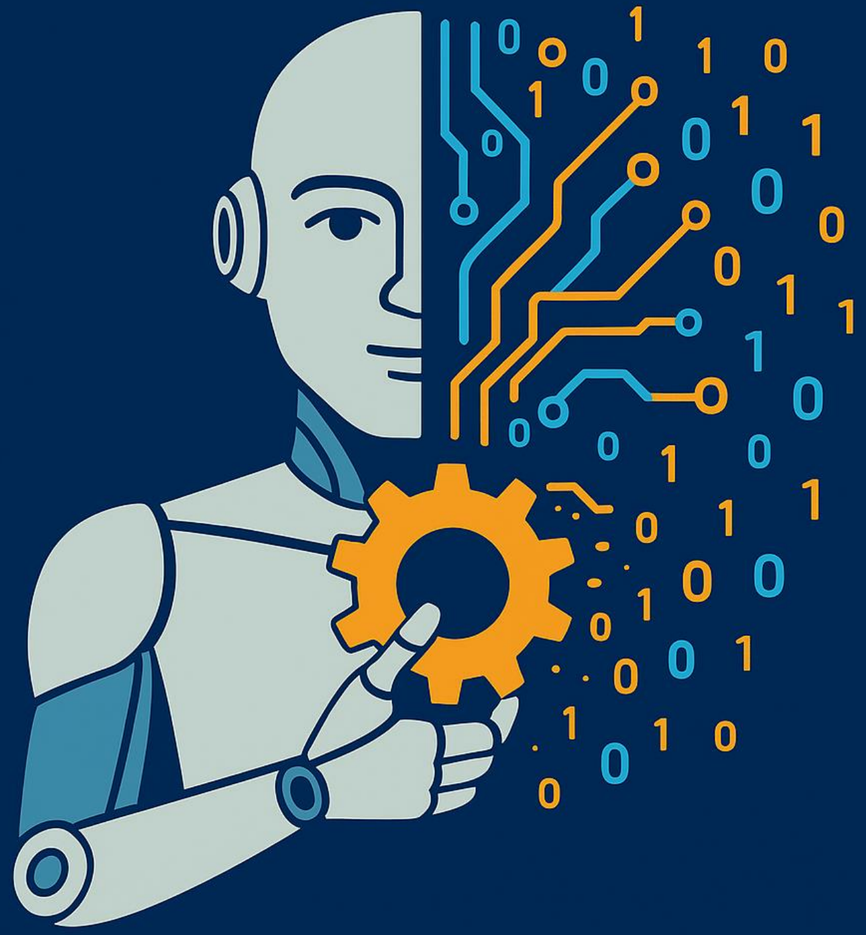
- ✔ Dialogo più equilibrato con il mercato
- ✔ Maggiore comparabilità delle offerte
- ✔ Riduzione del rischio di lock-in
- ✔ Negoziazioni più consapevoli
- ✔ Monitoraggio economico in fase di esecuzione

DECISIONI PUBBLICHE PIÙ INFORMATE E SOSTENIBILI

INTELLIGENZA ARTIFICIALE COME STRUMENTO E RUOLO DELL'INGEGNERE

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com

Automazione e riuso

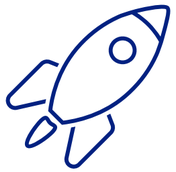


L’IA trasforma lo sviluppo software in un processo cognitivo e adattivo

Ing. Fabio Massimi

I progetti software verso un approccio cognitivo e adattivo

IA per lo sviluppo software. Algoritmi di *machine learning* e agenti intelligenti supportano analisi, progettazione, testing e manutenzione, migliorando qualità e velocità dei processi.



IA come potenziatore. L'IA non sostituisce il lavoro umano, ma lo amplifica, automatizzando attività ripetitive e fornendo raccomandazioni basate su dati e metriche reali.

IA per la governance. L'IA consente di creare ecosistemi digitali auto-miglioranti, dove l'IA diventa un alleato strategico per la qualità, la sicurezza e la sostenibilità dei sistemi complessi.

