

Corso di formazione



L'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE

AMMINISTRAZIONE





L'Evoluzione Normativa dell'AI Act: Dalle Origini alla sua Adozione

L'AI Act rappresenta il culmine di un processo graduale, politico, tecnico e culturale che ha preso avvio ben prima della sua proposta formale del 2021. Questo regolamento non nasce in un vuoto normativo, ma è il risultato di anni di riflessione e dibattito all'interno delle istituzioni europee.

Il percorso verso una regolamentazione completa dell'intelligenza artificiale in Europa riflette la crescente consapevolezza della necessità di bilanciare innovazione tecnologica e protezione dei diritti fondamentali, creando un quadro giuridico armonizzato per tutti gli Stati membri.

2017: I Primi Passi verso la Regolamentazione



Risoluzione del Parlamento Europeo

16 febbraio 2017 (2015/2103(INL)) intitolata "Norme di diritto civile sulla robotica". Prima manifestazione esplicita dell'intento politico dell'UE di disciplinare l'IA.



Concetti Innovativi

Introduce per la prima volta il concetto di personalità elettronica (oggi abbandonato) e sottolinea la necessità di un quadro giuridico europeo armonizzato.



Momento "Costituente"

Il legislatore prende atto della discontinuità tecnologica rappresentata dall'IA e della necessità di regolamentarla a livello europeo.



2018: Strategia Europea e Gruppo di Esperti

Comunicazione della Commissione

Nel 2018 la Commissione europea pubblica la Comunicazione COM(2018) 237, "Artificial Intelligence for Europe", dichiarando l'intenzione di:

- Promuovere investimenti pubblici e privati nell'IA
- Garantire il rispetto dei diritti fondamentali
- Sviluppare un quadro etico e giuridico per l'uso dell'IA

Nascita dell'AI HLEG

Nello stesso anno viene istituito lo **High-Level Expert Group on AI** (AI HLEG), un gruppo consultivo indipendente composto da esperti accademici, industriali e della società civile.

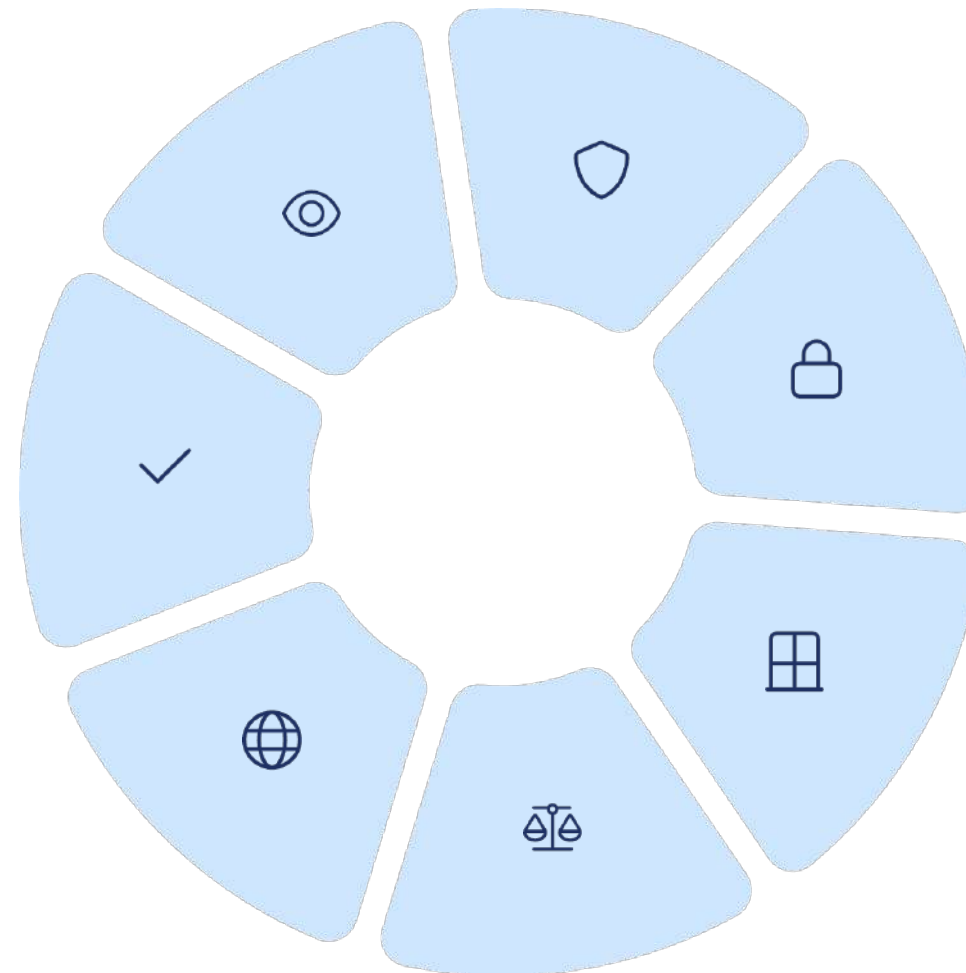
Questo gruppo avrà un ruolo determinante nella definizione dei principi etici che guideranno la futura legislazione europea sull'intelligenza artificiale.

2019: Linee Guida Etiche HLEG per un'IA Affidabile

Supervisione Umana
Garantire che i sistemi di IA rimangano sotto il controllo umano e non compromettano l'autonomia umana.

Responsabilizzazione
Implementare meccanismi per garantire la responsabilità e la rendicontabilità dei sistemi di IA.

Benessere Sociale
Promuovere il benessere sociale e ambientale attraverso sistemi di IA sostenibili.



Robustezza e Sicurezza

Assicurare che i sistemi di IA siano sicuri, affidabili e sufficientemente robusti per affrontare errori o incongruenze.

Privacy e Governance

Proteggere i dati personali e garantire che l'accesso ai dati sia adeguatamente governato.

Trasparenza

Garantire la tracciabilità e la spiegabilità dei sistemi di IA e delle loro decisioni.

Equità e Non Discriminazione

Evitare pregiudizi ingiusti, discriminazioni e garantire diversità e inclusività.

Nel 2019, l'AI HLEG pubblica le "Ethics Guidelines for Trustworthy AI", definendo i **sette requisiti** chiave per un'IA affidabile (lawful, ethical and robust). Questi principi saranno poi recepiti e trasposti nel corpo vincolante dell'AI Act.

2020: Il Libro Bianco sull'Intelligenza Artificiale

Nel febbraio 2020, la Commissione presenta il "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust" (COM(2020) 65 final), che costituisce la vera base concettuale dell'AI Act. Il documento apre una consultazione pubblica ampia, cui partecipano centinaia di soggetti pubblici e privati.

Approccio Basato sul Rischio

Proposta di un sistema di obblighi graduati in base al livello di rischio presentato dai sistemi di IA, con particolare attenzione ai sistemi ad alto rischio.

Focus sui Settori Critici

Particolare attenzione ai sistemi di IA utilizzati nei settori pubblici, sanitari e infrastrutturali, considerati particolarmente sensibili per i diritti dei cittadini.

Divieti per Usi Inaccettabili

Prima ipotesi di divieti assoluti per alcuni usi dell'IA considerati inaccettabili per il loro impatto sui diritti fondamentali e sui valori europei.

2021: La Proposta Ufficiale dell'AI Act

Proposta della Commissione

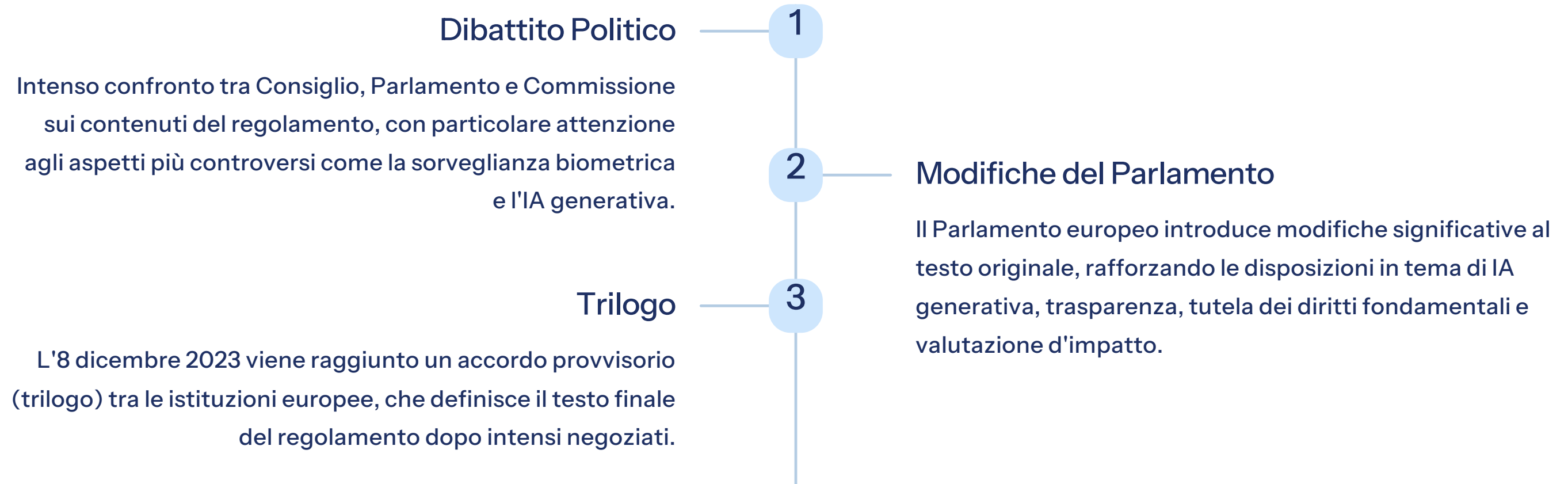
Il 21 aprile 2021, la Commissione presenta ufficialmente la **proposta di Regolamento sull'Intelligenza Artificiale (COM(2021) 206 final)**, il primo tentativo al mondo di regolamentazione orizzontale dell'IA.

La proposta si caratterizza per un approccio basato sul rischio, suddividendo i sistemi di IA in quattro categorie: rischio inaccettabile (vietati), alto rischio, rischio limitato e rischio minimo.

Caratteristiche Principali

- Focus su trasparenza, accountability e sorveglianza umana
- Attenzione alla qualità dei dati utilizzati nei sistemi di IA
- Applicazione extraterritoriale: si applica anche a fornitori e deployer extra-UE se i loro sistemi incidono nel mercato interno
- Sistema di governance con autorità nazionali e comitato europeo

2021-2023: L'Iter Legislativo e i Negoziati



Durante questo periodo, il testo dell'AI Act è stato oggetto di un intenso processo legislativo che ha visto il coinvolgimento di numerosi stakeholder, dalle istituzioni europee alle aziende tecnologiche, dalle organizzazioni per i diritti civili agli esperti del settore.

2024: Adozione Formale dell'AI Act

Approvazione del Parlamento

Il testo definitivo del Regolamento (UE) 2024/1689 viene approvato in via definitiva dal Parlamento europeo il 13 marzo 2024, segnando la conclusione formale del processo legislativo.

Pubblicazione Ufficiale

Il 12 luglio 2024, il testo del regolamento viene pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, rendendolo ufficialmente parte dell'ordinamento giuridico europeo.

Entrata in Vigore

L'AI Act entra ufficialmente in vigore il 1° agosto 2024, anche se la sua applicazione avverrà progressivamente secondo quanto stabilito dall'articolo 113 del regolamento stesso.



Obiettivi Primari dell'AI Act

Mercato Interno

Migliorare il funzionamento del mercato interno stabilendo un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'utilizzo dei sistemi di IA all'interno dell'Unione.

Un aspetto fondamentale è la prevenzione della frammentazione del mercato unico, che potrebbe derivare da normative nazionali divergenti in materia di IA.

IA Antropocentrica e Affidabile

Promuovere un'intelligenza artificiale antropocentrica e affidabile, garantendo al contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali.

Questo include la tutela dei principi di democrazia, stato di diritto e protezione ambientale, in linea con i valori fondamentali dell'Unione Europea.

Principi Fondamentali dell'AI Act



Diritti Fondamentali

L'AI Act è saldamente ancorato ai valori dell'Unione sanciti dalla Carta dei diritti fondamentali dell'Unione europea, ponendo la dignità umana e i diritti dei cittadini al centro della regolamentazione.



Approccio Basato sul Rischio

Il regolamento adotta un approccio proporzionato basato sul rischio, con obblighi più stringenti per i sistemi di IA che presentano rischi maggiori per la sicurezza e i diritti delle persone.



Armonizzazione Europea

Creazione di un quadro normativo armonizzato a livello europeo che garantisce certezza giuridica per le imprese e tutela uniforme per i cittadini di tutti gli Stati membri.

Questi principi riflettono l'ambizione dell'Unione Europea di diventare leader mondiale nella regolamentazione dell'intelligenza artificiale, promuovendo un modello di innovazione tecnologica che rispetti i diritti fondamentali e i valori democratici.

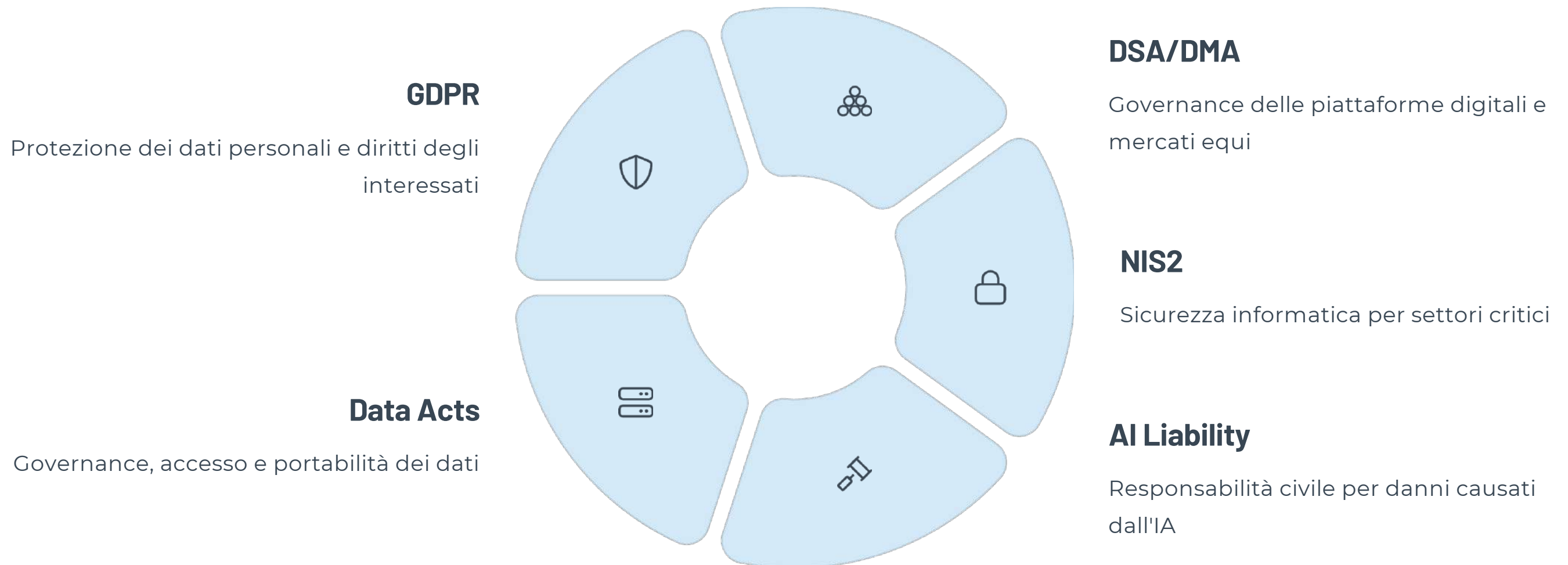
L'AI Act nell'ecosistema Normativo Europeo

L'Artificial Intelligence Act non è un corpo normativo isolato, ma parte di un disegno legislativo coerente, multilivello e integrato dell'Unione Europea. Questa architettura normativa mira a regolamentare lo spazio digitale europeo in modo trasversale, bilanciando innovazione, tutela dei diritti fondamentali e sicurezza.

L'AI Act si inserisce in un contesto di regolamenti e direttive interconnesse che insieme formano un quadro completo per governare le tecnologie digitali emergenti, con particolare attenzione ai sistemi di intelligenza artificiale e al loro impatto sulla società.



Un ecosistema normativo integrato



L'AI Act si inserisce in questo complesso ecosistema normativo, creando sinergie con gli altri regolamenti e direttive. Insieme, questi strumenti giuridici formano un quadro coerente che mira a promuovere un'innovazione tecnologica responsabile, rispettosa dei diritti fondamentali e allineata ai valori europei.

GDPR: Il Primo Pilastro

Il Regolamento Generale sulla Protezione dei Dati (GDPR) rappresenta il primo pilastro dell'ecosistema normativo europeo. Si applica ogni volta che un sistema di IA tratta dati personali, garantendo i diritti privacy degli interessati.

GDPR e AI Act convivono e si complementano: mentre il primo tutela i diritti degli individui relativi ai loro dati personali, il secondo disciplina specificamente la progettazione, lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale.



Un esempio pratico: un sistema di IA utilizzato per il riconoscimento facciale in ambito pubblico dovrà rispettare gli obblighi di trasparenza, minimizzazione dei dati e base giuridica del trattamento previsti dal GDPR, oltre alle prescrizioni dell'AI Act per i sistemi ad alto rischio.

Digital Services Act e Digital Markets Act



Digital Services Act

Il DSA (Regolamento 2022/2065) impone obblighi di due diligence, trasparenza algoritmica e gestione dei contenuti illeciti alle piattaforme digitali.



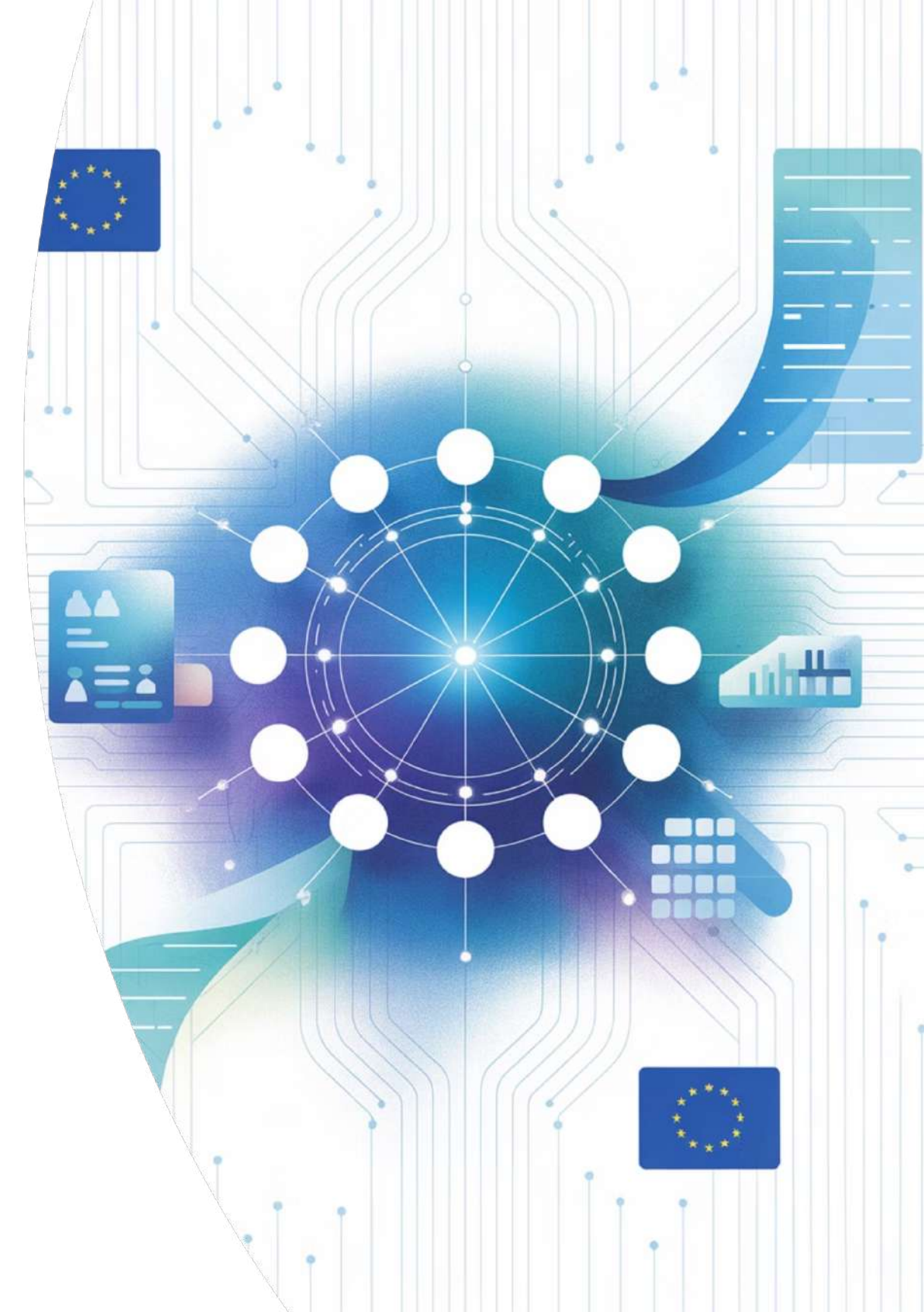
Digital Markets Act

Il DMA (Regolamento 2022/1925) mira a contenere il potere di mercato dei gatekeeper digitali, promuovendo un ambiente digitale più equo e competitivo.



Interazione con AI Act

Le piattaforme che impiegano sistemi di IA dovranno rispettare i requisiti di trasparenza, supervisione umana e valutazione dei rischi previsti dall'AI Act, in aggiunta a quelli del DSA/DMA.



Direttiva NIS2: Sicurezza Informatica



La Direttiva NIS2 (Direttiva UE 2022/2555) impone misure di sicurezza informatica rafforzate per soggetti pubblici e privati operanti in settori critici. La cybersecurity rappresenta un tema centrale anche nell'AI Act, soprattutto per quanto riguarda i sistemi classificati ad alto rischio (Articolo 15).

La connessione chiave tra questi due strumenti normativi è evidente: l'AI Act impone che i sistemi ad alto rischio garantiscano "robustezza, sicurezza e resilienza" anche contro attacchi malevoli, allineandosi quindi agli standard di sicurezza informatica stabiliti dalla NIS2.

Data Governance Act

Il Data Governance Act (Regolamento 2022/868) è un elemento chiave dell'ecosistema normativo europeo che mira a creare uno spazio europeo dei dati. Questo regolamento incentiva la creazione di intermediari fiduciari per la condivisione dei dati tra soggetti pubblici e privati.

L'obiettivo principale è facilitare la disponibilità di dati per l'innovazione, garantendo al contempo che questa condivisione avvenga in modo sicuro e conforme ai valori europei. Questo aspetto è particolarmente rilevante per l'AI Act, che si basa sulla disponibilità e qualità dei dati di addestramento.



Data Act: Accesso e Portabilità



Accesso ai Dati

Il Data Act (Regolamento 2023/2854) disciplina i diritti di accesso ai dati generati da dispositivi e applicazioni, garantendo che questi possano essere utilizzati per scopi innovativi.



Portabilità

Stabilisce norme sulla portabilità dei dati, permettendo agli utenti di trasferire i propri dati tra diversi servizi e piattaforme con maggiore facilità.



Interoperabilità

Promuove l'interoperabilità dei dati, facilitando la creazione di sistemi di IA equi, trasparenti e non discriminatori attraverso l'accesso a set di dati diversificati.



Direttiva sulla Responsabilità da IA

1 Complemento all'AI Act

La proposta di direttiva sulla responsabilità da IA (AI Liability Directive), attualmente in fase di approvazione, mira a integrare l'AI Act con regole specifiche in materia di responsabilità civile extracontrattuale.

2 Presunzione di causalità

Introduce una presunzione di causalità tra il danno subito e il comportamento dell'IA in determinate condizioni, facilitando l'onere della prova per le vittime.

3 Conservazione delle prove

Stabilisce obblighi di conservazione delle prove da parte degli operatori di sistemi di IA, garantendo la possibilità di accertare le responsabilità in caso di danni.



AI Act: Implementazione Graduale del Regolamento UE 2024/1689

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale, noto come AI Act, rappresenta una pietra miliare nella regolamentazione dell'IA in Europa. La sua caratteristica distintiva è l'implementazione graduale, strategicamente progettata per accompagnare l'ecosistema verso l'adeguamento.

Questa presentazione esplora il cronoprogramma dettagliato dell'AI Act, analizzando le diverse fasi di applicazione e le implicazioni per tutti gli attori coinvolti nel panorama dell'intelligenza artificiale europea.



La Strategia dell'Implementazione Graduale

- Adeguamento Progressivo**
Accompagnare l'ecosistema verso l'adeguamento in modo graduale e sostenibile.
- Conformità Strutturata**
Consentire agli operatori di organizzarsi e strutturarsi in modo conforme alle nuove normative.
- Preparazione alla Vigilanza**
Dare tempo all'AI Office e alle autorità nazionali di prepararsi adeguatamente ai compiti di vigilanza.
- Allineamento Normativo**
Coordinare le tempistiche con altri strumenti giuridici in via di completamento, come l'AI Liability Directive e il Registro UE dei sistemi IA.

EU Regulatory Implementation Timeline





Motivazioni e Implicazioni dell'Approccio Graduale

Proporzionalità

Non tutti i soggetti sono oggi pronti a conformarsi, soprattutto le PMI e gli attori non digitali. L'approccio graduale consente un adattamento sostenibile.

Effettività

Serve tempo per creare gli strumenti attuativi necessari, come moduli di registrazione, linee guida e banche dati per supportare l'implementazione.

Certezza Giuridica

La gradualità mitiga il rischio di contenzioso derivante da obblighi immediati, dando tempo per assorbire l'impatto normativo in modo ordinato.

Formazione

Il tempo è necessario per formare adeguatamente autorità, fornitori e deployer, garantendo uniformità interpretativa e applicativa della normativa.

Prima Fase: Entrata in Vigore Formale

L'AI Act è entrato formalmente in vigore il 1° agosto 2024, venti giorni dopo la sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea. Questa data segna l'inizio ufficiale del percorso di implementazione, anche se la maggior parte delle disposizioni non è ancora applicabile.

In questa fase iniziale, gli stakeholder hanno l'opportunità di familiarizzare con il testo normativo e iniziare a pianificare le strategie di adeguamento, mentre le istituzioni europee avviano i preparativi per l'istituzione dell'AI Office e degli altri organismi di governance.



Seconda Fase: Febbraio 2025



Capo I: Definizioni e Ambito

Entrano in vigore le definizioni fondamentali e l'ambito di applicazione del regolamento, stabilendo i confini della normativa e chiarendo quali sistemi di IA rientrano nel suo perimetro.



Capo II: Divieti Assoluti

Diventano applicabili i divieti assoluti di cui all'articolo 5, che proibiscono sistemi di IA considerati inaccettabili, come quelli che manipolano il comportamento umano o implementano sistemi di credito sociale.

Dal 2 febbraio 2025, si devono assicurare che i sistemi di IA non violino i divieti assoluti stabiliti dal regolamento, rappresentando il primo passo concreto verso la conformità.

Terza Fase: Agosto 2025



Trasparenza

Capo V (Artt. 50-54): Obblighi di trasparenza, gestione del rischio e conformità per i modelli di IA per finalità generali (GPAI).



Registro UE

Capo VII: Istituzione del Registro UE dei sistemi di IA ad alto rischio (Art. 60) e procedure per la marcatura CE.



Governance

Capo XII: Attivazione dell'AI Office e dei meccanismi di cooperazione, consultazione e vigilanza (Artt. 64-70).

Dal 2 agosto 2025, i fornitori di modelli di IA per finalità generali dovranno conformarsi agli obblighi di trasparenza e gestione del rischio, mentre si attiveranno le strutture di governance a livello europeo.



Quarta Fase: Agosto 2026

Il 2 agosto 2026 segna un momento cruciale nell'implementazione dell'AI Act, con l'applicazione integrale del Regolamento. Entrano in vigore tutte le disposizioni non ancora attive, inclusi:

- Capo III: Requisiti per i sistemi di IA ad alto rischio
- Capo IV: Valutazione di conformità e vigilanza
- Capo VI: Obblighi documentali
- Capo VIII: Codici di condotta
- Capo IX: Prove in condizioni reali

- Capo X: Notifiche di incidenti gravi
- Capo XI: Sanzioni e misure correttive
- Capo XIII: Cooperazione internazionale
- Capo XIV: Disposizioni finali e transitorie

A partire da questa data, tutti gli operatori dovranno essere pienamente conformi alla maggior parte degli obblighi previsti dal regolamento, con l'eccezione di quelli relativi alla classificazione dei sistemi ad alto rischio.

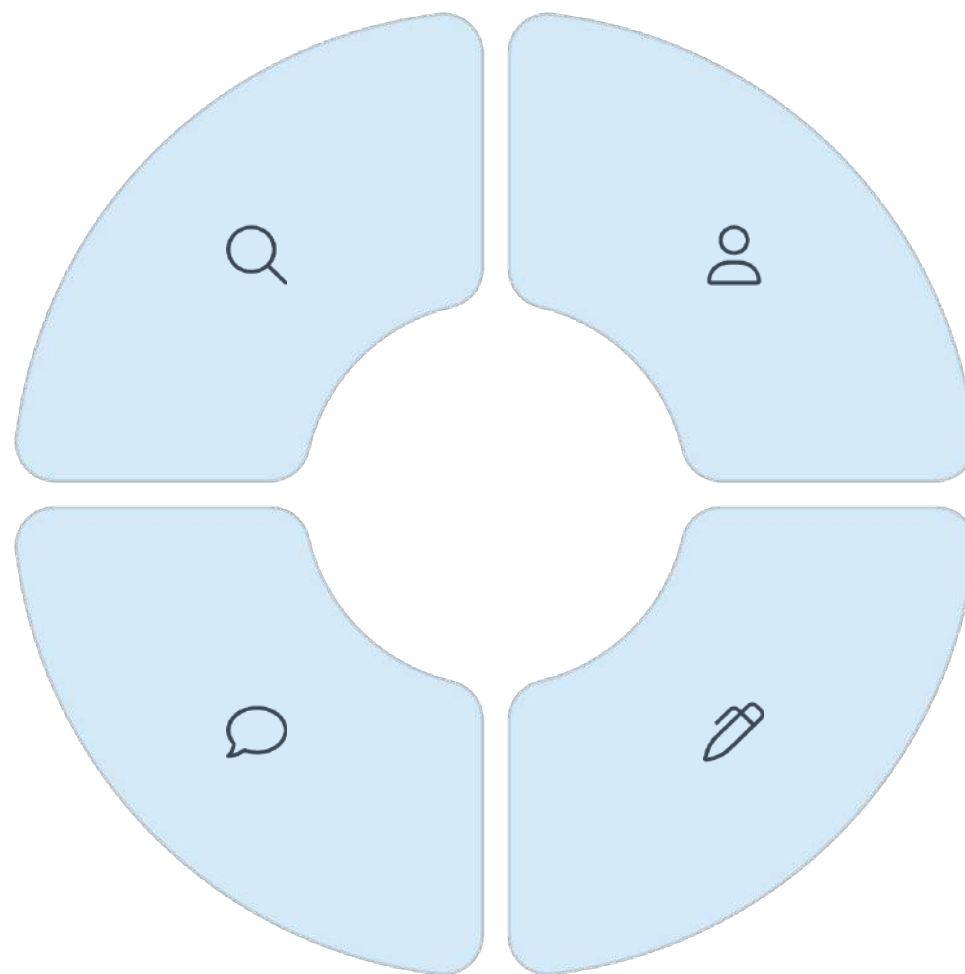
Fase Finale: Agosto 2027

Classificazione Sistemi ad Alto Rischio

Entra in vigore l'articolo 6, paragrafo 1, che disciplina la classificazione dei sistemi di IA ad alto rischio sulla base degli Allegati II e III.

Interazione con Organismi Notificati

Si perfezionano i processi di certificazione e valutazione della conformità attraverso gli organismi notificati designati.



Obblighi Correlati

Diventano applicabili tutti gli obblighi tecnici, organizzativi e documentali relativi ai sistemi classificati come ad alto rischio.

Aggiornamento Tecnologico

Gli operatori completano l'aggiornamento delle tecnologie per garantire la piena conformità ai requisiti più stringenti.

Ambito di applicazione (Art. 2, par. 1 AI Act)

Il Regolamento adotta un approccio estensivo ed extraterritoriale, simile a quello del GDPR, allo scopo di proteggere il mercato interno e i diritti fondamentali delle persone che si trovano nell'Unione. Si applica quindi anche a operatori extra-UE, se i loro sistemi producono effetti nell'Unione.



"Navigating the future
with confidence"



Il principio guida

"Chiunque impatti sul mercato o sui cittadini dell'Unione deve rispettare le regole dell'Unione".



**Unlock
Potential**

a) Fornitori che immettono sul mercato o mettono in servizio sistemi o modelli di IA nell'Unione



Norma: Art. 2, par. 1, lett. a

Chi coinvolge: Fornitori (soggetti che sviluppano o fanno sviluppare il sistema o modello IA e lo commercializzano).

Condizione: L'immissione sul mercato o la messa in servizio avviene nell'UE, indipendentemente dalla localizzazione geografica del fornitore.



Effetto extraterritoriale

Anche fornitori stabiliti fuori dall'UE devono rispettare l'AI Act se immettono i loro prodotti nel mercato europeo.



Esempio

Una società americana che vende un sistema di IA per la selezione del personale a una banca in Italia → è soggetta all'AI Act.

b) Deployer stabiliti o situati nell'Unione

Norma: Art. 2, par. 1, lett. b

Chi coinvolge: Chi utilizza un sistema di IA (deployer)

Condizione: Il deployer ha stabilimento o sede nell'UE.

Applicazione

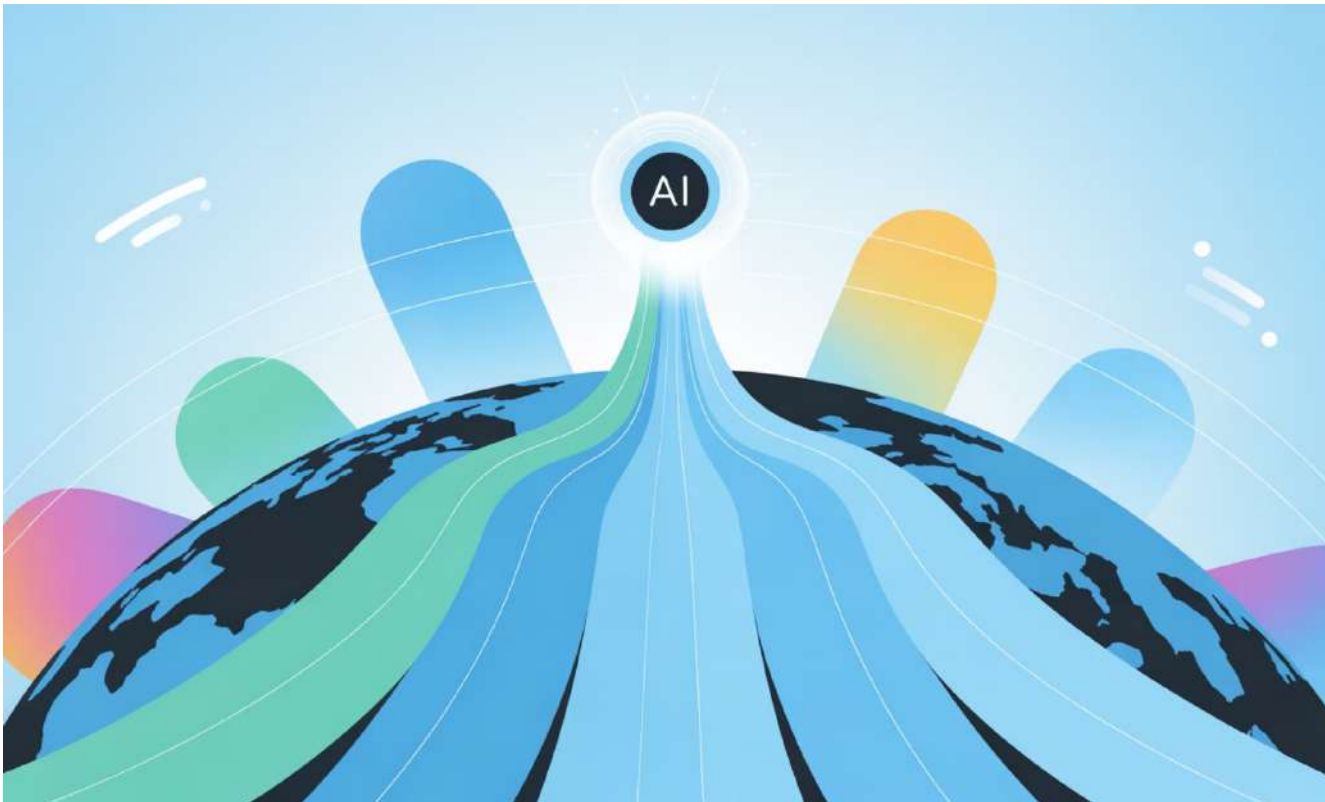
Anche se il sistema di IA è stato sviluppato altrove, l'uso che avviene all'interno dell'Unione è sufficiente per far scattare l'applicazione del Regolamento.

Esempio

Un'azienda italiana usa un software di IA per la gestione della logistica sviluppato in Cina → è soggetta all'AI Act in qualità di deployer.



c) Fornitori e deployer extra-UE, se l'output viene utilizzato nell'Unione



Norma: Art. 2, par. 1, lett. c

Chi coinvolge: Fornitori e deployer con sede fuori dall'UE.

Condizione: L'output del sistema viene utilizzato nell'Unione.



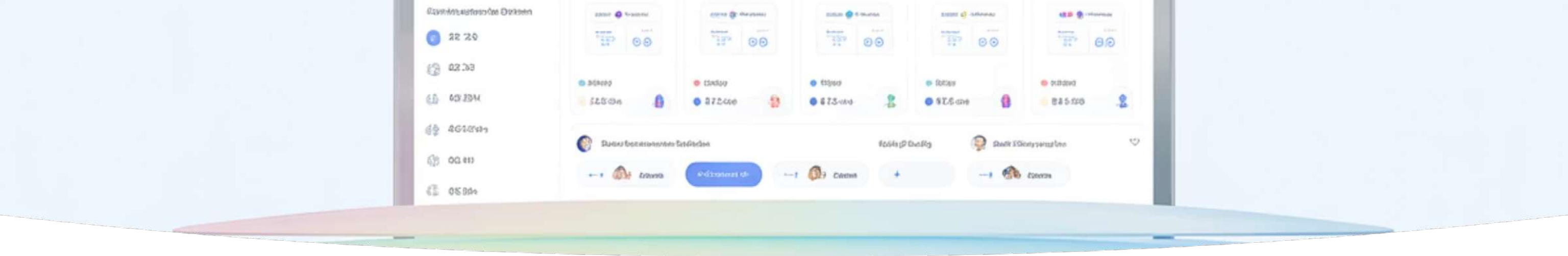
Extraterritorialità rafforzata

Si tratta di una clausola di extraterritorialità rafforzata, molto simile al meccanismo dell'effetto destinazione previsto dal GDPR (art. 3).



Esempio

Una piattaforma australiana offre servizi di IA per il riconoscimento vocale usati da cittadini o aziende europee → rientra nell'AI Act.



d) Importatori e distributori di sistemi di IA



Norma: Art. 2, par. 1, lett. d

Chi coinvolge: Tutti i soggetti che, senza sviluppare sistemi IA, li immettono sul mercato o li distribuiscono all'interno dell'UE.



Responsabilità

Questi soggetti non sono sviluppatori né utilizzatori diretti, ma sono comunque responsabili del rispetto di determinati obblighi di conformità e sorveglianza (artt. 23–25).



Esempio

Una società tedesca importa e rivende software IA coreani tramite e-commerce B2B → soggetta all'AI Act come importatore e distributore.

e) Fabbricanti di prodotti che integrano un sistema di IA



Norma: Art. 2, par. 1, lett. e

Chi coinvolge: Chi integra un sistema di IA in un prodotto e lo commercializza con il proprio nome o marchio.

Rilevanza settoriale

Rilevante per i settori regolati da direttive di armonizzazione (es. macchine, dispositivi medici, automotive). In questi casi, il sistema di IA è considerato componente di sicurezza del prodotto.

Esempio

Un produttore italiano di robot chirurgici integra un modulo IA per il riconoscimento dei tessuti → rientra nell'ambito dell'AI Act.

f) Rappresentanti autorizzati di fornitori non stabiliti nell'UE



Fornitore extra-UE

Una startup canadese che sviluppa sistemi di IA



Designazione

Nomina obbligatoria di un rappresentante nell'UE (art. 25)



Rappresentante nell'UE

Società o studio legale a Bruxelles soggetto al Regolamento

- ◆ Norma: Art. 2, par. 1, lett. f
- ◆ Chi coinvolge: Il rappresentante legale designato nell'UE da fornitori extraeuropei.
- 📌 Tale figura è obbligatoria per i fornitori extra-UE (vedi art. 25): serve a garantire un interlocutore stabile e responsabile nei confronti delle autorità europee.

Conarfedden - TK
Dexepocatie



Innovation meets expertise®

Inder Teckdejc - Brussels



g) Persone interessate che si trovano nell'Unione

- ◆ Norma: Art. 2, par. 1, lett. g
- ◆ Chi coinvolge: Le persone fisiche i cui diritti fondamentali sono incisi dai sistemi IA usati in Europa.
- 📌 Questo punto non individua un soggetto attivo ma sottolinea che il Regolamento protegge le persone che si trovano territorialmente nell'UE, a prescindere dalla cittadinanza o dalla sede del fornitore/deployer.
- 📌 Esempio: Una cittadina giapponese in viaggio a Roma viene profilata da un sistema IA per finalità di sorveglianza biometrica → è tutelata dall'AI Act.





✓ Conclusione

L'articolo 2, paragrafo 1, configura un perimetro applicativo ampio e multilivello, che:

- si estende oltre i confini dell'UE,
 - coinvolge tutti gli attori della filiera dell'IA (sviluppatori, distributori, utilizzatori),
 - tutela in modo ampio e preventivo i diritti fondamentali delle persone fisiche presenti nel territorio dell'Unione.
- 📌 Il Regolamento non si applica solo in base alla residenza del soggetto attivo, ma anche in base all'effetto prodotto nell'Unione (approccio "output-based").

Esclusione delle applicazioni militari e della sicurezza nazionale (art. 2, par. 3, lett. a)

Art. 2, par. 3, lett. a: "Il presente regolamento non si applica ai sistemi di IA utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale."

📌 Ratio: la materia della sicurezza nazionale è riservata agli Stati membri ex art. 4, par. 2 TUE. 📌 Condizione: l'uso deve essere esclusivamente militare o di sicurezza nazionale. Qualsiasi impiego civile o commerciale riporta il sistema entro l'ambito del Regolamento.



🚫 Esempio escluso

Un drone IA ad uso bellico.



✅ Esempio incluso

Un sistema di sorveglianza biometrica a uso misto civile-militare.

Esclusione per attività delle autorità pubbliche svolte fuori dal diritto UE (art. 2, par. 3, lett. b)

Art. 2, par. 3, lett. b: "Il presente regolamento non si applica alle autorità pubbliche che utilizzano sistemi di IA al di fuori dell'ambito di applicazione del diritto dell'Unione."

📌 Ratio: tutela della sovranità nazionale. 📌 Limite: se l'attività ricade nel diritto UE, l'esclusione non si applica.



✓ **Incluso**

IA usata per gestione migranti (materia armonizzata a livello UE).



🛑 **Escluso**

IA usata in operazioni coperte da segreto di Stato non regolato dal diritto UE.

Esclusione delle attività di ricerca e sviluppo (art. 2, par. 3, lett. c)

Art. 2, par. 3, lett. c: "Il presente regolamento non si applica alle attività di ricerca e sviluppo riguardanti sistemi di IA che non comportano l'immissione sul mercato o la messa in servizio."

Condizioni cumulative

1. Attività qualificabile come ricerca o sviluppo;
2. Nessuna immissione sul mercato (art. 3, n. 23) o messa in servizio (art. 3, n. 24).

Esempi

🔪 Esempio escluso (non coperto): università che testa un sistema IA su dati sintetici in laboratorio.

📢 Esempio incluso (coperto): startup che rilascia una beta pubblica del sistema = "messa in servizio".



Clausola di salvaguardia pro-ricerca (art. 2, par. 6)

Art. 2, par. 6: "Il presente regolamento non osta a che siano svolte attività di ricerca e sviluppo sui sistemi di IA, comprese le sperimentazioni, purché non comportino un utilizzo nel mercato interno."

📌 È una clausola di garanzia che tutela la libertà di ricerca (art. 13 della Carta UE), ma ribadisce che:

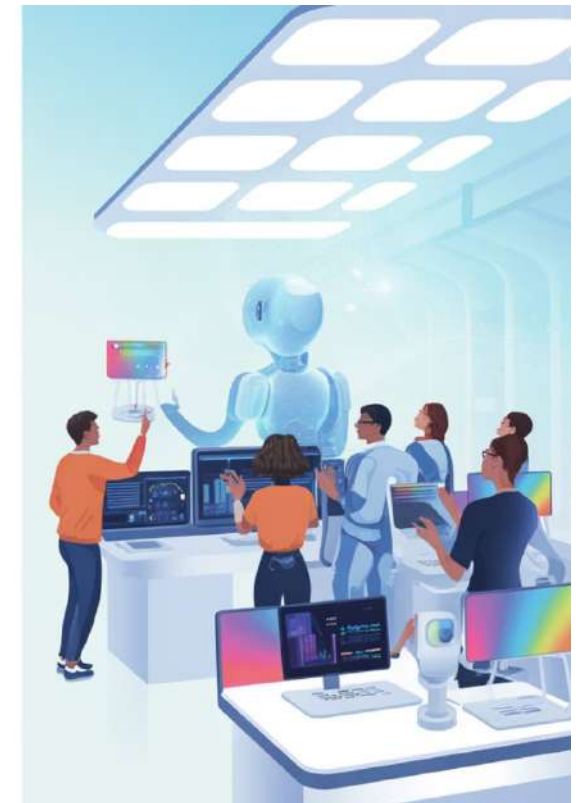
- La sperimentazione è ammessa solo se non comporta utilizzo reale o commerciale.
- Il confine si trova nel concetto di "mercato interno" e "impatto su utenti".

🧑‍🔬 Esempio escluso (cioè AI Act non si applica): test in ambiente chiuso simulato. 🏠 Esempio incluso (AI Act si applica): testing su clienti reali, anche se in ambiente pilota.

🔗 Coordinamento con art. 89 AI Act: sperimentazioni controllate in ambienti reali sono possibili, ma solo previa autorizzazione, con marcatura provvisoria CE e monitoraggio.