IA per la produttività. L'IA riduce drasticamente tempi e costi di sviluppo, moltiplica la produttività. Impatto significativo sulla valutazione di congruità tecnico-economica.

Riuso – Qualità – Sicurezza - Efficienza

“rivoluzione industriale” del software

Metrica	Dati US 2024*	Tendenza*	Applicazione dell’IA
Produttività	~8 FP/mese per persona	+750 %	Automazione delle fasi di progettazione, generazione del codice e test grazie a modelli e agenti IA
Defect Removal Efficiency (DRE)	~92,5 %	+7 % assoluti	Validazione automatica, analisi predittiva e test generati da IA riducono gli errori residui
Difetti consegnati	~0,30 per FP	–97 %	Uso di componenti riusabili certificati e revisione automatica del codice
Percentuale di riuso	~10 %	+75 %	Creazione di librerie di componenti intelligenti e modulari, certificati e sicuri
Progetti cancellati	~35 %	–97 %	Migliore pianificazione, stime più accurate e supporto decisionale basato su dati
Sforamenti di tempi e costi	~75 % dei progetti	–97 %	Previsione dei rischi e ottimizzazione delle risorse tramite IA predittiva
Costo per punto funzione (sviluppo)	~$1.000	–87 %	Riduzione dei tempi di sviluppo e del lavoro manuale