AI
Innovation



Un ambito applicativo esteso e controllato

L'art. 2 AI Act delinea un ambito di applicazione molto ampio, che si applica:

Sistemi e modelli di IA
Come definito nel par. 2 dell'articolo



Soggetti extra-UE

Anche quando sviluppati e gestiti da soggetti al di fuori dell'Unione Europea (par. 1)

Esclusioni limitate

Solo in casi limitati ed espressamente indicati consente l'esclusione (par. 3 e 6)



Sistema di IA, Modello AI, GPAI

Definizione Normativa

L'articolo 3, paragrafo 1 dell'AI Act definisce il "**sistema di intelligenza artificiale**" (sistema di IA) come:

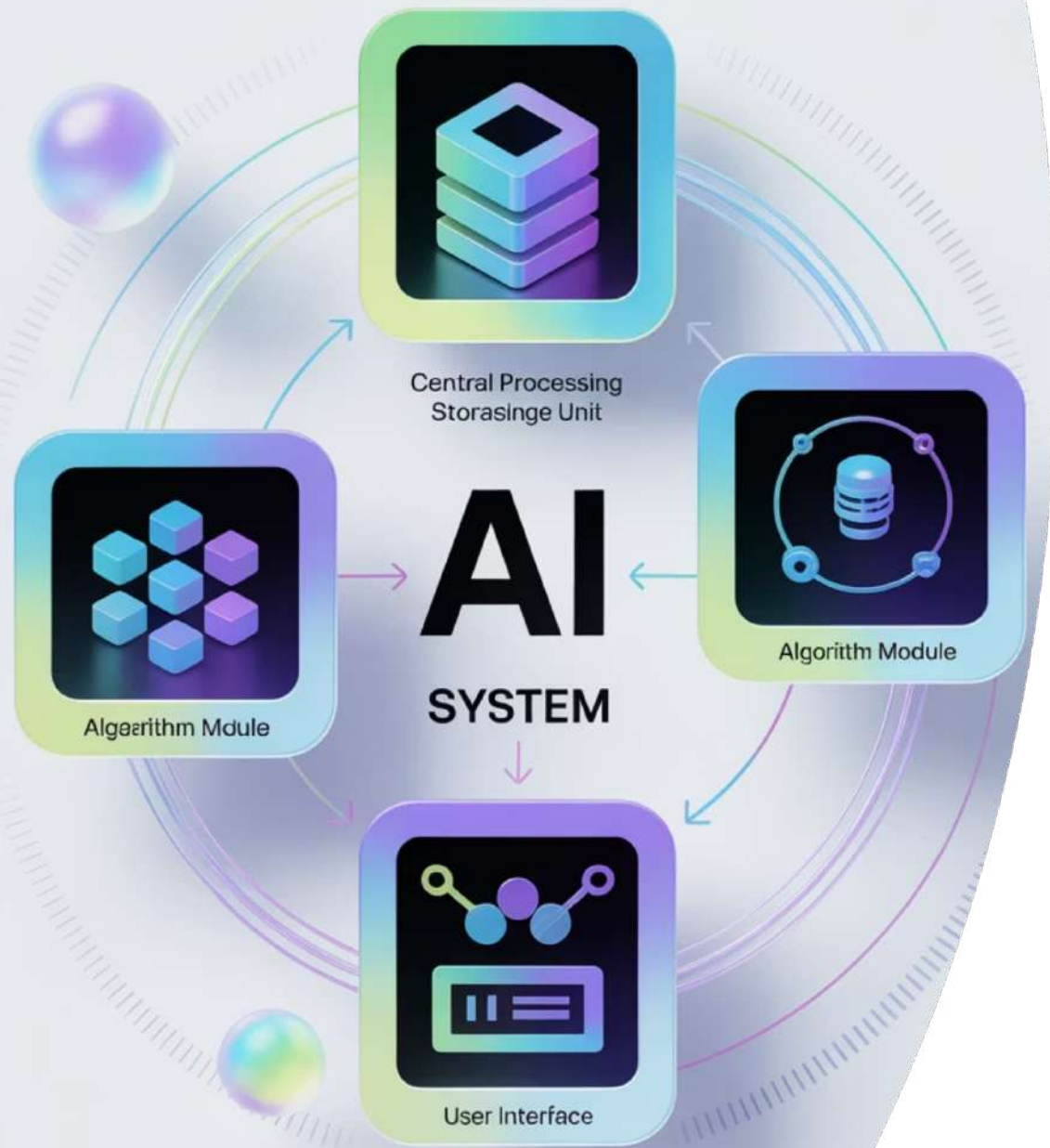
"un **sistema automatizzato** progettato per funzionare con livelli di **autonomia** diversi e che può presentare **adattabilità dopo la distribuzione** e che, per obiettivi espliciti o impliciti, **deduce, dall'input** che riceve, come **generare output** quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"



Elementi Costitutivi

La definizione presenta quattro elementi cumulativi essenziali:

- **Sistema automatizzato**
Il sistema deve operare senza intervento umano continuo, pur potendo prevedere supervisione o controllo umano in fase di progettazione o deployment.
- **Livelli di autonomia diversi**
Riconosce la varietà di gradi di indipendenza operativa, dalla semplice automazione deterministica ai sistemi più complessi con capacità decisionale autonoma.
- **Adattabilità post-distribuzione**
Elemento distintivo che include la capacità di machine learning, deep learning e altri meccanismi di apprendimento che modificano il comportamento del sistema dopo la messa in funzione.
- **Capacità inferenziale**
Il sistema deve essere capace di elaborare input per generare output che influenzano l'ambiente circostante.



Esempi Pratici di Sistemi di IA



Sistema di Credito Scoring Bancario

Un sistema che analizza dati finanziari del richiedente (input) per generare un punteggio di affidabilità creditizia (output) che influenza la decisione di concessione del prestito. Presenta autonomia operativa, adattabilità attraverso aggiornamenti del modello basati su nuovi dati storici.



Chatbot Conversazionale

Sistema che riceve query testuali (input) e genera risposte contestualizzate (output) utilizzando modelli di linguaggio pre-addestrati con capacità di adattamento conversazionale.



Sistema di Videosorveglianza Intelligente

Analizza flussi video (input) per identificare comportamenti anomali o riconoscimento facciale (output) con capacità di apprendimento da nuovi pattern comportamentali.

Modello AI

L'articolo 3, paragrafo 4 definisce il "modello di AI" come:

"un **modello automatizzato** che viene **addestrato** con **dati di input** e utilizza **tecniche di apprendimento automatico**, o logica e approcci basati sulla conoscenza, o tecniche statistiche, e può essere utilizzato dall'algoritmo di un sistema di IA per generare output quali contenuti, previsioni, raccomandazioni o decisioni"

Regulatory text

AI Model Definition

Regulatory text

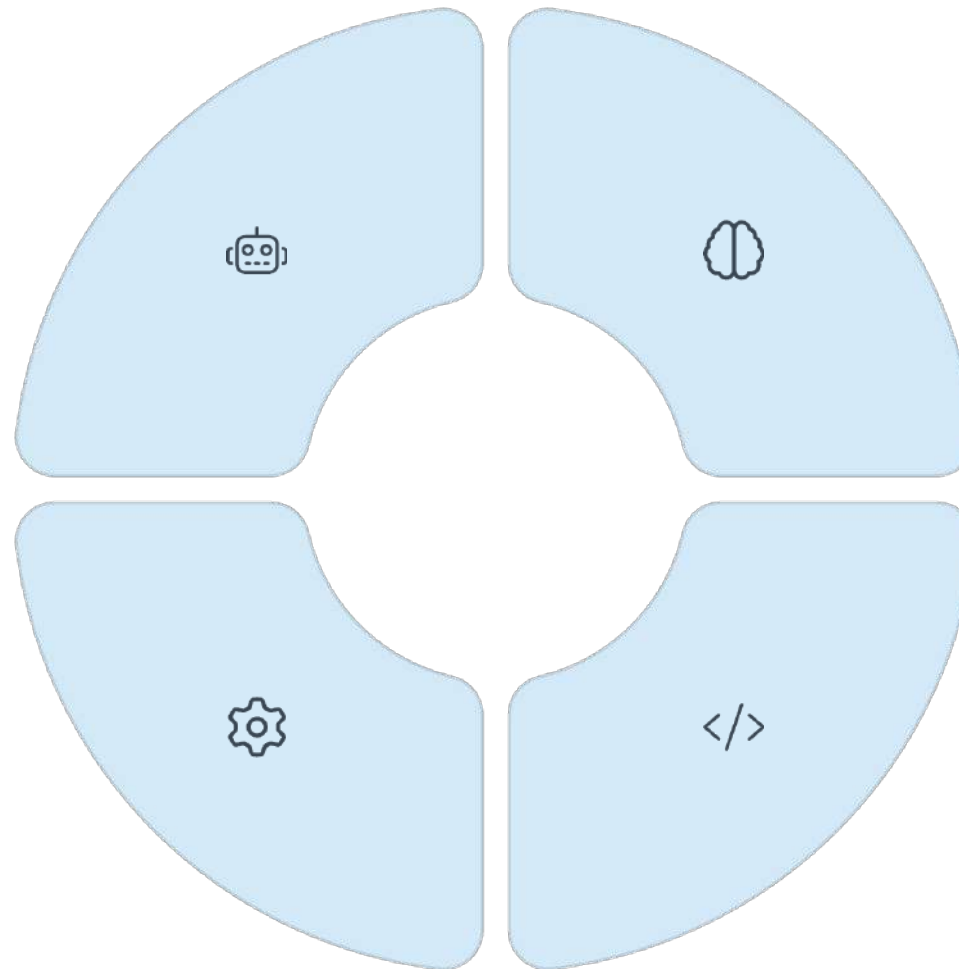
Elementi Costitutivi del Modello

Carattere automatizzato

Il modello opera senza supervisione umana diretta nel processo di generazione degli output.

Capacità generativa

Il modello deve essere utilizzabile per produrre output diversificati.



Processo di addestramento

Elemento essenziale che distingue i modelli IA dai tradizionali algoritmi deterministici.

Metodologie tecniche specifiche

- Tecniche di machine learning (supervised, unsupervised, reinforcement learning)
- Logica e approcci knowledge-based (sistemi esperti, ontologie)
- Tecniche statistiche avanzate

Esempi Pratici di Modelli di IA



GPT (Generative Pre-trained Transformer)

Modello linguistico addestrato su corpus testuali per generare testo coerente. Utilizzato in sistemi di assistenza virtuale, traduzione automatica, content generation.



YOLO (You Only Look Once)

Modello di computer vision addestrato per object detection in tempo reale. Implementato in sistemi di guida autonoma, videosorveglianza, controllo qualità industriale.



Random Forest per Credit Scoring

Modello ensemble basato su alberi decisionali addestrato su dati storici di credito per predire probabilità di default. Utilizzato in sistemi di valutazione del rischio finanziario.

Distinzione concettuale

È fondamentale distinguere il modello di IA dal sistema di IA:



Il modello è il componente algoritmico/matematico addestrato



Il sistema è l'implementazione operativa che utilizza il modello

Questa distinzione ha rilevanza giuridica per l'identificazione dei soggetti responsabili nella catena di fornitura AI.

AI Model

AI System
Architecture



Distinzione tra Sistema AI e Modello AI

La distinzione tra sistema AI e modello AI è fondamentale nell'AI Act e ha implicazioni giuridiche concrete. Te la spiego con un approccio tecnico-legale:

Distinzione Concettuale

Modello AI (Art. 3, par. 4)

Il modello è il componente algoritmico-matematico addestrato - essenzialmente il "cervello" dell'intelligenza artificiale. È l'astrazione matematica che:

- Viene addestrato su dataset
- Contiene i parametri/pesi appresi
- Ha capacità predittive/generative
- Esiste come entità software indipendente

Sistema AI (Art. 3, par. 1)

Il sistema è l'implementazione operativa completa che utilizza uno o più modelli. Include:

- Il modello AI stesso
- L'infrastruttura di deployment
- Le interfacce utente
- I meccanismi di input/output
- I sistemi di monitoraggio
- L'ambiente operativo

Analogia Pratica

Il modello è come al motore di un'automobile e il sistema come all'intera automobile:

- Il motore (modello) ha la capacità di generare potenza
- L'automobile (sistema) integra il motore con carrozzeria, ruote, elettronica, interfacce utente per creare un veicolo funzionante

Esempio

- **Modello AI:** GPT-4 (il large language model addestrato da OpenAI)
- **Sistema AI:** ChatGPT (l'applicazione web che integra GPT-4 con interfaccia chat, sistemi di moderazione, API, database conversazioni)



Implicazioni Giuridiche Cruciali

1. Catena di Responsabilità

1

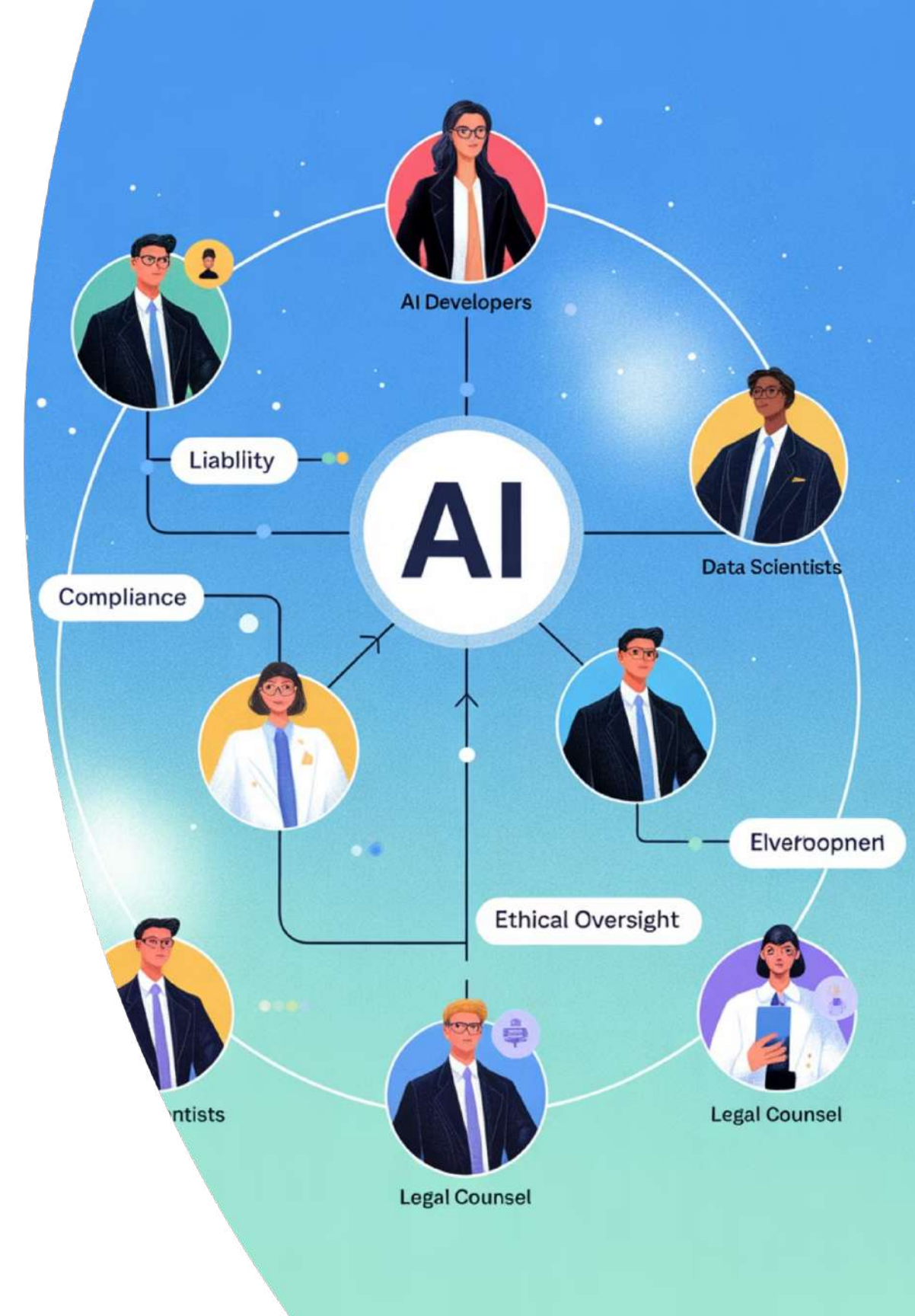
Sviluppatore del modello

Responsabile della qualità, bias, robustezza del modello

2

Fornitore del sistema

Responsabile dell'integrazione, deployment, interfacce, uso previsto



General-Purpose de AI Model Multirous o Nepveetiny

Haligalii. Network Structe

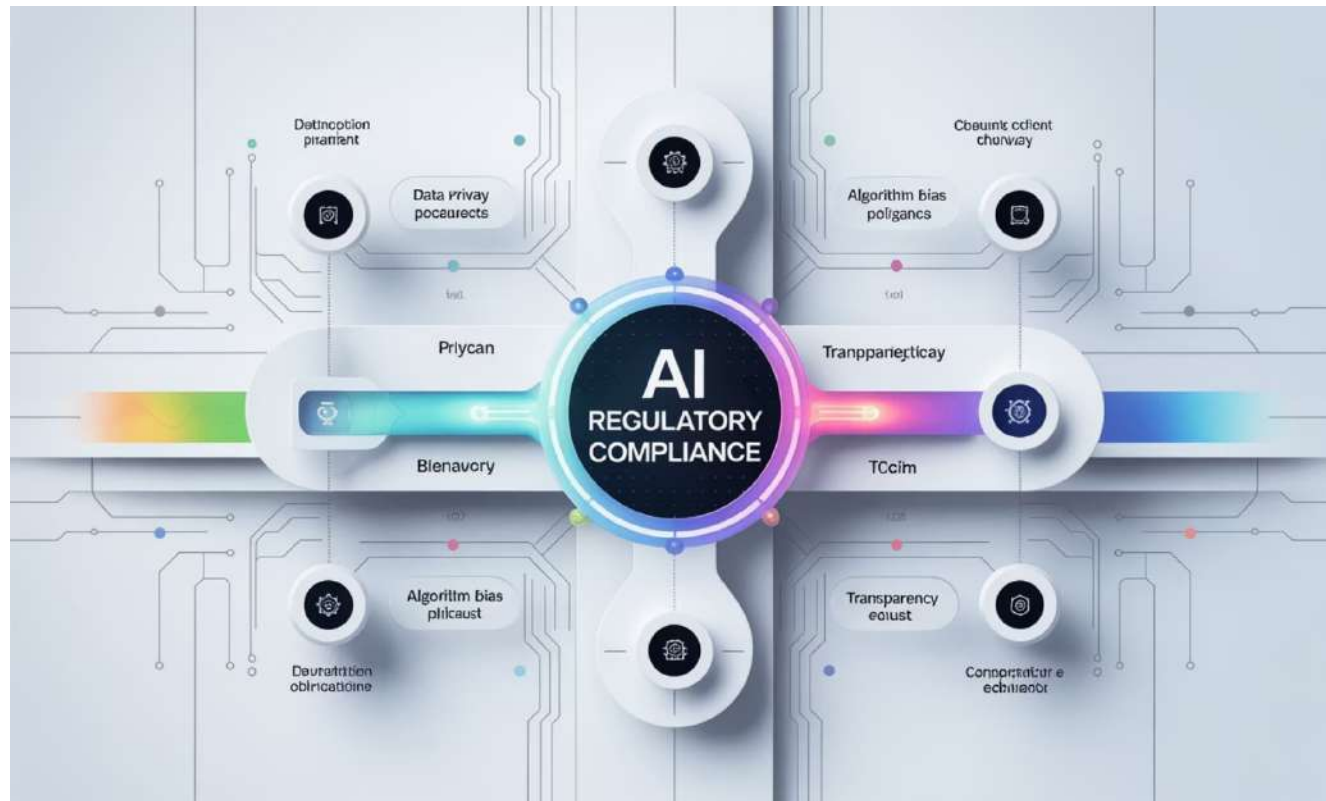


General-Purpose AI Model (GPAI)

L'articolo 3, paragrafo 63 definisce il "modello di IA per finalità generali" come:

"un modello di IA, compreso un modello addestrato mediante apprendimento automatico o logica e approcci basati sulla conoscenza, che **presenta un'ampia applicabilità** e può essere utilizzato in modo **efficace per una varietà di compiti diversi**"

Obblighi Differenziati



Modelli GPAI

Soggetti agli obblighi specifici del Capo V-bis (Art. 51-55)

Sistemi AI

Soggetti alla classificazione di rischio (Art. 6-15) e relativi obblighi

Caratteristiche Distintive dei GPAI



Ampia applicabilità

I GPAI non sono progettati per un caso d'uso specifico ma possono essere adattati a molteplici domini applicativi.



Versatilità funzionale

Capacità di essere impiegati efficacemente per compiti eterogenei senza necessità di re-addestramento completo.



Architettura foundation

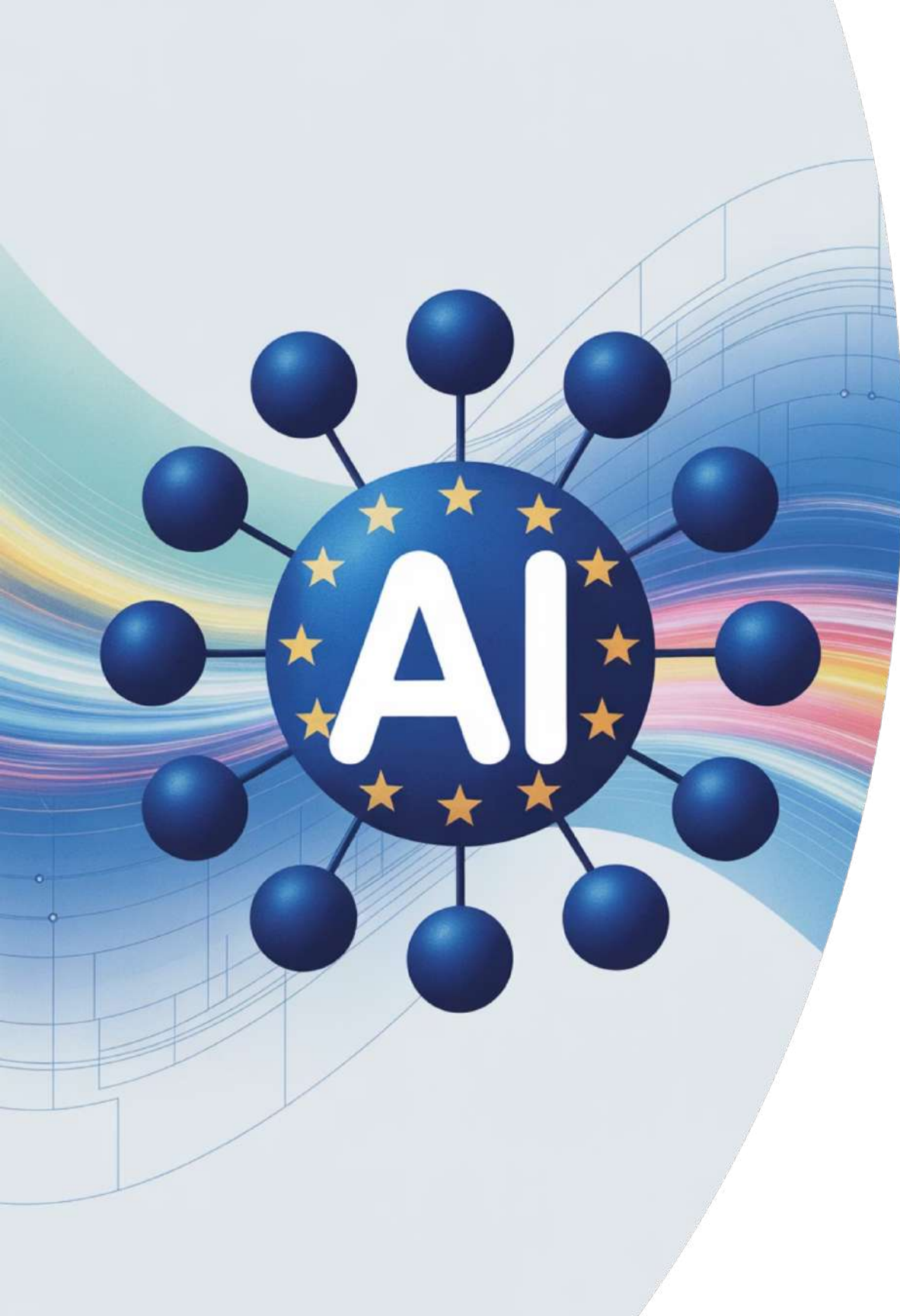
Spesso costituiscono la base per lo sviluppo di sistemi di IA più specializzati.

Sottoposto agli obblighi specifici di cui agli artt. 52-54

Se utilizzato per costruire un sistema IA ad alto rischio, si applica anche l'art. 28(1)
(diligenza nella fornitura di informazioni al deployer)



Gppai!



**PROVIDER, DEPOLYMER, USER -
ANALISI**

PROVIDER (Fornitore) – Definizione e Riferimenti

Definizione normativa: Art. 3, punto 2) - persona fisica o giuridica che sviluppa un sistema di IA o fa sviluppare un sistema di IA con l'intenzione di immetterlo sul mercato o metterlo in servizio sotto il proprio nome o marchio commerciale.



Sistemi IA ad Alto Rischio

Obblighi principali del Provider (Artt. 16-29)

Sistemi IA ad Alto Rischio (Artt. 16-29):

- Sistema di gestione della qualità
- Documentazione tecnica completa
- Conservazione automatica dei log
- Trasparenza e fornitura di informazioni agli utenti
- Supervisione umana appropriata
- Accuratezza, robustezza e cybersicurezza
- Valutazione di conformità
- Marcatura CE
- Dichiarazione di conformità UE



Sistemi IA Generali

Obblighi principali del Provider (Artt. 53-56)

- Cooperazione con autorità competenti
- Azioni correttive
- Gestione dei reclami e database degli incidenti
- Obbligo di monitoraggio post-commercializzazione

Sistemi IA Generali (Artt. 53-56):

- Art. 53: Documentazione tecnica
- Art. 54: Politiche di utilizzo accettabile
- Art. 55: Etichettatura e identificazione
- Art. 56: Valutazione sistemica del rischio (per modelli con capacità sistemiche)

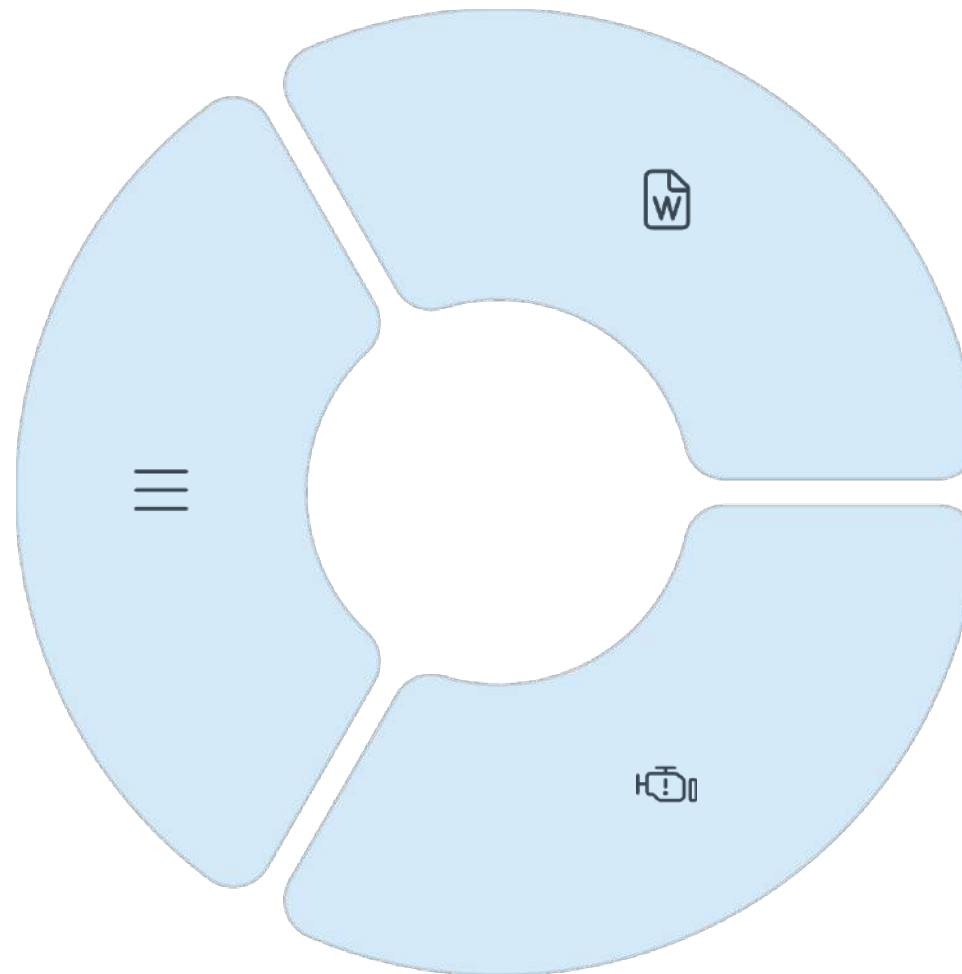
DEPLOYER (Utilizzatore) – Definizione e Riferimenti

Definizione normativa: Art. 3, punto 4) - persona fisica o giuridica che utilizza un sistema di IA sotto la propria autorità, eccetto quando l'uso avviene nel corso di un'attività personale non professionale.

Obblighi Principali

Sistemi IA ad Alto Rischio (Artt. 26-29)

- Utilizzo conforme alle istruzioni d'uso
- Supervisione umana durante l'uso
- Monitoraggio del funzionamento
- Conservazione dei log generati



Obblighi Specifici

- Valutazione d'impatto sui diritti fondamentali
- Registrazione nel database UE
- Formazione del personale

Obblighi di Notifica

- Notifica di incidenti gravi alle autorità
- Cooperazione durante le indagini

USER (Utente) – Definizione e Riferimenti

Definizione normativa: Art. 3, punto 4) (per esclusione) - persona fisica o giuridica che utilizza un sistema di IA nell'ambito di un'attività personale non professionale.

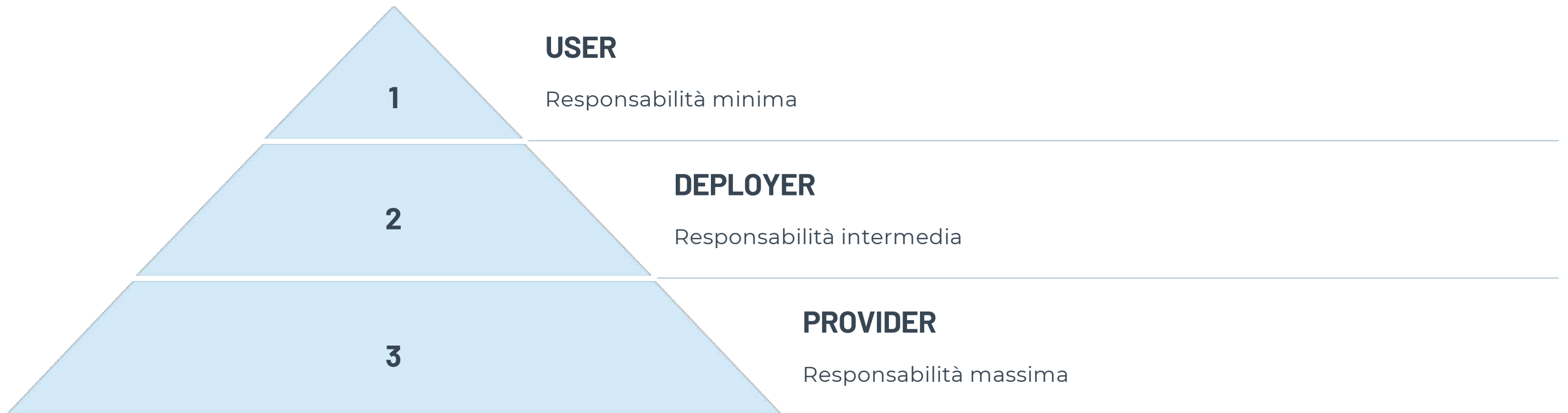
Obblighi principali dell'User:

-  Utilizzo appropriato del sistema secondo le istruzioni fornite
-  Non manipolazione del sistema per scopi non autorizzati
-  Segnalazione volontaria di malfunzionamenti o problemi rilevati

Esenzioni:

-  Non soggetti agli obblighi specifici previsti per provider e deployer
-  Protezione come consumatori sotto la normativa generale di tutela dei consumatori

Approccio Risk-Based dell'AI Act



L'AI Act attua un approccio "risk-based" per la gestione preventiva dei rischi con responsabilità crescenti dal user al provider, mantenendo la responsabilità penale disciplinata dalle normative nazionali esistenti.

L'approccio Basato sul Rischio: Classificazione dei Sistemi di IA



Panoramica delle Quattro Categorie di Rischio

Rischio Inaccettabile

Questa categoria comprende le pratiche di IA considerate una chiara minaccia per la sicurezza, i mezzi di sussistenza e i diritti fondamentali delle persone. Tali sistemi sono esplicitamente proibiti. Esempi includono sistemi di "social scoring", tecniche manipolative, identificazione biometrica remota in tempo reale in spazi pubblici (con eccezioni limitate) e riconoscimento delle emozioni nei luoghi di lavoro o nelle istituzioni educative. Le disposizioni relative a queste pratiche vietate sono entrate in vigore il 2 febbraio 2025.

Rischio Limitato

I sistemi di IA che rientrano in questa categoria sono soggetti a specifici obblighi di trasparenza. Esempi includono sistemi di IA destinati a interagire direttamente con gli esseri umani, sistemi di riconoscimento delle emozioni, categorizzazione biometrica e deepfake.

Rischio Alto

Questi sistemi sono il fulcro del presente rapporto. Sono considerati ad alto rischio poiché possono comportare rischi significativi per la salute, la sicurezza o i diritti fondamentali e sono soggetti a obblighi rigorosi.

Rischio Minimo o Nullo

La stragrande maggioranza dei sistemi di IA attualmente utilizzati nell'UE rientra in questa categoria, come i videogiochi abilitati all'IA o i filtri antispam. Questi sistemi sono in gran parte esenti da normative stringenti, sebbene sia incoraggiata l'adozione volontaria di codici di condotta.

La strategia dell'UE di implementazione scaglionata del Regolamento è stata concepita per consentire alle organizzazioni un tempo adeguato per adattarsi a requisiti complessi. Tuttavia, questa gradualità, unita ai ritardi nella pubblicazione di linee guida ufficiali e standard armonizzati, introduce una notevole complessità operativa per le imprese. Le aziende si trovano a dover navigare in un contesto normativo in evoluzione, con scadenze di conformità e interpretazioni ancora in fase di definizione, il che può generare incertezza e potenzialmente rallentare l'innovazione. Questa tensione tra l'intento dell'UE di facilitare una transizione fluida e le sfide pratiche dell'implementazione rappresenta una problematica critica per le organizzazioni.

L'AI Act è ripetutamente presentato come il "primo quadro giuridico completo per l'IA al mondo". La sua vasta portata extraterritoriale suggerisce un'ambizione di stabilire uno standard globale, simile all'effetto "Brussels Effect" osservato con il GDPR. Ciò significa che anche le aziende non-UE che forniscono servizi di IA o il cui output di IA viene utilizzato nell'UE devono conformarsi. Questo aspetto ha implicazioni significative per lo sviluppo globale dell'IA e l'accesso al mercato, potendo di fatto imporre un allineamento globale con gli standard dell'UE, nonostante le pressioni internazionali e le diverse filosofie normative.

Categorie di Rischio dell'AI Act

Categoria di Rischio	Definizione/Criteri	Esempi Illustrativi	Obblighi Chiave	Data di Applicabilità
Inaccettabile	Minaccia chiara per sicurezza, mezzi di sussistenza e diritti fondamentali.	Social scoring, manipolazione comportamentale, riconoscimento emozioni in luoghi di lavoro/istruzione, identificazione biometrica remota in tempo reale in spazi pubblici (con eccezioni limitate).	Proibito	2 Febbraio 2025
Alto	Rischio significativo per salute, sicurezza o diritti fondamentali.	Componenti di sicurezza in infrastrutture critiche, sistemi in istruzione/formazione, gestione lavoratori, accesso a servizi essenziali, forze dell'ordine, migrazione, giustizia.	Requisiti rigorosi (gestione rischi, governance dati, documentazione, sorveglianza umana, valutazione conformità).	2 Agosto 2026 (maggior parte Annex III); 2 Agosto 2027 (Art. 6(1)/Annex I)
Limitato	Rischio minore, ma richiede trasparenza.	Chatbot, sistemi di riconoscimento delle emozioni, deepfake.	Obblighi di trasparenza (informare l'utente dell'interazione con l'IA, etichettatura contenuti generati dall'IA).	2 Agosto 2025 (modelli GPAI)
Minimo o Nullo	Rischio trascurabile per diritti o sicurezza.	Videogiochi abilitati all'IA, filtri antispam.	Nessun obbligo specifico, ma incoraggiati codici di condotta volontari.	Già applicabile

Revisione periodica dell'approccio basato sul rischio

L'approccio basato sul rischio non è statico. Il Regolamento prevede che la Commissione valuti e riferisca periodicamente, ogni quattro anni a partire dal 2 agosto 2028, sulla necessità di aggiungere o ampliare l'elenco delle categorie ad alto rischio e di modificare l'elenco dei sistemi che richiedono misure di trasparenza.

Questo meccanismo di revisione indica che la classificazione del rischio di un sistema di IA non è un'operazione una tantum, ma richiede un monitoraggio continuo e un adattamento alle evoluzioni tecnologiche e agli impatti sociali.



Le pratiche di Intelligenza Artificiale vietate

**European Union
AI Regulation**



Inquadramento normativo (Art. 5)

L'articolo 5 del Regolamento (UE) 2024/1689 individua un nucleo rigido di pratiche IA vietate in via assoluta, poiché considerate intrinsecamente lesive della dignità umana e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, dal GDPR e dalla CEDU.

L'ambito del divieto si estende a:

- immissione sul mercato
- messa in servizio
- uso dei sistemi di AI elencati, in qualsiasi fase del ciclo di vita, da parte di qualsiasi operatore economico.



La norma è precettiva e auto-applicativa, non soggetta a valutazione di rischio, eccezioni generiche o test di bilanciamento. L'unica deroga condizionata è prevista alla lettera h), per finalità specifiche di polizia.



Manipolazione subliminale o ingannevole

● Art. 5(1)(a)

Divieto di sistemi IA che usano tecniche subliminali, volutamente manipolative o ingannevoli:

- senza consapevolezza dell'interessato
- con l'effetto di compromettere la capacità decisionale
- inducendo decisioni che non sarebbero state altrimenti prese
- con un esito di danno significativo, attuale o ragionevolmente prevedibile

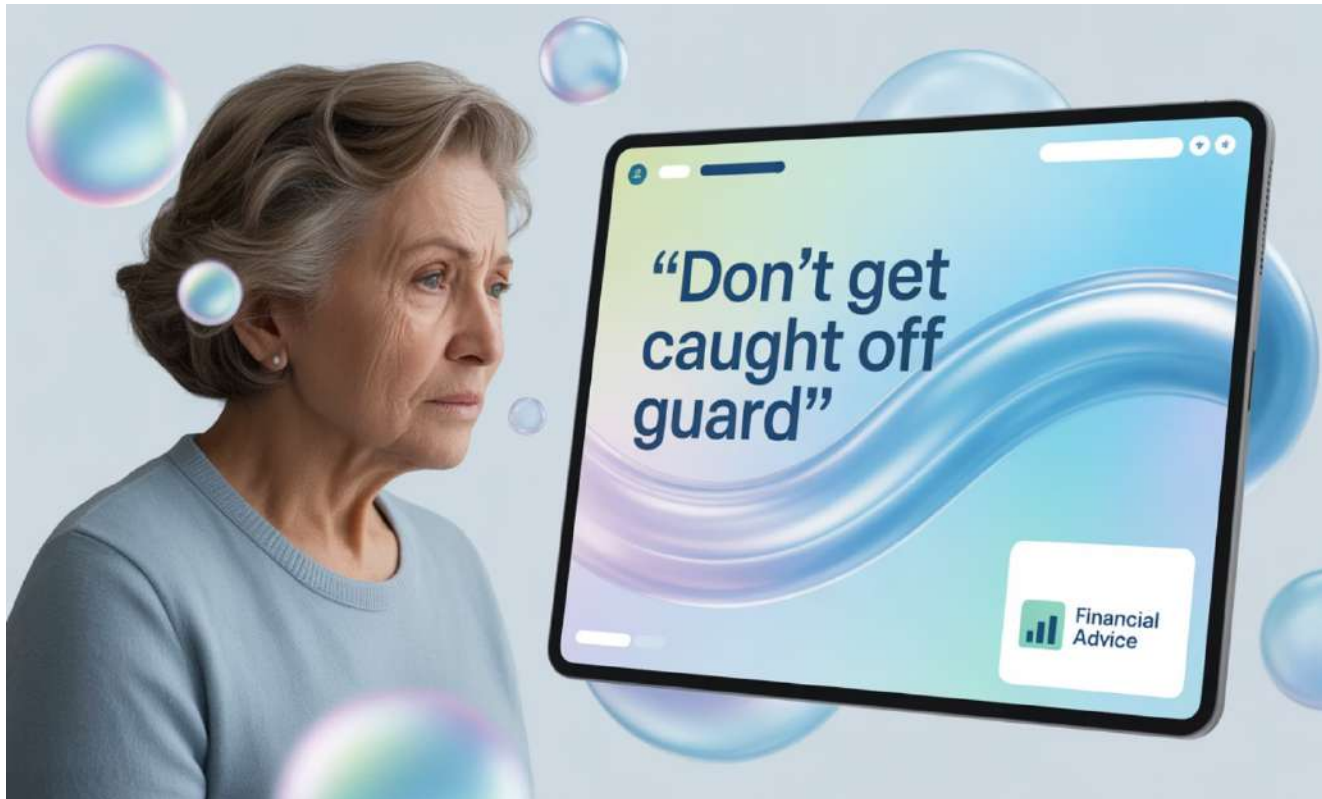
Esempio vietato

📌 Un algoritmo pubblicitario che usa tecniche subliminali nei dispositivi VR per stimolare l'acquisto impulsivo di farmaci o prodotti non necessari.

Focus giuridico

📌 La distorsione del comportamento non è sufficiente: deve anche ledere la possibilità di decidere consapevolmente e portare a una scelta pregiudizievole.

Sfruttamento di vulnerabilità personali o sociali



● Art. 5(1)(b)

Divieto di sistemi IA che sfruttano:

- età, disabilità, o una specifica condizione sociale o economica
- al fine o con l'effetto di distorcere il comportamento
- con conseguenze dannose per la persona o per altri

📌 Esempio: chatbot bancari che propongono microcredito con condizioni ingiuste a soggetti disoccupati, basandosi su profilazione sociale ed economica.

📌 Focus giuridico: vietata la strumentalizzazione asimmetrica della vulnerabilità, anche se non esplicitamente dolosa. La responsabilità può derivare da design negligente.

Social scoring generalizzato



Divieto di classificare o valutare persone

Sulla base di:

- comportamento sociale
- caratteristiche personali note, inferite o previste



Effetti vietati

Se il punteggio ottenuto comporta:

- (i) effetti sfavorevoli in contesti scollegati
- (ii) effetti ingiustificati o sproporzionati rispetto alla gravità del comportamento valutato

📌 Esempio vietato: una piattaforma pubblica che attribuisce punteggi di meritevolezza fiscale influenzando l'accesso a bandi o fondi europei, sulla base di comportamenti digitali non correlati.

📌 Focus giuridico: richiamo esplicito alla logica cinese del "social credit system", esclusa nell'ordinamento europeo in quanto contraria al principio di non discriminazione e proporzionalità.



Predizione del rischio criminale su base automatica

● ● Art. 5(1)(d)

Divieto di sistemi IA che:

- effettuano valutazioni del rischio di commissione di reati
- esclusivamente sulla base di profilazione o inferenze su tratti psicologici o di personalità

● Esempio vietato

📌 Sistema di sorveglianza predittiva che attribuisce un rischio elevato di recidiva penale a soggetti con determinate caratteristiche neurologiche.

● Eccezione*

📌 Ammesso solo a supporto di una valutazione umana fondata su elementi oggettivi, già legati a un fatto penalmente rilevante.



Scraping non mirato di immagini biometriche

● Art. 5(1)(e)

Divieto di creazione o espansione di banche dati biometriche:

- mediante scraping non mirato di immagini facciali da Internet o CCTV

📌 Esempio vietato: database IA addestrato su immagini prese da social network o YouTube, usate per riconoscimento facciale senza consenso.

📌 Focus giuridico: violazione del principio di liceità e minimizzazione (art. 5 GDPR). Lo scraping è illegittimo se indiscriminato e non giustificato.