*Dati IFPUG International Function Points Users Group

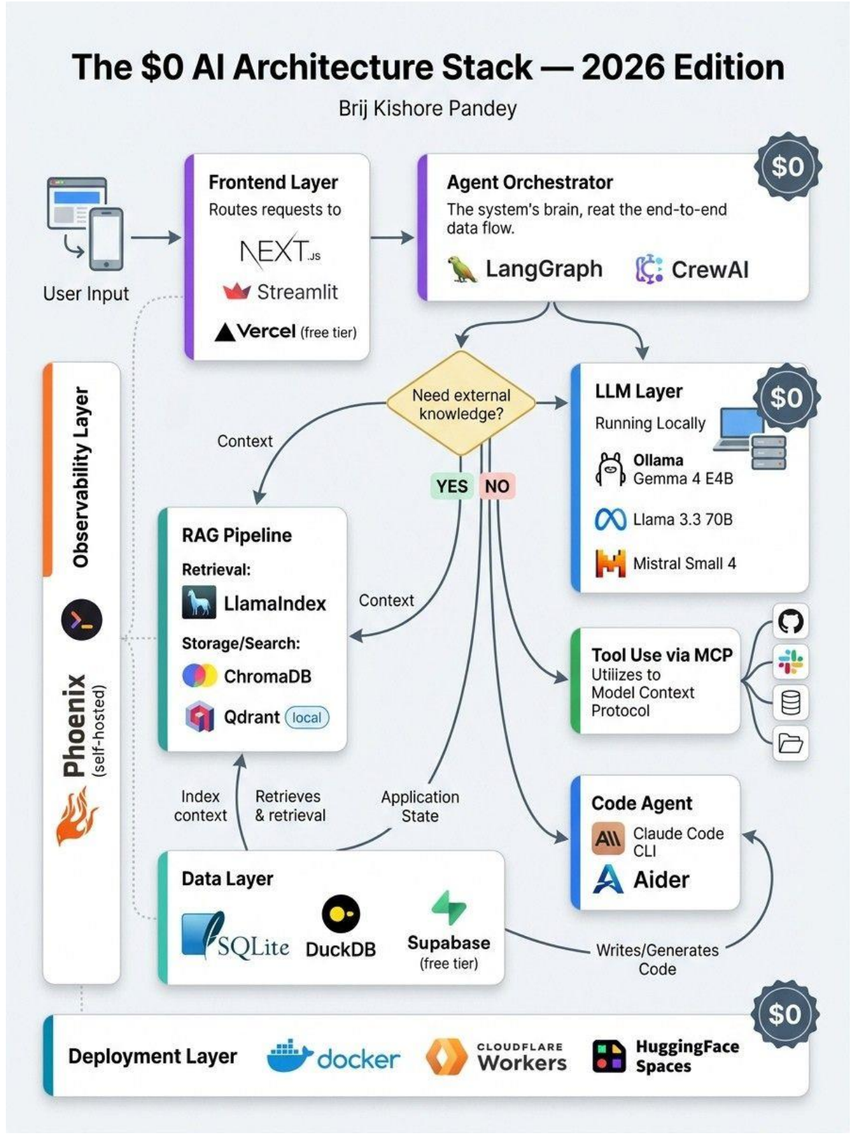
IA e riuso di componenti certificati

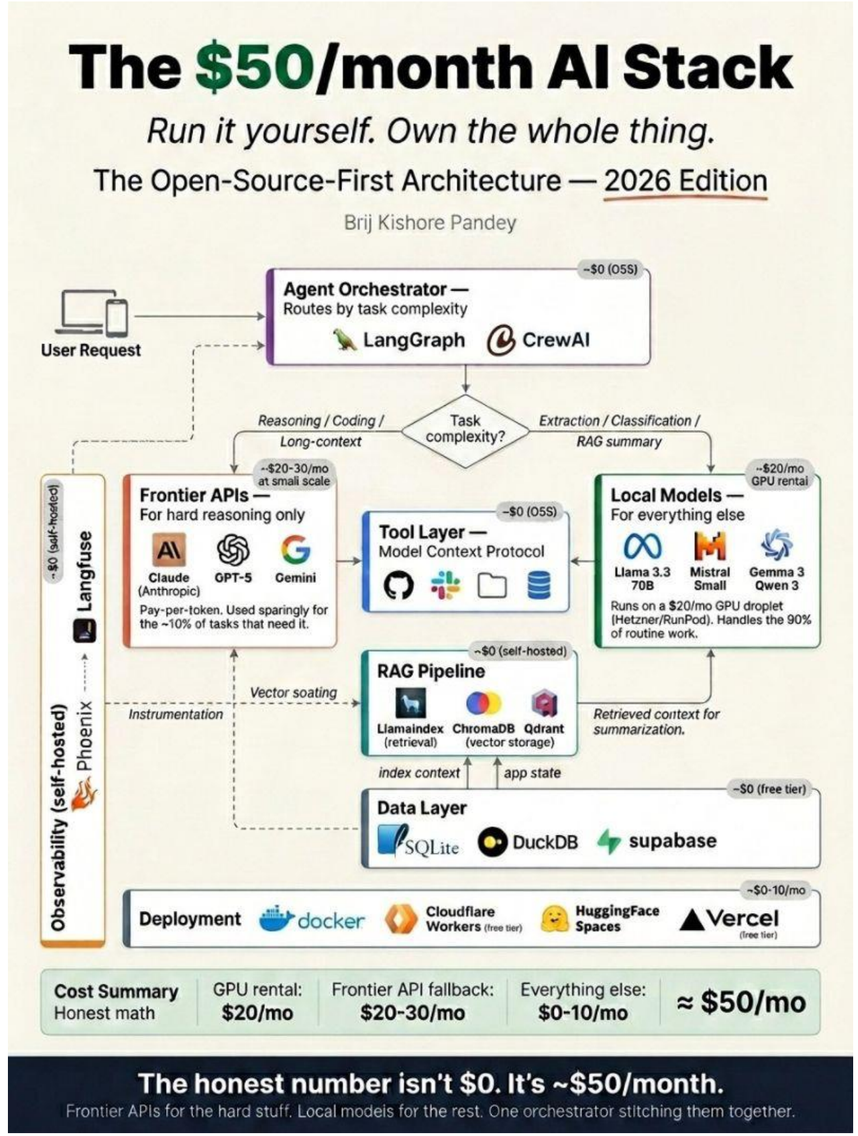
Sviluppare software come si costruiscono automobili: assemblando **componenti certificati riusabili**, **generati** e **orchestrati** da sistemi di Intelligenza Artificiale.

Riuso:
non solo codice

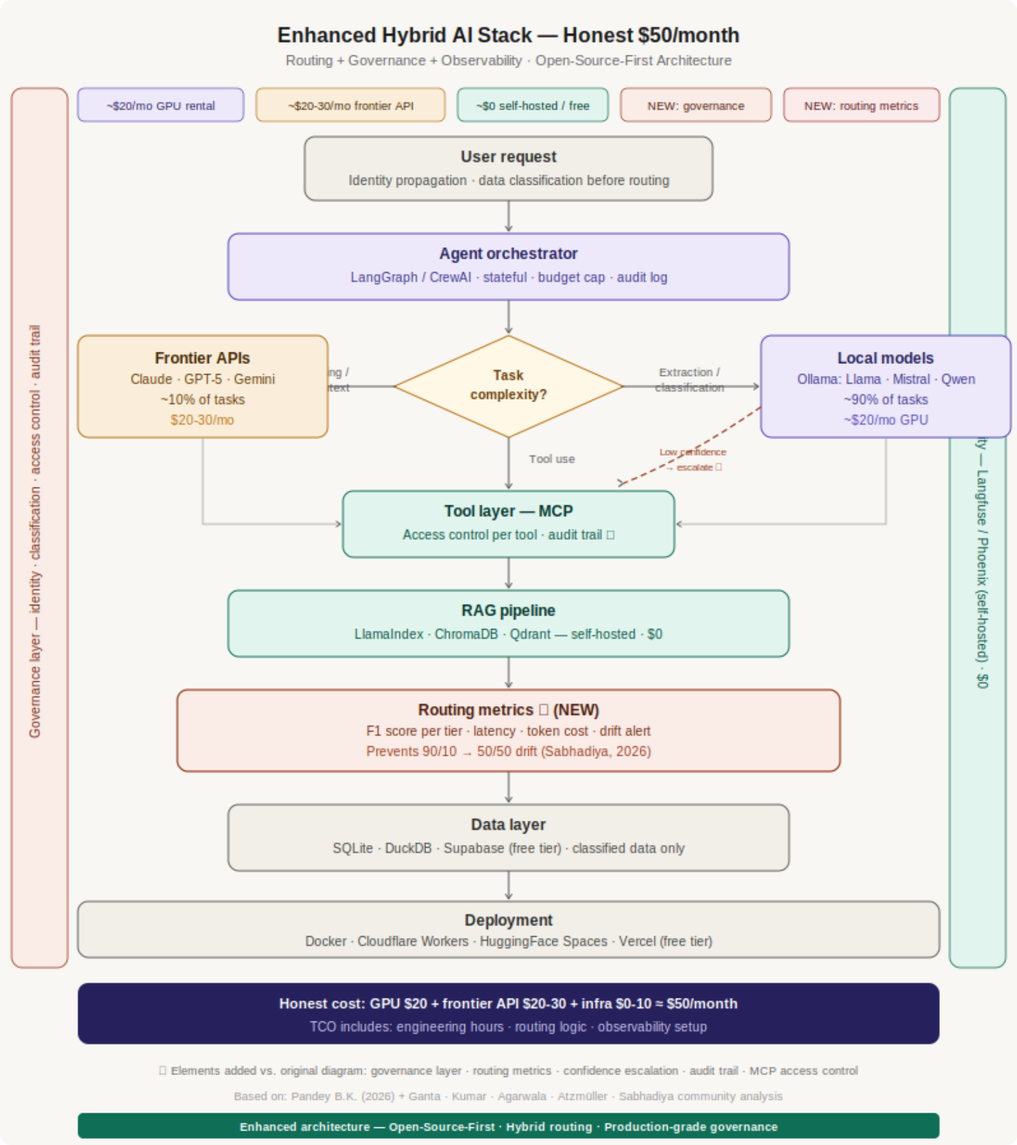
Tipologia	Esempi
Requisiti e architetture	Use cases, modelli di dominio
Design e piani di progetto	Diagrammi, WBS, stime, baseline
Codice e test	Classi, script, bugs, test case automatizzati
Documentazione e formazione	Manuali utente, HELP, materiali di training
Supporto e manutenzione	Piani di customer support, patch management