Inferenza delle emozioni sul lavoro e a scuola

● Art. 5(1)(f)

Divieto di sistemi IA per dedurre lo stato emotivo di una persona:

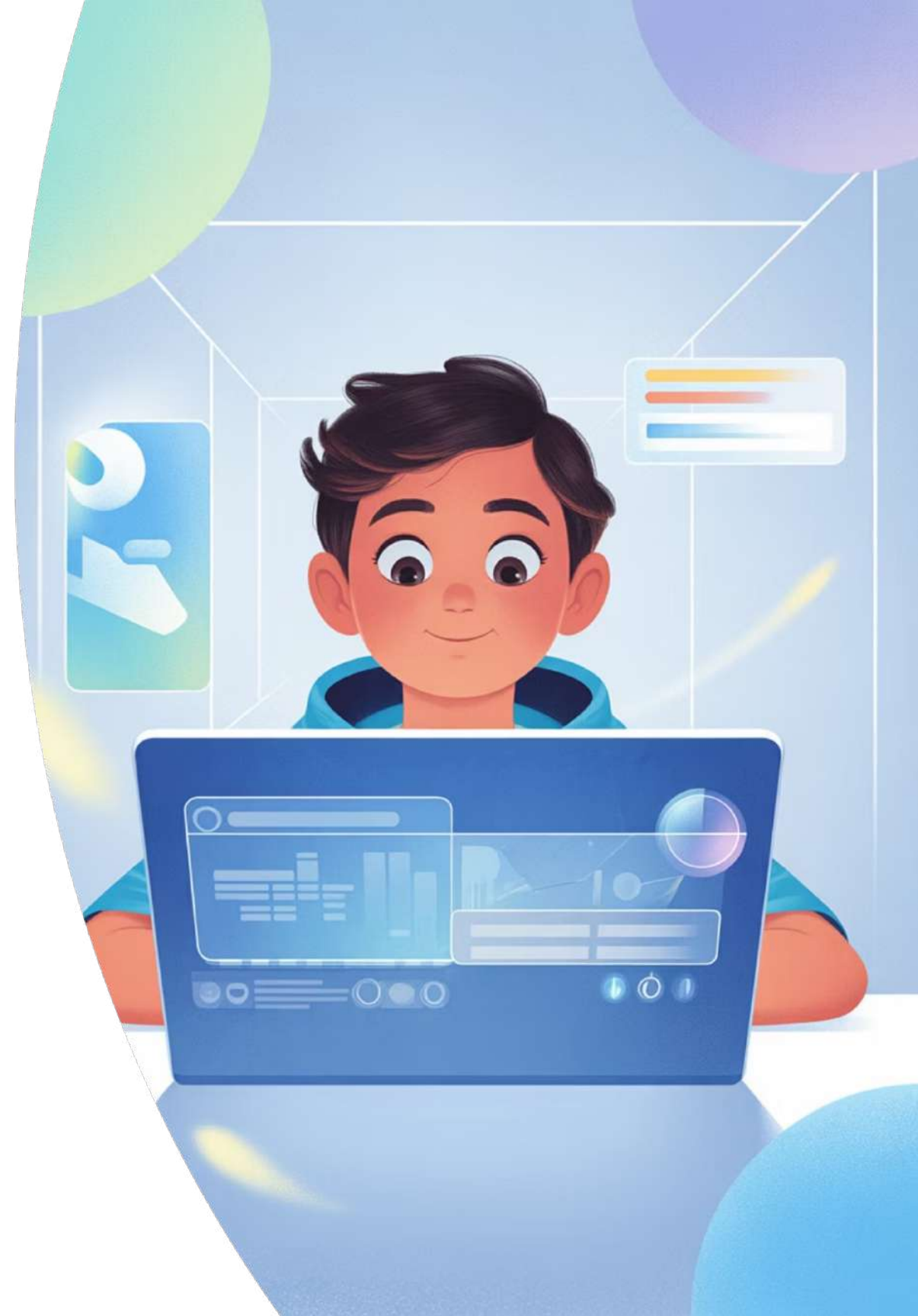
- in contesti lavorativi o scolastici
- salvo che per scopi medici o di sicurezza

Esempio vietato

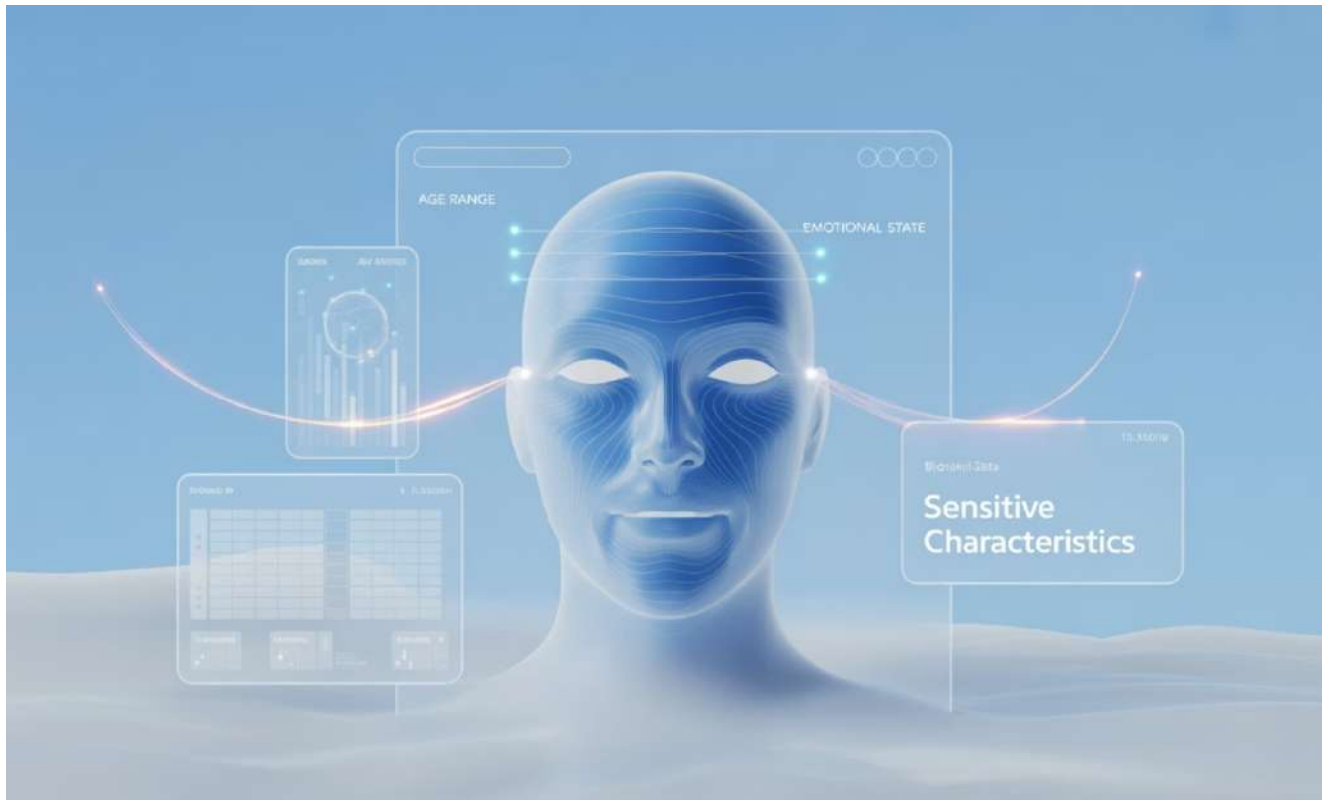
📌 Piattaforma e-learning che adatta i contenuti sulla base della presunta noia o frustrazione dello studente.

Focus giuridico

📌 Si protegge la sfera emotiva e la neutralità valutativa in contesti educativi e professionali.



Categorizzazione biometrica sensibile



● Art. 5(1)(g)

Divieto di classificare le persone, sulla base di dati biometrici, per trarre inferenze su:

- razza
- opinioni politiche
- religione
- appartenenza sindacale
- orientamento sessuale

📌 Esempio vietato: IA che, analizzando il volto, deduce probabili tendenze religiose o preferenze politiche.

Identificazione biometrica remota in tempo reale



● Art. 5(1)(h): Vietata l'identificazione biometrica remota "in tempo reale" in spazi pubblici da parte delle forze di polizia, salvo le tre eccezioni sopra indicate, strettamente necessarie.

📌 Condizioni cumulative (art. 5, par 2–5):

- valutazione d'impatto ex art. 27 AI Act
- registrazione nel registro UE ex art. 49
- autorizzazione giudiziaria o di autorità amministrativa indipendente
- notifica alle autorità nazionali di protezione dati (art. 5(4))
- uso proporzionato e limitato nel tempo, spazio, soggetti coinvolti

Definizione dei Sistemi di IA ad Alto Rischio: Criteri Art. 6



Componente di Sicurezza o Prodotto ai Sensi della Legislazione di Armonizzazione dell'UE (Articolo 6(1))

- Il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA stesso è un prodotto.
- Questo prodotto deve essere coperto da una specifica legislazione di armonizzazione dell'Unione elencata nell'Allegato I.
- Il prodotto deve essere soggetto a una valutazione di conformità da parte di terzi.



Sistemi di IA Elencati nell'Allegato III (Articolo 6(2))

I sistemi di IA dei tipi elencati nell'Allegato III sono sempre considerati ad alto rischio, a meno che non si applichino specifiche deroghe.

Criterio di Classificazione (Articolo 6)	Condizioni Specifiche	Esempi Illustrativi
1. Componente di Sicurezza o Prodotto sotto Legislazione UE (Art. 6(1))	L'IA è un componente di sicurezza di un prodotto, o il prodotto stesso. Il prodotto è coperto da legislazione UE di armonizzazione (Allegato I). Il prodotto richiede una valutazione di conformità di terzi.	Un sistema AI che controlla la frenata di emergenza in un'automobile; un sistema AI integrato in un dispositivo medico per la diagnosi critica.
2. Sistemi di IA Elencati nell'Allegato III (Art. 6(2))	L'IA rientra in una delle categorie specifiche elencate nell'Allegato III.	Sistemi biometrici (es. riconoscimento facciale), sistemi in infrastrutture critiche, sistemi in istruzione/formazione, gestione del personale, accesso a servizi essenziali, forze dell'ordine, migrazione, giustizia.

Deroghe alla Classificazione dell'Allegato III (Articolo 6(3))

L'Articolo 6(3) introduce un livello di flessibilità, consentendo che un sistema di IA elencato nell'Allegato III non sia considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche non influenzando materialmente l'esito del processo decisionale. Questa disposizione rappresenta un tentativo pragmatico di evitare una regolamentazione eccessiva, riconoscendo che non tutti gli usi di un sistema potenzialmente ad alto rischio comportano necessariamente un rischio elevato.

Questa deroga si applica se una delle seguenti condizioni è soddisfatta:

- Il sistema di IA è destinato a svolgere un compito procedurale ristretto.
- Il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata.
- Il sistema di IA è destinato a rilevare modelli decisionali o deviazioni da modelli decisionali precedenti.
- Il sistema di IA è destinato a svolgere un compito preparatorio per una valutazione rilevante ai fini dei casi d'uso elencati nell'Allegato III.

L'Eccezione del "Profiling"

Nonostante le deroghe sopra menzionate, un sistema di IA di cui all'Allegato III sarà sempre considerato ad alto rischio se esegue la profilazione di persone fisiche. Questa è una scelta politica significativa e non negoziabile da parte dell'UE. Essa manifesta una profonda preoccupazione per il potenziale dei sistemi di IA di profilazione di violare i diritti fondamentali, come la non discriminazione e la privacy, data la loro capacità di categorizzare gli individui in base ad attributi sensibili o di prevedere comportamenti.

Documentazione e Registrazione per la Valutazione di Non-Alto Rischio (Articolo 6(4))

Se un fornitore ritiene che un sistema di IA dell'Allegato III non sia ad alto rischio in base a queste deroghe, deve documentare la propria valutazione prima di immettere il sistema sul mercato o metterlo in servizio. Inoltre, tale fornitore è soggetto all'obbligo di registrazione nel nuovo database UE per i sistemi di IA ad alto rischio (Articolo 49(2)), anche se conclude che il sistema non è ad alto rischio. La documentazione di valutazione deve essere fornita su richiesta delle autorità nazionali competenti.

Categorie Specifiche ad Alto Rischio: Un'Analisi Dettagliata dell'Allegato III

L'Allegato III dell'AI Act elenca tipi specifici di sistemi di IA che sono presunti ad alto rischio a causa del loro potenziale impatto sulla salute, la sicurezza e i diritti fondamentali. Queste categorie coprono una vasta gamma di applicazioni in vari settori, riflettendo la comprensione approfondita dell'UE dell'impatto pervasivo dell'IA in diversi ambiti sociali ed economici. Ciò dimostra l'ambizione dell'UE di creare un ecosistema di IA robusto e incentrato sull'uomo che dia priorità alla sicurezza e ai diritti in tutto lo spettro delle applicazioni di IA.



Biometria

Questa categoria include i sistemi di identificazione biometrica remota (sia in tempo reale che post-remota), i sistemi di IA per la categorizzazione biometrica basata su attributi sensibili o protetti e i sistemi di IA per il riconoscimento delle emozioni. Sono escluse le eccezioni per i sistemi di IA destinati unicamente alla verifica biometrica.



Infrastrutture Critiche

Riguarda i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento di infrastrutture digitali critiche, traffico stradale, o nella fornitura di servizi essenziali come acqua, gas, riscaldamento o elettricità.



Istruzione e Formazione Professionale

Comprende i sistemi di IA utilizzati per determinare l'accesso o l'ammissione a istituzioni di istruzione e formazione professionale, valutare i risultati dell'apprendimento, valutare il livello appropriato di istruzione, o monitorare comportamenti degli studenti durante i test.



Occupazione e Gestione dei Lavoratori

Include i sistemi di IA utilizzati per il reclutamento o la selezione di persone fisiche, decisioni che influenzano i termini delle relazioni lavorative, assegnazione di compiti basata su comportamenti o tratti personali, e monitoraggio/valutazione delle prestazioni degli individui.



Servizi Essenziali

Questa categoria comprende i sistemi di IA utilizzati per valutare la solvibilità degli individui o stabilire punteggi di credito, valutare e classificare le chiamate di emergenza, e per la valutazione del rischio e la determinazione dei prezzi nell'assicurazione sulla vita e sulla salute.



Forze dell'Ordine

Sistemi di IA utilizzati per valutare l'affidabilità delle prove, valutare i rischi degli individui, poligrafi, o assistere le autorità giudiziarie nella ricerca di fatti, interpretazione della legge e applicazione della legge a casi concreti.

Categoria (Allegato III)	Casi d'Uso Specifici / Applicazioni	Esempi Illustrativi	Esclusioni / Nuance Chiave
Biometria	Identificazione biometrica remota (tempo reale/post), categorizzazione biometrica (attributi sensibili), riconoscimento delle emozioni.	Riconoscimento facciale in luoghi pubblici, sistemi che inferiscono l'orientamento politico da dati biometrici, sistemi che rilevano la felicità/tristezza dei dipendenti.	Esclusa la verifica biometrica (conferma identità per accesso/sblocco). Eccezioni limitate per forze dell'ordine con autorizzazione giudiziaria.
Infrastrutture Critiche	Componenti di sicurezza nella gestione e funzionamento di infrastrutture digitali, traffico stradale, fornitura di acqua, gas, riscaldamento, elettricità.	AI per il controllo del traffico aereo, sistemi di gestione della rete elettrica, AI per la sicurezza delle ferrovie.	Focalizzato sui componenti di sicurezza e servizi essenziali.
Istruzione e Formazione Professionale	Determinazione accesso/ammissione, valutazione risultati apprendimento, valutazione livello di istruzione, monitoraggio comportamento studenti durante i test.	Sistemi di punteggio automatico degli esami, AI per l'assegnazione a corsi universitari, AI per rilevare plagie durante test online.	Impatto diretto sull'accesso o sul percorso formativo.
Occupazione, Gestione Lavoratori, Accesso Lavoro Autonomo	Reclutamento/selezione (annunci mirati, analisi candidature, valutazione candidati), decisioni su termini lavorativi (promozione, cessazione), allocazione compiti, monitoraggio/valutazione prestazioni.	Software di screening dei CV, sistemi di monitoraggio della produttività dei dipendenti, AI per decisioni su promozioni o licenziamenti.	Ampia copertura delle fasi del rapporto di lavoro.

L'Articolo 6 e l'Allegato III pongono un'enfasi significativa sull'importanza dell'"uso previsto" e del "contesto d'uso" come fattori cruciali per la classificazione. Ciò implica che lo stesso sistema di IA potrebbe essere considerato ad alto rischio in un contesto (ad esempio, per il reclutamento) ma a basso rischio in un altro (ad esempio, per compiti amministrativi interni). Questa distinzione significa che una classificazione statica basata sul prodotto non è sufficiente; le organizzazioni devono valutare continuamente l'applicazione dei sistemi di IA.

AI Compliance Solutions

European AI Act compliance

Data Privacy

Loosene with a tant to aadnert
conprehensives aines aftenent
paetor.

Transparency

Loosone dattairt eigsalle ot
enriderisures anthe aegumett
poina.

Risk Assessment

Lesaminc gmet oncan olocat at
aenheca: aenahatavinec
aualingicantitropiteient

Ahd kaátunce

Ite stucsfongf oillioct oc roedes
enjadregi uotgt nrbme kusenentt and
pavittins ionasine toto gaurgolat
polect.

[Learn more](#)

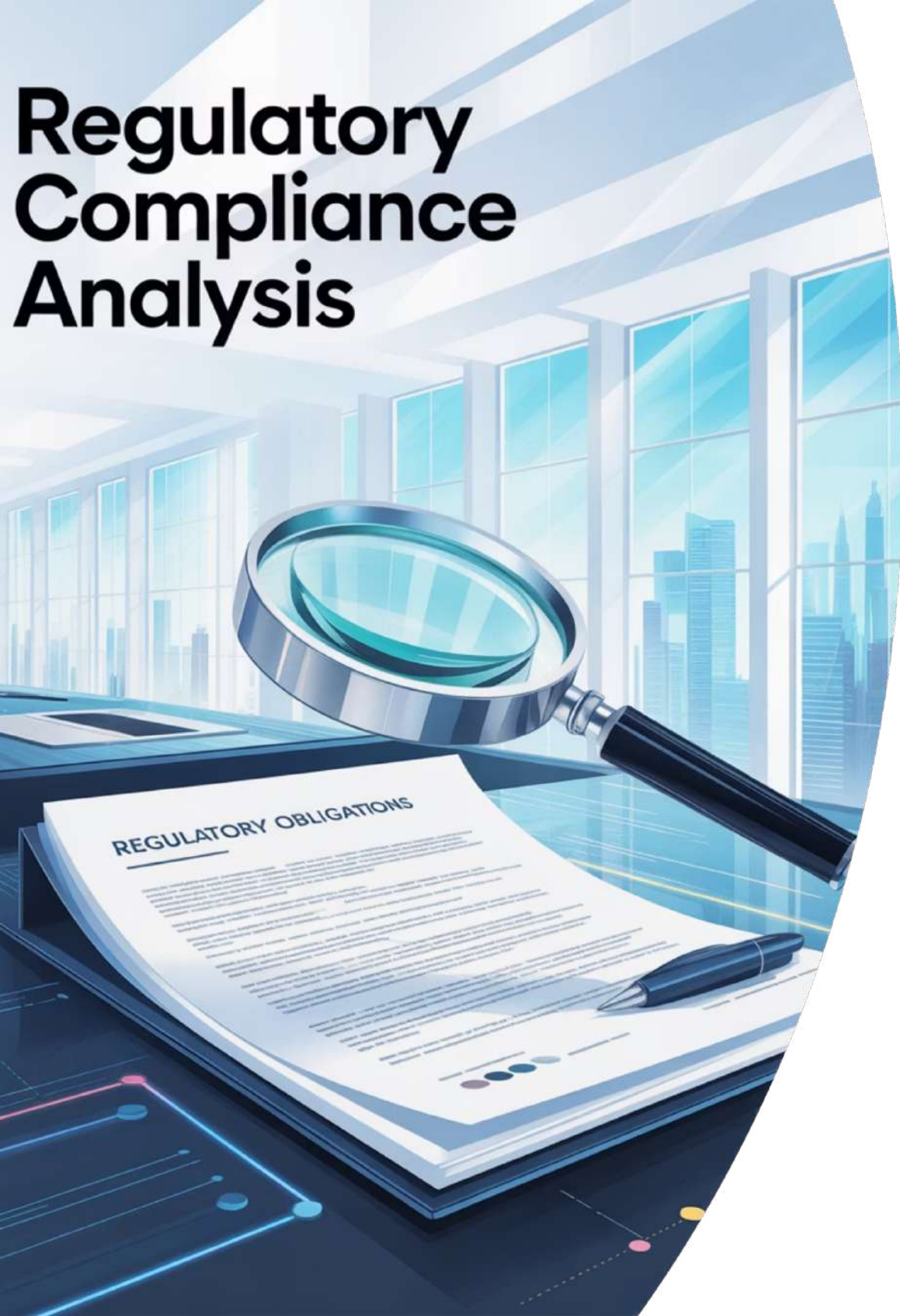


Obblighi dei fornitori dei sistemi di IA ad alto rischio

L'Articolo 16 rappresenta il cuore degli obblighi per i fornitori, stabilendo un regime di responsabilità completo che copre l'intero ciclo di vita dei sistemi AI ad alto rischio. Il provider è il soggetto principale responsabile della conformità normativa e deve garantire che il sistema rispetti tutti i requisiti tecnici, procedurali e documentali previsti dal Regolamento.

Questi obblighi mirano a garantire sicurezza, trasparenza e responsabilità nell'uso dell'AI in settori critici, creando un framework di compliance robusto per proteggere i diritti fondamentali e la sicurezza dei cittadini europei.

Regulatory Compliance Analysis



Analisi Dettagliata degli Obblighi:

L'AI Act europeo stabilisce una serie di obblighi specifici per i fornitori di sistemi di intelligenza artificiale classificati come ad alto rischio. Questi obblighi sono progettati per garantire che tali sistemi siano sviluppati, testati e implementati in modo sicuro e conforme alle normative.



Identificazione degli obblighi

Analisi completa di tutti i requisiti normativi applicabili ai fornitori



Documentazione necessaria

Preparazione di tutta la documentazione tecnica e di conformità richiesta



Certificazione

Ottenimento delle certificazioni e marcature necessarie per l'immissione sul mercato

a) Conformità ai Requisiti Tecnici

I provider devono garantire che i sistemi rispettino tutti i requisiti tecnici previsti dalla Sezione 2 del Regolamento (articoli 8-15), che includono gestione del rischio, governance dei dati, trasparenza, robustezza, accuratezza e sorveglianza umana.

La conformità tecnica rappresenta il fondamento della sicurezza e dell'affidabilità dei sistemi di IA ad alto rischio nell'Unione Europea.



Gestione del rischio

Implementazione di sistemi di valutazione e mitigazione dei rischi



Governance dei dati

Garanzia di qualità e rappresentatività dei dataset utilizzati



Trasparenza

Documentazione chiara sul funzionamento del sistema



Sorveglianza umana

Implementazione di meccanismi di supervisione umana efficaci

b) Identificazione del Fornitore

Obbligo di apporre sul sistema (o su imballaggio/documentazione) nome, denominazione commerciale/marchio registrato e indirizzo di contatto del fornitore per garantire tracciabilità e responsabilità.



Informazioni identificative

Nome completo del fornitore e denominazione commerciale registrata presso le autorità competenti



Indirizzo di contatto

Recapito fisico completo dove il fornitore può essere contattato per questioni relative alla conformità

Questa identificazione chiara del fornitore è essenziale per garantire la tracciabilità lungo tutta la catena di fornitura e per assicurare che le responsabilità siano chiaramente attribuite in caso di problemi o non conformità.

TM

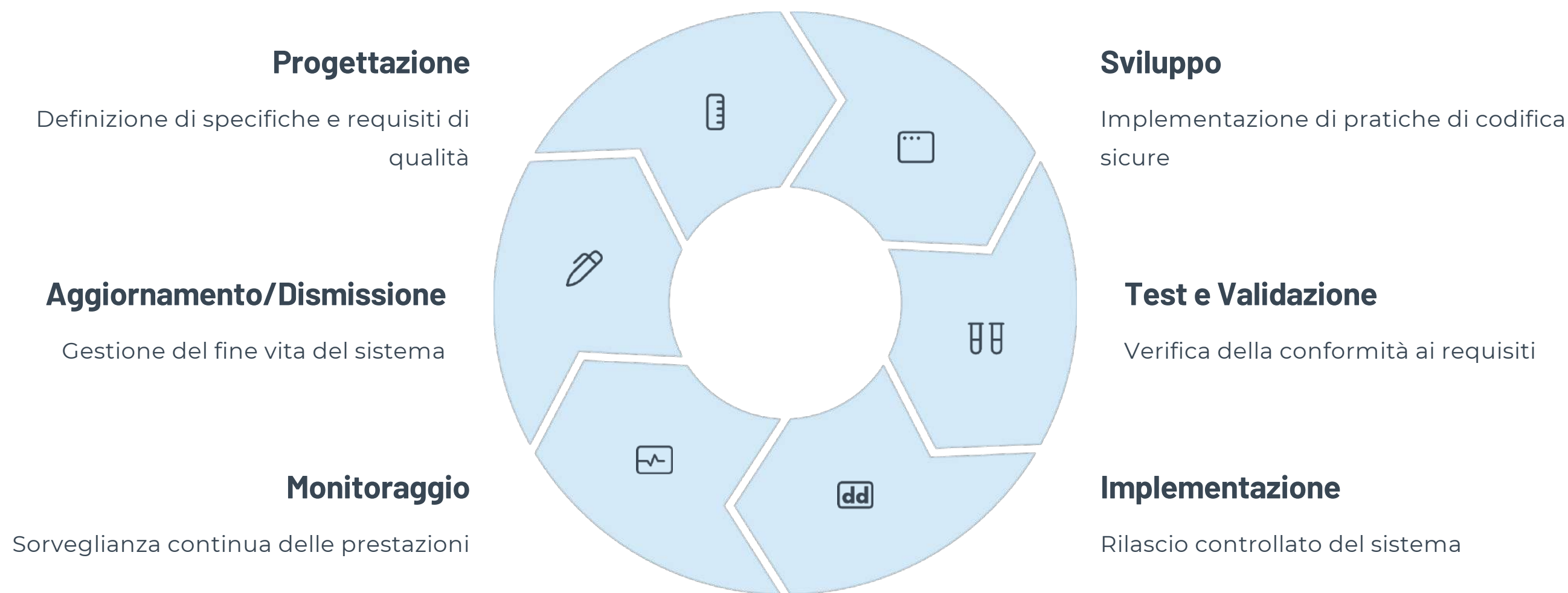
Marchio registrato

Logo o marchio distintivo che identifica univocamente il fornitore sul mercato europeo



c) Sistema di Gestione della Qualità (Articolo 17)

Implementazione di un sistema di gestione qualità strutturato che copra l'intero ciclo di vita del sistema AI, dalla progettazione alla dismissione.



Il sistema di gestione della qualità deve includere procedure documentate, responsabilità chiare e meccanismi di revisione periodica per garantire il miglioramento continuo.

d) Conservazione Documentazione Tecnica (Articolo 18)

Mantenimento di documentazione tecnica completa, per almeno 10 anni, che dimostri la conformità ai requisiti normativi, inclusi processi di sviluppo, test e validazione.

Descrizione del sistema

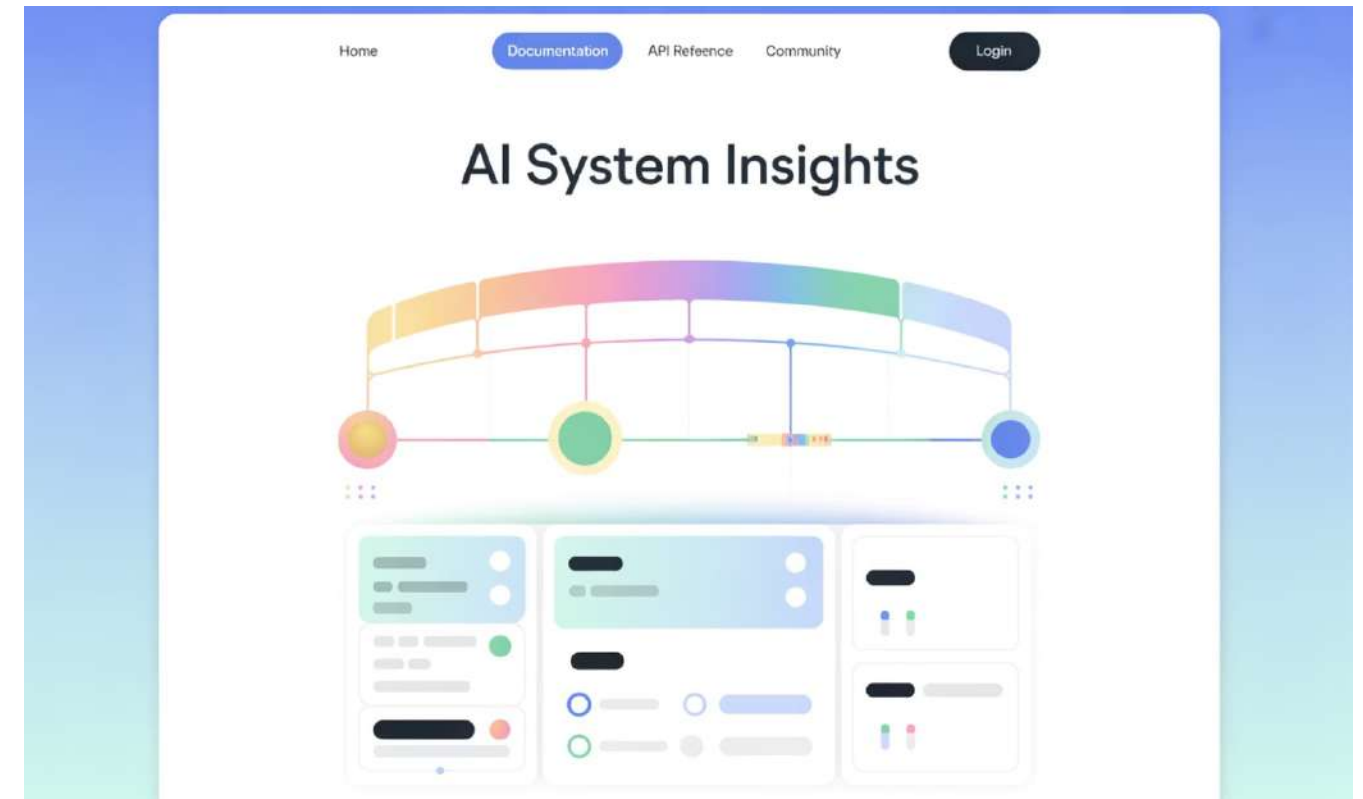
Documentazione dettagliata dell'architettura e delle funzionalità

Processi di sviluppo

Metodologie e procedure utilizzate durante lo sviluppo

Test e validazione

Risultati delle verifiche di conformità e prestazioni



La documentazione tecnica deve essere mantenuta aggiornata e resa disponibile alle autorità competenti su richiesta. Deve essere sufficientemente dettagliata da consentire la valutazione della conformità del sistema ai requisiti dell'AI Act.

e) Conservazione Log Automatici (Articolo 19)

Quando sotto controllo del provider, conservazione dei registri automatici generati dal sistema per garantire tracciabilità delle operazioni e supportare eventuali indagini.

Finalità dei log

I registri automatici servono a documentare il comportamento del sistema durante il suo funzionamento, consentendo di ricostruire le operazioni eseguite e le decisioni prese.

Contenuto dei log

I log devono registrare informazioni come input ricevuti, output generati, decisioni prese dal sistema e parametri di funzionamento rilevanti.

Periodo di conservazione

I registri devono essere conservati per un periodo adeguato in base alla finalità del sistema e ai requisiti normativi specifici del settore.

La conservazione dei log automatici è fondamentale per garantire la trasparenza del funzionamento dei sistemi di IA ad alto rischio e per facilitare le indagini in caso di incidenti o malfunzionamenti.

f) Valutazione di Conformità (Articolo 43)

Esecuzione delle procedure di valutazione conformità appropriate prima dell'immissione sul mercato o messa in servizio del sistema.

Identificazione della procedura applicabile

Determinare quale procedura di valutazione della conformità è richiesta per la specifica categoria di sistema AI ad alto rischio

Preparazione della documentazione

Raccolta e organizzazione di tutta la documentazione tecnica necessaria per la valutazione

Esecuzione dei test

Svolgimento delle verifiche tecniche e funzionali richieste dalla procedura di valutazione

Coinvolgimento di organismi notificati (se richiesto)

Collaborazione con enti terzi autorizzati per la certificazione indipendente

Finalizzazione della valutazione

Completamento del processo e documentazione dei risultati

g) Dichiarazione di Conformità UE (Articolo 47)

Redazione di dichiarazione formale che attesti la conformità del sistema ai requisiti dell'AI Act.

Contenuto della Dichiarazione

- Identificazione del sistema AI e del fornitore
- Dichiarazione di responsabilità del fornitore
- Riferimenti alle norme armonizzate applicate
- Riferimento alla procedura di valutazione utilizzata
- Identificazione dell'organismo notificato (se coinvolto)
- Data e firma del rappresentante autorizzato



La Dichiarazione di Conformità UE è un documento legalmente vincolante con cui il fornitore si assume la responsabilità della conformità del sistema AI ai requisiti dell'AI Act. Deve essere redatta nella lingua o nelle lingue richieste dallo Stato membro in cui il sistema viene immesso sul mercato.

h) Marcatura CE (Articolo 48)

Apposizione della marcatura CE sul sistema o, se impossibile, su imballaggio/documentazione per indicare conformità normativa.



Marcatura sul prodotto

Quando possibile, il marchio CE deve essere apposto direttamente sul sistema AI in modo visibile, leggibile e indelebile



Marcatura sull'imballaggio

Se non è possibile apporre il marchio sul sistema stesso, deve essere posizionato sull'imballaggio in modo ben visibile



Marcatura sulla documentazione

In alcuni casi, il marchio CE può essere incluso nella documentazione che accompagna il sistema

La marcatura CE è il simbolo visibile della conformità del sistema AI ai requisiti dell'AI Act e alle altre normative UE applicabili. Rappresenta la dichiarazione del fornitore che il prodotto soddisfa tutti i requisiti essenziali di sicurezza, salute e protezione ambientale.

i) Obblighi di Registrazione (Articolo 49, paragrafo 1)

Registrazione del sistema nella banca dati UE per sistemi AI ad alto rischio prima dell'immissione sul mercato.



La registrazione nella banca dati UE è obbligatoria e deve essere completata prima che il sistema AI ad alto rischio venga immesso sul mercato o messo in servizio. Questo registro centralizzato consente alle autorità di monitorare i sistemi AI ad alto rischio presenti sul mercato europeo.

j) Misure Correttive e Informazioni (Articolo 20)

Adozione di misure correttive tempestive in caso di non conformità e fornitura di informazioni necessarie alle autorità e agli utenti.

1 **Identificazione della non conformità**

Rilevamento di problemi o deviazioni dai requisiti normativi

La tempestività nella gestione delle non conformità è essenziale per minimizzare i rischi e mantenere la fiducia degli utenti e delle autorità di vigilanza.

2 **Valutazione dell'impatto**

Analisi delle potenziali conseguenze della non conformità

I fornitori devono mantenere un sistema di monitoraggio post-commercializzazione per identificare rapidamente eventuali problemi e adottare le misure correttive necessarie. La comunicazione trasparente con le autorità competenti e gli utenti è un elemento fondamentale di questo processo.

3 **Definizione delle misure correttive**

Pianificazione delle azioni necessarie per risolvere il problema

4 **Implementazione delle correzioni**

Attuazione delle misure identificate

5 **Comunicazione alle parti interessate**

Informazione tempestiva alle autorità e agli utenti coinvolti

k) Dimostrazione di Conformità

Su richiesta delle autorità nazionali competenti, dimostrazione della conformità attraverso documentazione e prove tecniche appropriate.



Documentazione completa

Preparazione e mantenimento di un set completo di documenti che dimostrano la conformità a tutti i requisiti dell'AI Act



Risultati dei test

Conservazione dei risultati di tutti i test e delle valutazioni effettuate sul sistema AI per dimostrare le sue prestazioni e la sua conformità



Cooperazione con le autorità

Disponibilità a collaborare pienamente con le autorità di vigilanza durante le ispezioni e le verifiche di conformità

I fornitori devono essere in grado di dimostrare la conformità dei loro sistemi AI ad alto rischio in qualsiasi momento durante il ciclo di vita del prodotto. Questo include la capacità di fornire spiegazioni dettagliate sul funzionamento del sistema e sulle misure adottate per garantire la conformità ai requisiti normativi.

I) Requisiti di Accessibilità

Conformità ai requisiti di accessibilità previsti dalle Direttive (UE) 2016/2102 (accessibilità siti web) e (UE) 2019/882 (Atto Europeo sull'Accessibilità).

Direttiva (UE) 2016/2102

- Accessibilità dei siti web e delle applicazioni mobili
- Conformità agli standard WCAG
- Dichiarazione di accessibilità
- Meccanismo di feedback per gli utenti

Direttiva (UE) 2019/882

- Accessibilità dei prodotti e servizi
- Requisiti funzionali di accessibilità
- Informazioni sull'accessibilità
- Servizi di supporto accessibili



I sistemi di IA ad alto rischio devono essere progettati tenendo conto delle esigenze delle persone con disabilità, garantendo che possano essere utilizzati da tutti gli utenti in condizioni di parità. Questo include l'implementazione di funzionalità come:

- Interfacce utente accessibili
- Compatibilità con tecnologie assistive
- Alternative testuali per contenuti non testuali
- Opzioni di personalizzazione per diverse esigenze



OBBLIGHI DEL DEPLOYER DI SISTEMI DI IA AD ALTO RISCHIO



Articolo 26 – "Obblighi dei deployer dei sistemi di AI ad alto rischio"

(Regolamento UE 2024/1624, Capo III, Sezione 2)

L'articolo 26 del Regolamento UE 2024/1624 stabilisce gli obblighi specifici per i soggetti che implementano e utilizzano sistemi di Intelligenza Artificiale classificati come ad alto rischio.

Conformità all'uso previsto (par. 1)

"I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso..."

Significato:

Il deployer (cioè il soggetto che utilizza il sistema AI, ad esempio un'azienda o una PA) è obbligato ad attenersi strettamente alle istruzioni d'uso fornite dal provider (art. 19 AI Act).



Implicazione:

- L'uso difforme può comportare responsabilità contrattuale, civile, regolamentare.
- Serve una procedura interna per assicurare che l'uso sia aderente alle specifiche del fornitore.

Supervisione umana qualificata (par. 2)

"I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie..."

Significato:

Chi controlla il sistema deve essere una persona formata, autorizzata e supportata, non un soggetto passivo.



Implicazione:

- Le imprese devono formare adeguatamente il personale deputato al controllo umano.
- Non basta la mera presenza umana: serve controllo significativo (rif. art. 20 AI Act).



Rinvio a obblighi UE e nazionali (par. 3)

"Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale..."

Significato:

Il rispetto dell'AI Act non esonera da obblighi paralleli, ad esempio:

 GDPR

 L. 231/2001

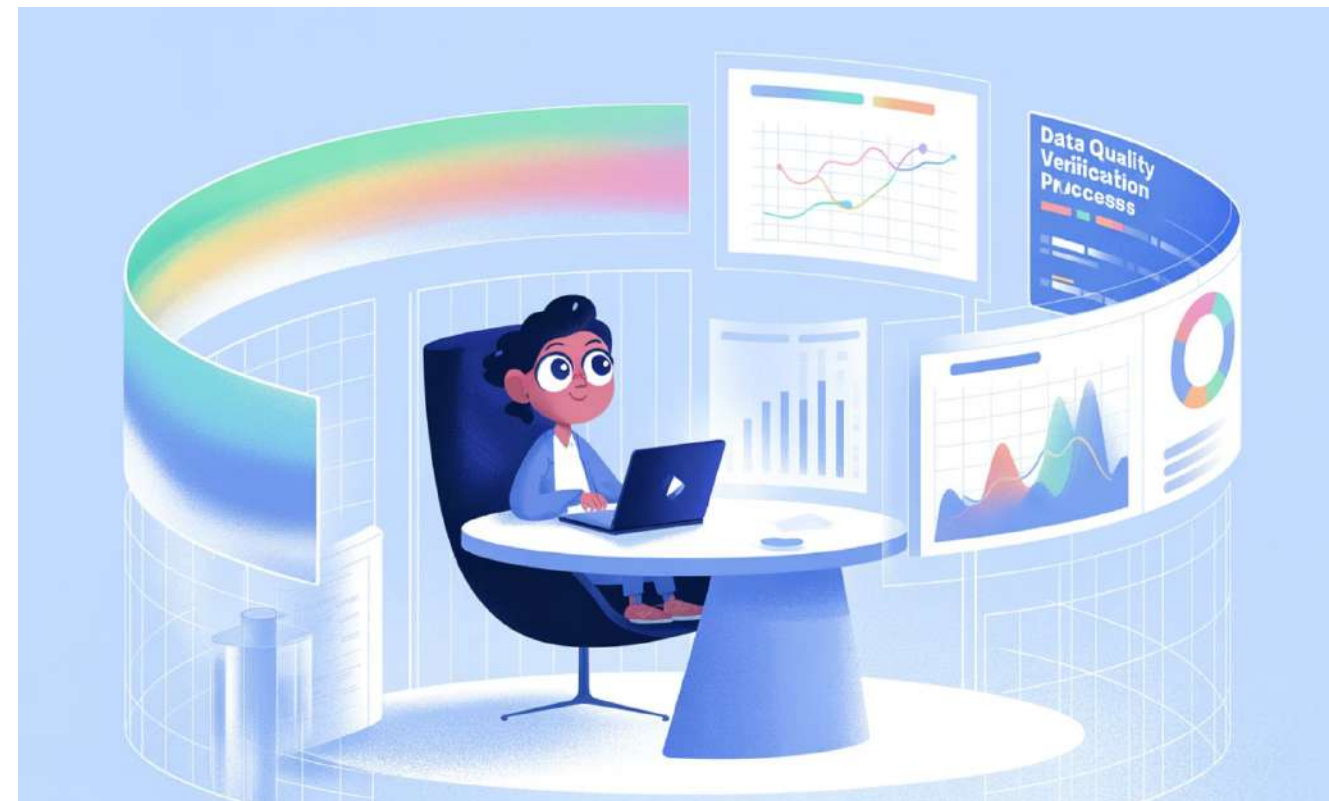
 Normative settoriali (sanità, finanza, PA)

Qualità dei dati di input (par. 4)

"Il deployer garantisce che i dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista..."

Significato:

Il deployer, quando ha controllo sui dati in ingresso, è responsabile della qualità, rilevanza e adeguatezza dei dati usati.



Esempio:

Un tribunale che alimenta un sistema di analisi con dati di sentenze deve assicurarsi che questi siano bilanciati, attuali e completi.

Monitoraggio e obbligo di sospensione (par. 5)

Il deployer monitora il funzionamento del sistema

Informa il fornitore in caso di anomalie (art. 72)

Sospende l'uso in caso di rischi gravi (art. 79)

Notifica incidenti gravi alle autorità

Clausola bancaria:

Se il deployer è un istituto finanziario soggetto a normativa UE settoriale, l'obbligo si considera soddisfatto se rispetta le regole interne previste dal diritto finanziario (es. MiFID II, CRD V).

Nota tecnica:

Le notifiche devono rispettare le forme e tempistiche previste anche dal GDPR e dalla Direttiva NIS2, se applicabili.

Conservazione dei log (par. 6)

"I deployer conservano i log generati automaticamente... per almeno sei mesi..."

Significato:

Chi utilizza il sistema deve conservare le registrazioni automatiche degli eventi (log), se sono sotto il suo controllo.



Eccezione bancaria:

Per gli operatori finanziari, l'obbligo si integra con la documentazione conservativa già richiesta dal diritto UE finanziario.



AI Integration: a transparent path forward

Obbligo informativo verso i lavoratori (par. 7)

"I deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati..."



Informazione preventiva

Prima dell'uso sul luogo di lavoro, va data informazione preventiva ai lavoratori



Chiarezza

L'informazione deve essere chiara e comprensibile



Conformità normativa

Secondo le norme nazionali e dell'UE (es. D.lgs. 152/1997 in Italia)



Significato:

Prima dell'uso sul luogo di lavoro, va data informazione preventiva e chiara ai lavoratori, secondo le norme nazionali e dell'UE (es. D.lgs. 152/1997 in Italia).

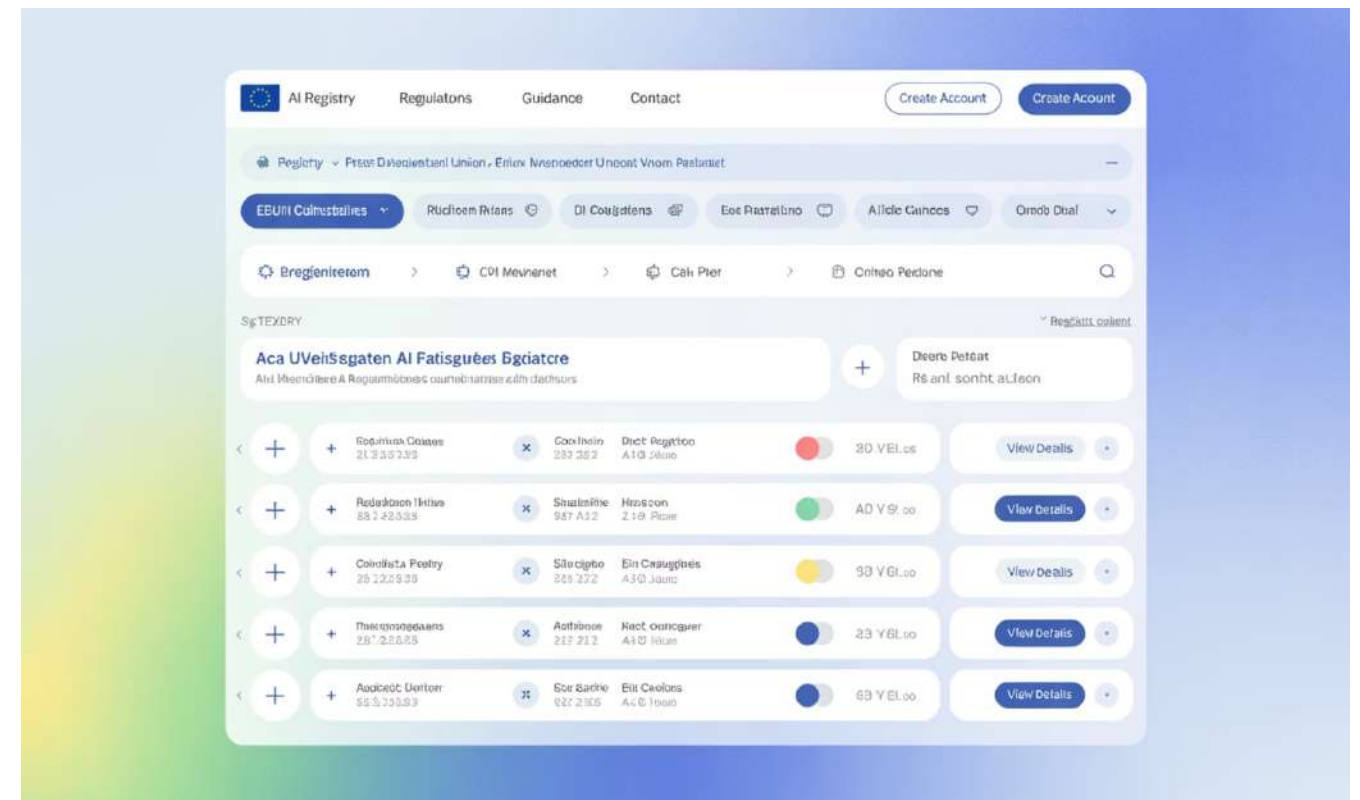
Obbligo di registrazione nella banca dati UE (par. 8)

"I deployer pubblici... rispettano gli obblighi di registrazione di cui all'articolo 49..."

Significato:

Le PA o istituzioni UE devono assicurarsi che i sistemi siano registrati nel database europeo dei sistemi AI ad alto rischio (art. 71).

In mancanza: non possono utilizzarli e devono avvisare il provider.





Valutazione d'impatto privacy (par. 9)

"I deployer usano le informazioni dell'art. 13 per adempiere all'art. 35 GDPR o 27 della Direttiva (UE) 2016/680..."



 Significato:

Il deployer, quando tratta dati personali, deve valutare gli impatti privacy mediante DPIA, utilizzando le informazioni fornite dal provider.

Uso dei sistemi biometrici da parte delle forze di polizia (par. 10)

Complesso sistema autorizzativo per l'uso a posteriori dell'identificazione biometrica remota.

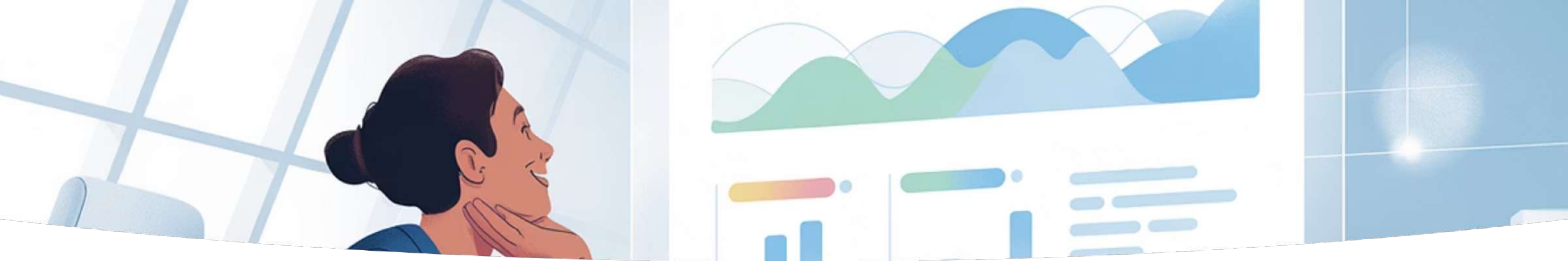
- 1** Richiesta di autorizzazione giudiziaria o amministrativa (entro 48 ore)
- 2** Cancellazione dati se autorizzazione negata
- 3** Obbligo di tracciabilità, relazioni annuali, e limiti di utilizzo strettamente connessi a reati

Principio cardine:

L'uso indiscriminato (non mirato) è vietato. Ogni uso va documentato e notificato.