Lo stack IA autonomo: scelte architetturali e costi reali





Enhanced Hybrid AI Stack



- **Governance layer trasversale** (identity propagation, classificazione dei dati prima del routing, access control per singolo tool MCP, audit log delle chiamate)
- **Confidence-based escalation**: default su modello locale, escalation automatica verso il tier frontier quando la confidence scende sotto soglia — in alternativa alla classificazione upfront della complessità
- **Routing metrics layer** dedicato: F1 score per tier, latenza, token cost, drift alert per prevenire la deriva silenziosa del rapporto tra tier (es. da 90/10 a 50/50)
- **Observability trasversale**: Langfuse o Phoenix self-hosted strumentano routing decisions, latency per tier e quality metrics su tutti i layer

Il ruolo dell'ingegnere nel governo dell’intelligenza artificiale

Etica by design

L'ingegnere integra valori etici fin dalla fase di progettazione: equità, non discriminazione, tutela dei dati e rispetto della dignità umana non sono vincoli esterni, ma requisiti architetturali.

Responsabilità tecnica

Sotto l'AI Act, il fornitore risponde della conformità del sistema per l'intero ciclo di vita. La responsabilità dell'ingegnere include la documentazione tecnica, la gestione del rischio e la correzione post-market.

Human oversight

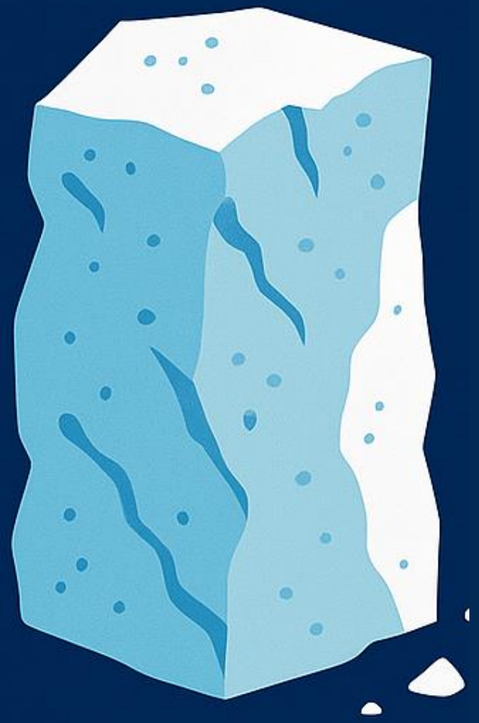
I sistemi ad alto rischio richiedono supervisione umana effettiva (art. 14 AI Act). L'ingegnere progetta le interfacce e i meccanismi che rendono il controllo umano reale, non solo formale.

Competenza professionale

Conoscere il quadro normativo (AI Act, GDPR, NIS2), gli standard armonizzati e i framework di governance è parte integrante della competenza tecnica dell'ingegnere che opera nel mercato europeo.

L'ingegnere non è solo costruttore di sistemi: è garante della qualità tecnica, della conformità normativa e della tutela dei diritti fondamentali delle persone che quei sistemi utilizzeranno.

Semplice o complessa la tecnologia è nelle mani dell’uomo



Il futuro non dipende da quanto sarà intelligente l’IA, ma da quanto sapremo esserlo noi nell’usarla.

Ing. Fabio Massimi

GRAZIE!

Ing. Fabio Massimi (Expert Mode)
AGID Direzione Generale
EC AI Board Standards
UNI/CT 533 «Intelligenza Artificiale»
CEN&CELELEC JTC 21 «Artificial Intelligence»
ing.fabiomassimi@gmail.com