Deroghe e divieti:

- Divieto di decisioni automatizzate negative basate solo sull'output.
- Obbligo di documentazione e cooperazione con DPA e autorità di vigilanza del mercato.



Obbligo informativo verso le persone fisiche (par. 11)

Obbligo di trasparenza

I deployer devono informare le persone fisiche soggette all'uso del sistema, in modo trasparente

Obbligo di cooperazione (par. 12)

"I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione."

Significato:

Responsabilità attiva e continua nella cooperazione con autorità, anche nel caso di audit, ispezioni, segnalazioni o richieste di informazioni.



Conclusioni operative

- ✓ I deployer non sono semplici utilizzatori, ma soggetti attivi e responsabili nella governance dei sistemi di IA ad alto rischio.
- ✓ Devono documentare, monitorare, informare e cooperare.
- ✓ Per settori regolamentati (finanza, PA, forze dell'ordine), si applicano norme speciali e integrative.



**Valutazione d'impatto sui diritti
fondamentali per i sistemi di IA ad
alto rischio (Art. 27)**



Punti chiave

- ✓ L'art. 27 rappresenta un obbligo giuridico sostanziale, non solo formale.
- ✓ La FRIA non è un adempimento documentale, ma uno strumento di garanzia effettiva dei diritti fondamentali.
- ✓ Va integrata nel sistema di governance del rischio IA, unitamente a:



DPIA (GDPR)

Valutazione d'impatto sulla protezione dei dati personali



Audit di equità algoritmica

Verifica dell'imparzialità e non discriminazione



Accountability

Responsabilità e trasparenza decisionale



Monitoraggio post-commercializzazione

Controllo continuo ex art. 28

1. Contesto normativo: quando si applica l'obbligo?

Soggetti obbligati (Art. 27, par. 1):

L'obbligo di valutazione di impatto ex art. 27 AI Act ricade sui deployer che:

- sono organismi di diritto pubblico (es. PA, enti regolatori, ASL),
- sono privati che forniscono servizi pubblici (es. società che gestiscono trasporto, sanità, energia),
- utilizzano sistemi di cui all'Allegato III, punto 5, lettere b) e c), ovvero:

 **Sistemi per valutare ammissibilità a benefici sociali**  **Sistemi di scoring creditizio o finanziario**

Esclusione: Sono esclusi i sistemi di cui all'Allegato III, punto 2 (cioè quelli usati nel contesto lavorativo o di gestione delle risorse umane), per i quali l'art. 26, §7 già impone un obbligo informativo.

Contenuto minimo della valutazione (Art. 27, Par. 1)

La FRIA deve includere i seguenti 6 elementi obbligatori:

Descrizione del processo



Durata e frequenza

Misure correttive



Categorie di soggetti

Supervisione umana



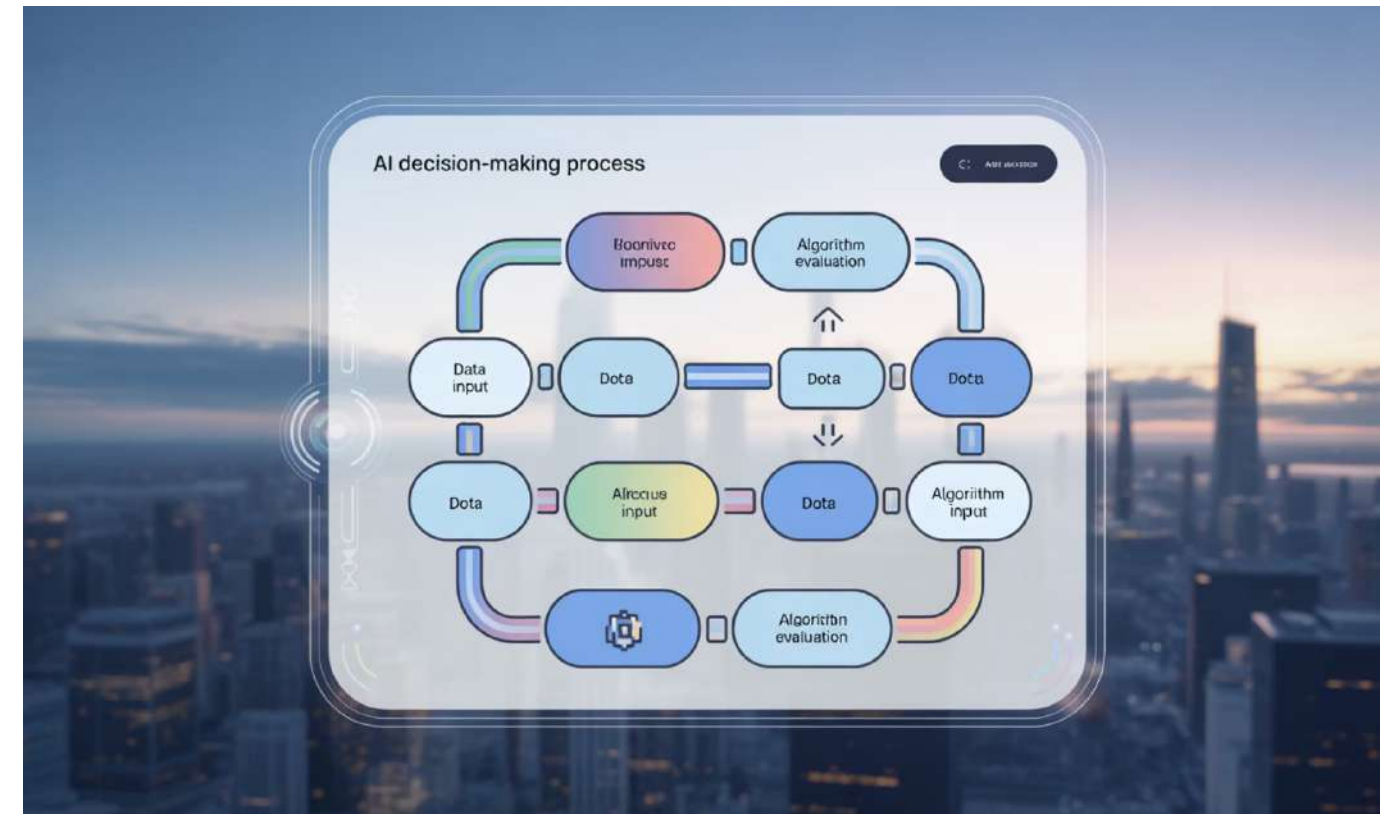
Rischi specifici

a) Descrizione del processo coinvolto

"...in cui il sistema sarà utilizzato, in linea con la sua finalità prevista"

📌 Obbligo di contestualizzazione concreta:

- Qual è il processo decisionale automatizzato?
- In quale fase interviene il sistema IA?



Identificazione del processo

Mappatura dettagliata del flusso decisionale in cui si inserisce il sistema IA

Finalità prevista

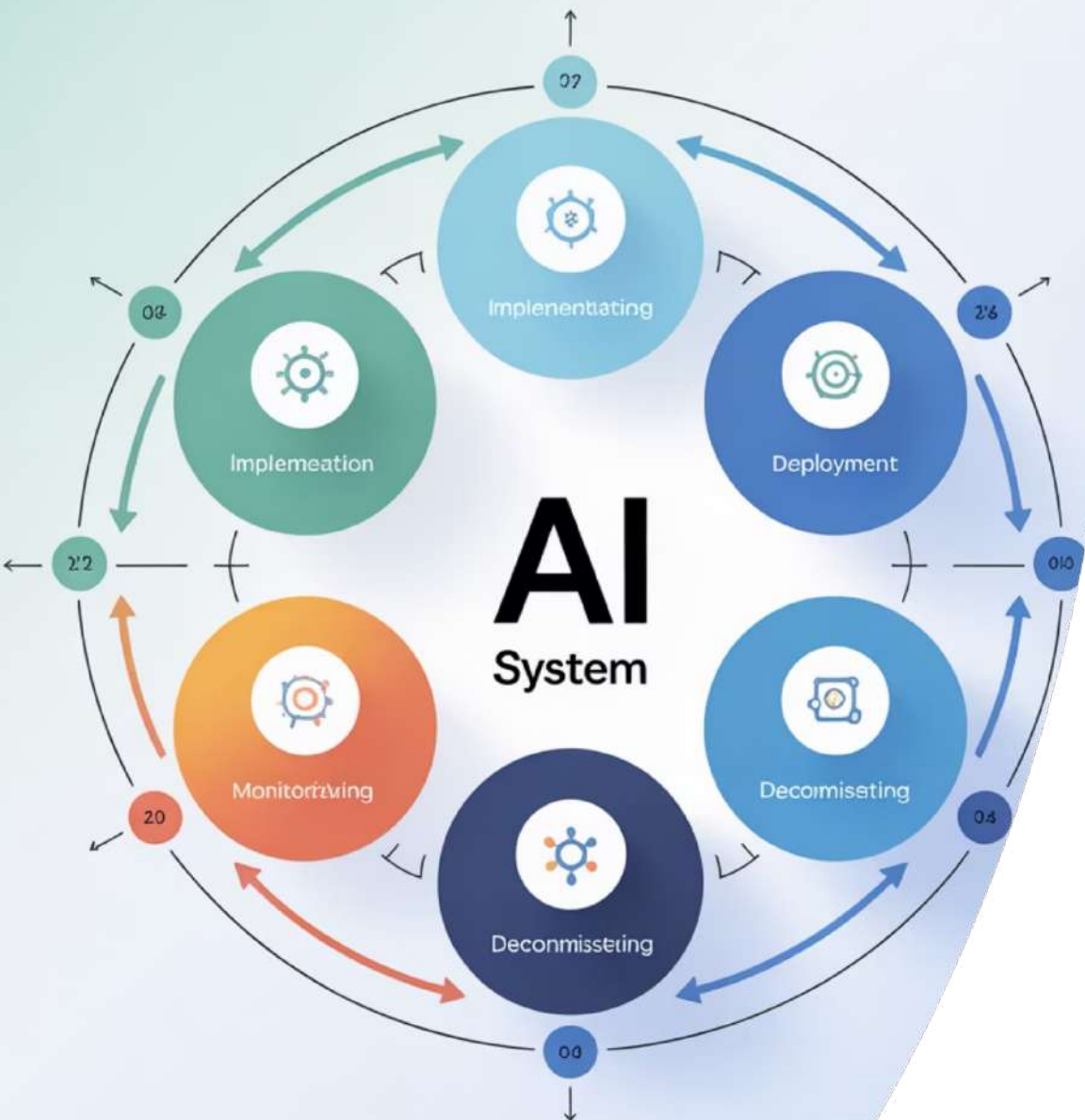
Descrizione degli obiettivi specifici per cui il sistema viene implementato

Contestualizzazione

Analisi del contesto operativo e delle interazioni con altri processi

AI System Lifecycle

From concept to retirement



b) Durata e frequenza d'uso

"...del periodo di tempo entro il quale il sistema è destinato a essere utilizzato"

1

Durata prevista

Specificare l'intero arco temporale di utilizzo previsto (es. fase di test di 6 mesi, implementazione operativa di 2 anni, eventuale fase di dismissione)

2

Frequenza d'uso

Dettagliare quando e quanto spesso il sistema verrà utilizzato: continuativo (24/7), quotidiano con picchi specifici, settimanale per determinate operazioni, mensile per analisi periodiche

3

Ciclo di vita

Descrivere le fasi distinte del ciclo di vita: implementazione iniziale, periodo di rodaggio, piena operatività, manutenzione programmata, aggiornamenti periodici e processo di revisione

📌 **Importanza della precisione temporale:** È essenziale fornire una stima accurata sia della durata complessiva dell'utilizzo del sistema che della frequenza con cui verrà impiegato nei processi decisionali, poiché questi fattori influenzano direttamente l'entità e la persistenza dell'impatto sui diritti fondamentali dei soggetti coinvolti.

c) Categorie di soggetti interessati

"...persone fisiche e gruppi verosimilmente interessati"

📌 Obbligo di identificare:

- Chi è oggetto dell'output del sistema? (Es. beneficiari, clienti, cittadini...)
- Eventuali categorie vulnerabili (es. minori, stranieri, persone fragili...)



Destinatari diretti

Persone direttamente sottoposte alle decisioni del sistema IA (beneficiari, richiedenti, utenti)



Categorie vulnerabili

Soggetti che potrebbero subire impatti sproporzionati (minori, anziani, persone con disabilità)



Gruppi sociali

Comunità o gruppi demografici potenzialmente interessati dalle decisioni algoritmiche



d) Rischi specifici di danno

"...tenendo conto delle informazioni trasmesse dal fornitore (art. 13)"

- **Discriminazione algoritmica?**
Valutare se il sistema possa produrre risultati discriminatori basati su caratteristiche protette come genere, etnia, età o disabilità
- **Effetti su accesso a servizi essenziali?**
Analizzare potenziali barriere all'accesso a servizi fondamentali create dal sistema IA
- **Profilazione indebita?**
Identificare rischi di categorizzazione eccessiva o inappropriata degli individui
- **Mancanza di trasparenza nella decisione?**
Valutare la comprensibilità e spiegabilità delle decisioni algoritmiche per i soggetti interessati

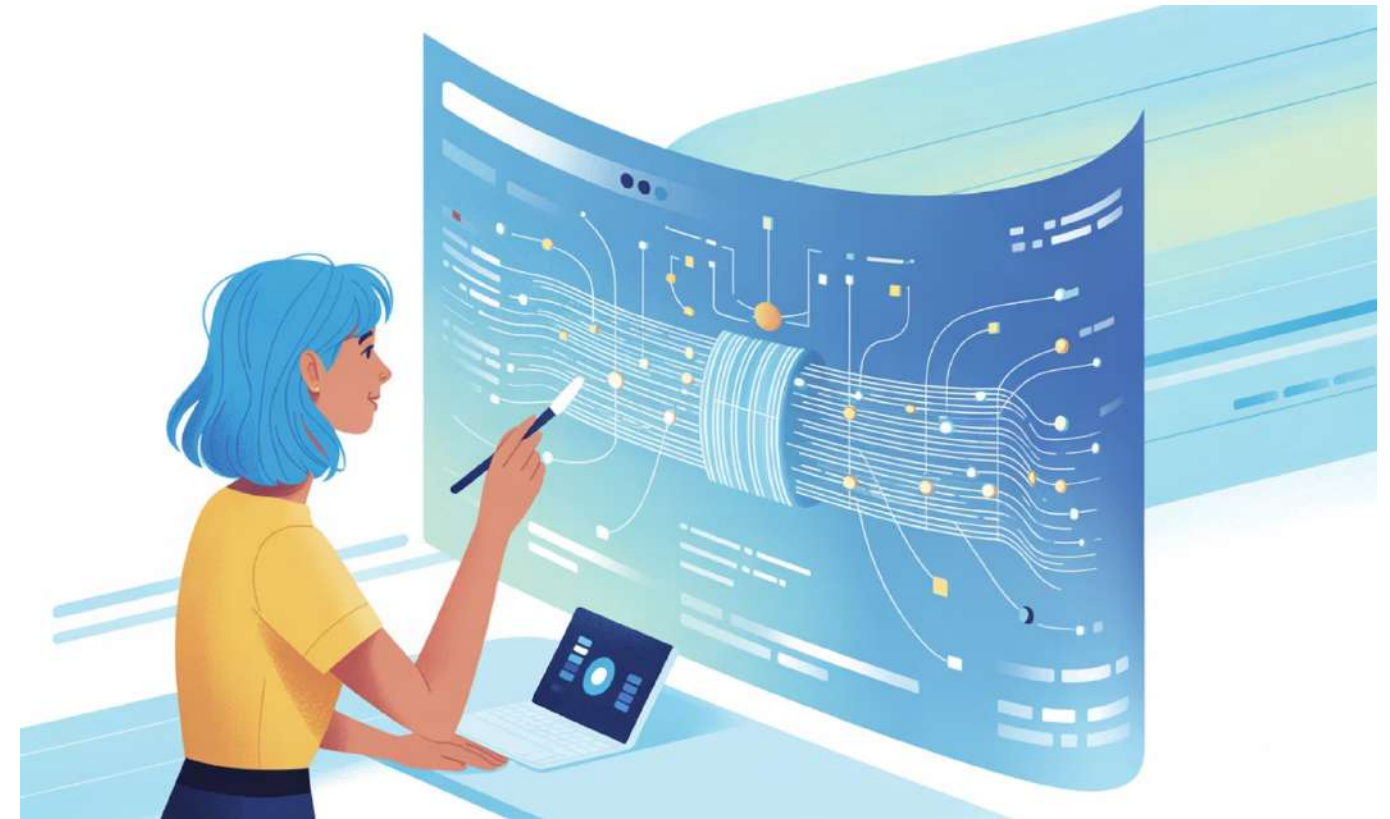
📌 Obbligo di analisi dei rischi per i diritti fondamentali richiede una valutazione approfondita di tutti i potenziali impatti negativi.

e) Misure di supervisione umana

"...secondo le istruzioni per l'uso"

📌 Valutazione delle contromisure:

- La sorveglianza umana è effettiva?
- I controlli sono ex ante, in itinere o ex post?
- È previsto intervento umano nei casi critici?



Monitoraggio continuo

Supervisione costante del funzionamento del sistema



Verifica dei risultati

Controllo umano sugli output prima dell'applicazione



Intervento correttivo

Capacità di modificare o annullare decisioni algoritmiche

f) Misure correttive in caso di danno

"...comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo"



Canali di segnalazione

- Whistleblowing
- Reclami formali
- Portali dedicati



Procedure correttive

- Sospensione del sistema
- Escalation gerarchica
- Revisione manuale



Misure di accountability

- Registrazione delle decisioni
- Audit periodici
- Reportistica trasparente

📌 Obbligo di prevedere meccanismi efficaci per gestire eventuali danni causati dal sistema e garantire responsabilità.

Tempistiche e aggiornamenti (Art. 27 paragrafo 2)

Prima valutazione

La valutazione deve essere effettuata prima del primo utilizzo del sistema.

Riutilizzo e aggiornamento

È possibile riutilizzare una FRIA esistente in casi analoghi, ma:

- va verificata l'attualità e coerenza delle condizioni,
- in caso di cambiamento (es. modifica sistema, processo, dati o utenti), il deployer deve aggiornare la valutazione.



Obbligo di notifica (Art. 27, Par. 3)

Dopo aver completato la FRIA, il deployer deve notificare i risultati all'autorità di vigilanza del mercato, tramite un modello predisposto dall'AI Office .

Esenzione: solo nei casi previsti dall'art. 46, paragrafo 1 (es. in caso di sistemi in fase sperimentale regolata – "AI sandbox").



Completamento FRIA

Finalizzazione della valutazione d'impatto sui diritti fondamentali

Compilazione modello

Utilizzo del formato standardizzato fornito dall'AI Office

Notifica all'autorità

Invio formale all'autorità di vigilanza del mercato

Coordinamento con la DPIA del GDPR (Art. 27, Par. 4)

📌 Se il deployer ha già effettuato una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi di:

● **Art. 35 GDPR (Reg. 2016/679) o**

● **Art. 27 Direttiva 2016/680 (per le autorità di contrasto)**

→ La valutazione ex art. 27 AI Act integra e non sostituisce la DPIA.

📌 Esempio operativo: Un Comune che usa un sistema AI per valutare l'idoneità ai contributi per l'affitto:

DPIA (GDPR)

Redige la DPIA per il trattamento dei dati (es. reddituali, familiari)

FRIA (AI Act)

Effettua la FRIA per analizzare il rischio di esclusione ingiustificata, bias sociale, trasparenza algoritmica.

Modello standardizzato (Art. 27, Par. 5)

"L'Ufficio per l'IA elabora un modello di questionario, anche attraverso uno strumento automatizzato..."

Strumento semplificato

📌 L'AI Office metterà a disposizione uno strumento semplificato per la compilazione, ispirato al principio di "compliance by design".

Standard di riferimento

📌 Il modulo (obbligatorio per la notifica) diventerà standard di riferimento per la documentazione di impatto.

Questionario strutturato

Format predefinito con campi obbligatori

Compilazione guidata

Interfaccia user-friendly con istruzioni

Generazione automatica

Produzione del documento finale standardizzato



Gli organi di governance AI nell'UE

Struttura di governance europea dell'IA

È importante esaminare la struttura di governance europea dell'IA, per comprendere i ruoli degli organi amministrativi che avranno compiti di supervisione e altri ruoli, tra cui l'adozione delle oltre 80 misure di follow-up previste nei prossimi anni (ad esempio atti di esecuzione, atti delegati, linee guida) e le opportunità che la struttura di governance offrirà alle aziende.

L'AI ACT nel Capitolo VII definisce la Governance per l'AI. Si suddivide in due sezioni: nella prima si descrive l'organizzazione a livello comunitario, nella seconda a livello dei singoli stati membri.





Ufficio per l'IA (AI Office) Art. 64



Ruolo e natura

L'Ufficio per l'IA è l'organismo interno alla Commissione europea incaricato di:

- sviluppare le competenze e le capacità dell'Unione nel settore dell'intelligenza artificiale;
- supportare attivamente l'implementazione del Regolamento AI, con funzione tecnica, amministrativa e di coordinamento.

L'Ufficio per l'IA non è un'autorità indipendente, ma un'articolazione della Commissione con funzioni centrali nella governance e nella supervisione dei sistemi di IA ad alto rischio e GPAI.



Cooperazione con gli Stati membri

Gli Stati membri devono agevolare l'attività dell'Ufficio, fornendo supporto funzionale e operativo per l'attuazione del Regolamento.

Consiglio per l'IA (Art. 65)

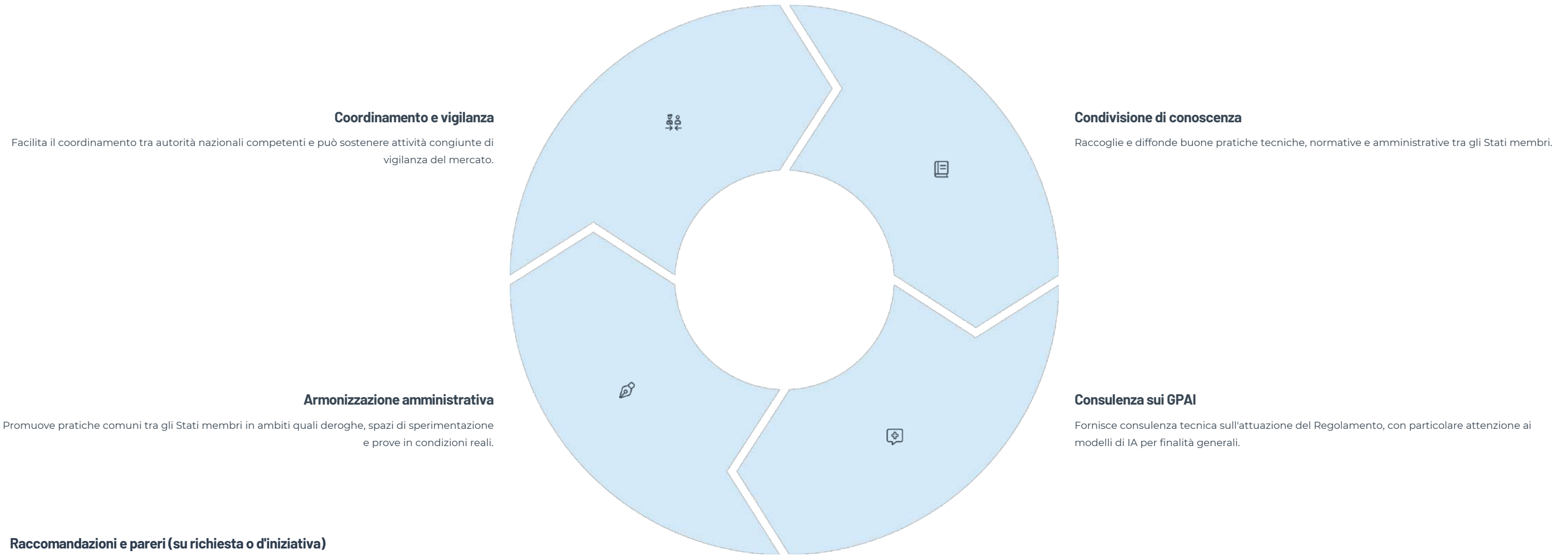


Compiti del Consiglio per l'IA (Art. 66)

Il Consiglio per l'IA europeo (European AI Board) rappresenta il fulcro della governance collaborativa e multilivello dell'AI Act. È un organo di supporto e coordinamento che svolge funzioni consultive, propositive e operative, al fine di garantire un'attuazione uniforme, efficace e coerente del Regolamento in tutta l'Unione europea.

 Missione principale

Fornire consulenza e assistenza tecnica alla Commissione e agli Stati membri, in un'ottica di armonizzazione normativa e cooperazione amministrativa tra le autorità nazionali.



Raccomandazioni e pareri (su richiesta o d'iniziativa)

Il Consiglio può formulare raccomandazioni e pareri scritti, su:

- Codici di condotta, codici di buone pratiche e orientamenti della Commissione;
- Valutazione e revisione del Regolamento, incidenti gravi, funzionamento della banca dati UE, atti delegati e di esecuzione, allineamento con la normativa di armonizzazione;
- Specifiche tecniche e norme per sistemi IA ad alto rischio;
- Norme armonizzate e specifiche comuni;
- Trend emergenti: competitività UE, adozione dell'IA, competenze digitali, evoluzione delle catene del valore, implicazioni giuridiche e di responsabilità;
- Eventuali modifiche dell'Allegato III e revisione dell'art. 5 (divieti), sulla base di evidenze e sviluppi tecnologici.

Forum consultivo (Art. 67)



Funzione e ruolo

Il Forum consultivo è un organismo istituito per fornire consulenza tecnica e competenze specialistiche al Consiglio per l'IA e alla Commissione europea, contribuendo concretamente all'attuazione e allo sviluppo delle attività previste dal Regolamento.

Nomina e durata

- I membri sono nominati dalla Commissione europea, sulla base delle competenze riconosciute nel settore IA.
- Durata iniziale: 2 anni
- Possibile proroga: fino a un massimo complessivo di 4 anni

Membri permanenti

Sono membri permanenti di diritto:

- FRA (Agenzia per i Diritti Fondamentali)
- ENISA (Agenzia dell'Unione europea per la cybersicurezza)
- CEN, CENELEC (Comitati europei di normazione)
- ETSI (Istituto europeo per le norme di telecomunicazione)



Composizione pluralistica

La sua composizione è rappresentativa e bilanciata, includendo attori industriali, start-up e PMI, società civile, mondo accademico. Si garantisce equilibrio tra interessi commerciali e non commerciali e proporzionalità tra PMI e grandi imprese.

Regole di funzionamento

- Il Forum adotta un regolamento interno.
- Elegge due copresidenti, con mandato di 2 anni, rinnovabile una sola volta.
- Si riunisce almeno due volte all'anno.
- Può invitare esperti esterni e stakeholder alle proprie riunioni.

Attività e output

Su richiesta del Consiglio per l'IA o della Commissione, il Forum può:

- elaborare pareri tecnici,
- fornire raccomandazioni,
- trasmettere contributi scritti.

Il Forum può istituire sottogruppi, permanenti o temporanei, su temi specifici e redige una relazione pubblica annuale sulle proprie attività.

Gruppo di esperti scientifici indipendenti (Art. 68)

 Finalità

L'articolo 68 disciplina l'istituzione e il funzionamento del gruppo di esperti scientifici indipendenti, organo consultivo altamente specializzato che supporta l'attuazione tecnica e scientifica del Regolamento, in particolare in relazione ai modelli di IA per finalità generali (GPAI) e ai rischi sistemici.



Istituzione formale

Il gruppo è istituito tramite atto di esecuzione della Commissione europea, adottato secondo la procedura d'esame. Opera in supporto all'esecuzione del Regolamento, soprattutto nell'ambito tecnico-scientifico.

Composizione e requisiti

Gli esperti sono selezionati dalla Commissione, in consultazione con il Consiglio per l'IA, sulla base di competenze scientifiche e tecniche aggiornate, assenza di conflitti d'interesse e capacità di operare con diligenza, obiettività e accuratezza.

Compiti principali

Il gruppo fornisce consulenza specialistica all'Ufficio per l'IA su modelli GPAI, rischi sistemici, strumenti di valutazione tecnica e supporto alle autorità nazionali.

Compiti relativi ai GPAI

- Segnalazione dei rischi sistemici a livello UE (art. 90)
- Sviluppo di strumenti e benchmark per la valutazione tecnica dei GPAI
- Classificazione dei GPAI, in particolare quelli a rischio sistemico
- Consulenza tecnica su classificazioni e sviluppo di strumenti tecnici

Supporto alle autorità

- Assistenza su richiesta alle autorità di vigilanza del mercato
- Supporto alle attività transfrontaliere di vigilanza (art. 74, par. 11)
- Supporto alla Commissione nella procedura di salvaguardia dell'Unione (art. 81)

Obblighi di indipendenza e trasparenza

Gli esperti devono:

- operare con imparzialità e in modo obiettivo;
- rispettare la riservatezza dei dati e delle informazioni trattate;
- non ricevere istruzioni esterne;
- compilare e rendere pubblica una dichiarazione di interessi.

L'Ufficio per l'IA predispone procedure per prevenire e gestire conflitti di interesse, anche in modo proattivo.

Disposizioni attuative

L'atto esecutivo di istituzione del gruppo definisce:

- modalità e condizioni operative;
- procedure per segnalazioni e richieste di supporto da parte del gruppo all'Ufficio per l'IA;
- modalità di interazione tra gli esperti e gli organi competenti.

Osservazioni giuridiche conclusive

Il gruppo di esperti rappresenta un presidio tecnico-indipendente, essenziale per:

- prevenire e mitigare i rischi sistemici legati ai GPAI;
- fornire valutazioni tecniche autorevoli, utili per decisioni regolatorie e politiche;
- garantire un approccio evidence-based nell'attuazione del Regolamento.

La sua esistenza rafforza la stratificazione tecnico-istituzionale della governance dell'AI Act, a tutela dell'interesse pubblico europeo.

Designazione delle autorità nazionali competenti (Art. 70)

	Designazione delle autorità Ogni Stato membro deve designare almeno un'autorità di notifica e un'autorità di vigilanza del mercato per garantire l'applicazione del Regolamento.
	Comunicazioni alla Commissione Entro il 2 agosto 2025, gli Stati membri devono comunicare alla Commissione l'identità delle autorità designate e designare un punto di contatto unico nazionale.
	Requisiti di risorse Le autorità competenti devono disporre di risorse tecniche, finanziarie e umane adeguate e personale qualificato con conoscenze specifiche.

Principi di funzionamento

- Le autorità devono agire in modo indipendente, imparziale e obiettivo, evitando conflitti d'interesse.
- Gli Stati sono liberi di distribuire i compiti su una o più autorità, secondo le proprie esigenze organizzative.
- Le autorità devono adottare misure di sicurezza informatica adeguate per proteggere l'integrità dei loro processi e sistemi.
- Nell'esercizio delle loro funzioni, le autorità devono rispettare obblighi di riservatezza come previsto dall'art. 78.

Competenze richieste

- Il personale delle autorità deve avere conoscenze specifiche in:
- Tecnologie e modelli IA
 - Protezione dei dati personali
 - Cybersicurezza
 - Diritti fondamentali
 - Normative UE rilevanti
- Gli Stati devono valutare annualmente l'adeguatezza delle risorse e aggiornare le esigenze di competenza se necessario.

Reporting e coordinamento

- Entro il 2 agosto 2025, e successivamente ogni due anni, gli Stati membri devono riferire alla Commissione sull'adeguatezza delle risorse delle autorità nazionali.
- La Commissione inoltra tali dati al Consiglio per l'IA, che potrà formulare raccomandazioni.
- La Commissione svolge un ruolo attivo nel favorire lo scambio di buone pratiche ed esperienze tra le autorità nazionali.

Orientamenti alle imprese

Le autorità possono:

- Fornire orientamenti e consulenza pratica sull'attuazione dell'AI Act, soprattutto a PMI e start-up, in coerenza con le indicazioni del Consiglio per l'IA e della Commissione.
- In caso di sovrapposizione con altri settori normati a livello UE, devono consultare le autorità competenti in base a quelle normative.

Sorveglianza sulle istituzioni UE

Per quanto riguarda istituzioni, organi e organismi dell'Unione Europea, il Garante Europeo della Protezione dei Dati (EDPS) è l'autorità competente per la vigilanza.

L'articolo 70 è centrale nella governance multilivello dell'AI Act, poiché incardina le responsabilità amministrative e regolatorie a livello nazionale, prevede un sistema integrato di coordinamento tra Stati e Commissione, impone standard qualitativi elevati alle autorità e è funzionale alla legittimità e all'efficacia esecutiva del Regolamento.

Banca dati dell'UE per i sistemi di IA ad alto rischio (Art. 71)



Istituzione e gestione

La Commissione Europea, in collaborazione con gli Stati membri, deve istituire e mantenere una banca dati unica a livello UE per i sistemi di IA ad alto rischio elencati nell'Allegato III.



Inserimento dei dati

I dati da inserire sono specificati nell'Allegato VIII, sezioni A e B, e sono forniti dal fornitore o, quando previsto, dal suo rappresentante autorizzato.



Inserimento da parte del deployer pubblico

I dati della sezione C dell'Allegato VIII sono inseriti nella banca dati dall'ente pubblico deployer o da chi agisce per loro conto, in conformità all'articolo 49.

Accessibilità delle informazioni

Salvo alcune eccezioni (art. 49, par. 4 e art. 60, par. 4 lett. c), le informazioni registrate ai sensi dell'articolo 49 sono pubblicamente accessibili in formato facilmente consultabile e leggibile meccanicamente.

Le informazioni registrate ai sensi dell'articolo 60 sono invece accessibili solo alle autorità di vigilanza del mercato e alla Commissione, a meno che il fornitore o potenziale fornitore non acconsenta alla loro pubblicazione.

Trattamento dei dati personali

La banca dati contiene dati personali solo nella misura strettamente necessaria, limitati a:

- Nomi e dati di contatto delle persone fisiche responsabili della registrazione;
- Persone con autorità legale per rappresentare il fornitore o il deployer.

Riflessioni sulla banca dati UE



Strumento centrale di trasparenza

L'articolo 71 crea uno strumento centrale di trasparenza e controllo sui sistemi IA ad alto rischio nell'UE, favorendo il monitoraggio e la supervisione coordinata tra Stati membri e Commissione.



Responsabilizzazione diretta

Il coinvolgimento di fornitori e deployer nella registrazione assicura una responsabilizzazione diretta, mentre il controllo sulla struttura e specifiche tecniche da parte della Commissione e del Consiglio per l'IA ne garantisce l'adequazione tecnologica e normativa.



Bilanciamento tra trasparenza e riservatezza

La differenziazione tra dati pubblicamente accessibili e dati riservati alle autorità garantisce un bilanciamento tra trasparenza, protezione della proprietà intellettuale e riservatezza.



Protezione dei dati personali

Il trattamento limitato dei dati personali risponde ai principi di minimizzazione e protezione dei dati personali previsti dal GDPR.



Disegno di Legge 1146/24 sull'Intelligenza Artificiale

Il Disegno di Legge n. 1146/24 recante “**Disposizioni e delega al Governo in materia di intelligenza artificiale**” rappresenta il primo tentativo organico dell'Italia di dotarsi di una normativa nazionale sull'intelligenza artificiale. Il DDL mira a rafforzare la competitività e garantire un utilizzo affidabile dell'IA, ponendo al centro la tutela dei diritti fondamentali dei cittadini.

Attualmente il disegno di legge è in discussione alla Camera dei Deputati, dove ha assunto la numerazione A.C. 2316/25,

Iter Parlamentare e Stato di Approvazione

1

20 maggio 2024

Presentazione del DDL n. 1146/24 come iniziativa governativa per regolamentare l'intelligenza artificiale in Italia.

2

20 marzo 2025

Approvazione del disegno di legge da parte del Senato della Repubblica, completando la prima fase dell'iter legislativo.

3

Post 20 marzo 2025

Passaggio alla Camera dei Deputati con numerazione A.C. 2316/25, dove il testo è attualmente in esame.

4

17 giugno 2025

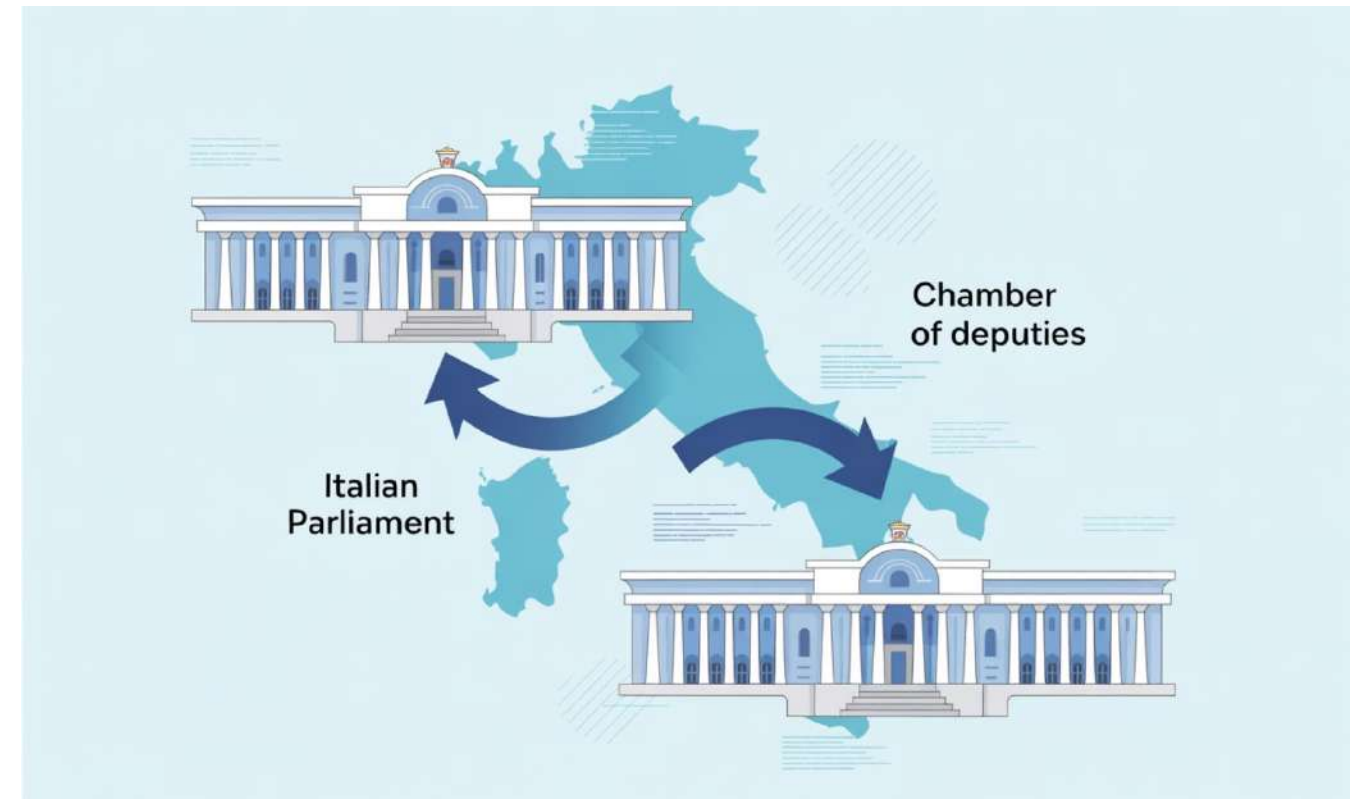
Approvazione del testo da parte delle commissioni IX e X della Camera, segnando un progresso significativo nell'iter.



Caratteristiche del Sistema Bicamerale

Il sistema bicamerale italiano richiede l'approvazione di un testo **identico da parte di entrambe le Camere**. Questo significa che le modifiche introdotte alla Camera dei Deputati richiederanno un ritorno del testo al Senato, attraverso il meccanismo noto come "**navetta parlamentare**".

Questo processo di andirivieni tra le due camere allungherà prolungare significativamente i tempi di approvazione definitiva della legge, specialmente considerando la complessità della materia trattata e le diverse sensibilità politiche coinvolte.





Deleghe al Governo



Delega Legislativa

Il DDL contiene significative deleghe al Governo per l'adozione di decreti legislativi che definiranno i dettagli normativi specifici.



Decreti Attuativi

La piena portata e l'impatto della legge si manifesteranno solo dopo l'emanazione di tali decreti, che dovranno essere adottati entro termini prestabiliti.

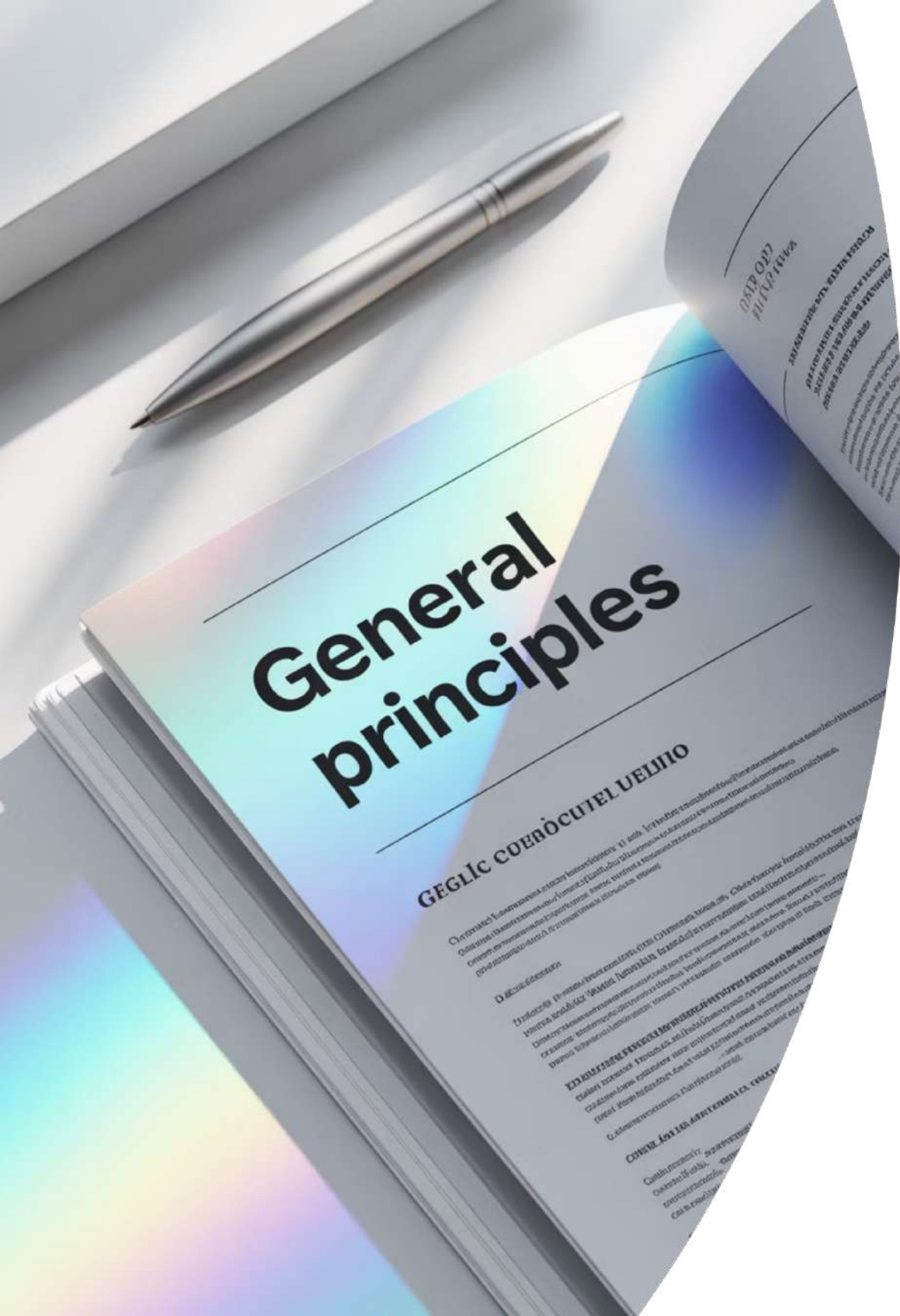


Flessibilità Normativa

Questa scelta conferisce agilità nella definizione di aspetti tecnici in un campo in rapida evoluzione come l'IA, permettendo adattamenti più rapidi.

**Il testo legislativo è composto da
26 articoli e si articola in 4 sezioni
fondamentali**





1. Principi generali (Art. 1-6)

Questo capitolo definisce il quadro generale e i principi fondamentali che guidano l'intero disegno di legge.

Principi Generali

Definizione del quadro generale e dei principi fondamentali che guidano l'intero disegno di legge.

Articoli 1-6

Stabiliscono finalità, definizioni, principi generali, informazione e riservatezza, sviluppo economico e sicurezza nazionale.

Base Normativa

Conformità al Regolamento (UE) 2024/1689 (AI Act) e alle normative italiane vigenti.

Articoli 1-2: Finalità e Definizioni

Art. 1 (Finalità e ambito di applicazione)

Stabilisce i principi per la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione di sistemi e modelli di intelligenza artificiale. Sottolinea la promozione di un utilizzo corretto, trasparente e responsabile dell'IA, in una dimensione **antropocentrica**, e garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali. Le disposizioni della legge si interpretano e si applicano conformemente al Regolamento (UE) 2024/1689 (AI Act).

Art. 2 (Definizioni)

Definisce i termini chiave come:

- **Sistema di intelligenza artificiale:** il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689.
- **Dato:** qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali elementi, anche sotto forma di registrazione sonora, visiva o audiovisiva.
- **Modelli di intelligenza artificiale:** i modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689.

Per quanto non espressamente previsto, si rimanda alle definizioni del regolamento (UE) 2024/1689

Articoli 3-6: Principi Fondamentali

Art. 3 (Principi generali)

Afferma che lo sviluppo e l'uso dell'IA devono rispettare i diritti e le libertà fondamentali, nonché principi quali trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità di genere e sostenibilità. Richiede la sorveglianza e l'intervento umano e sottolinea che l'uso dell'IA non deve minare la vita istituzionale democratica. Evidenzia anche l'importanza della cybersicurezza lungo l'intero ciclo di vita dei sistemi di IA.

Art. 5 (Principi in materia di sviluppo economico)

Lo Stato promuove l'IA per migliorare l'interazione uomo-macchina nei settori produttivi, aumentare la produttività e favorire nuove attività economiche, al fine di accrescere la competitività nazionale e la sovranità tecnologica. Incoraggia la creazione di un mercato dell'IA innovativo, equo e concorrenziale, facilita l'accesso a dati di alta qualità e privilegia soluzioni che garantiscano la localizzazione e il trattamento dei dati all'interno di data center nazionali per gli appalti pubblici elettronici. Favorisce la ricerca collaborativa tra imprese e organismi di ricerca.

Art. 4 (Principi in materia di informazione e riservatezza dei dati personali)

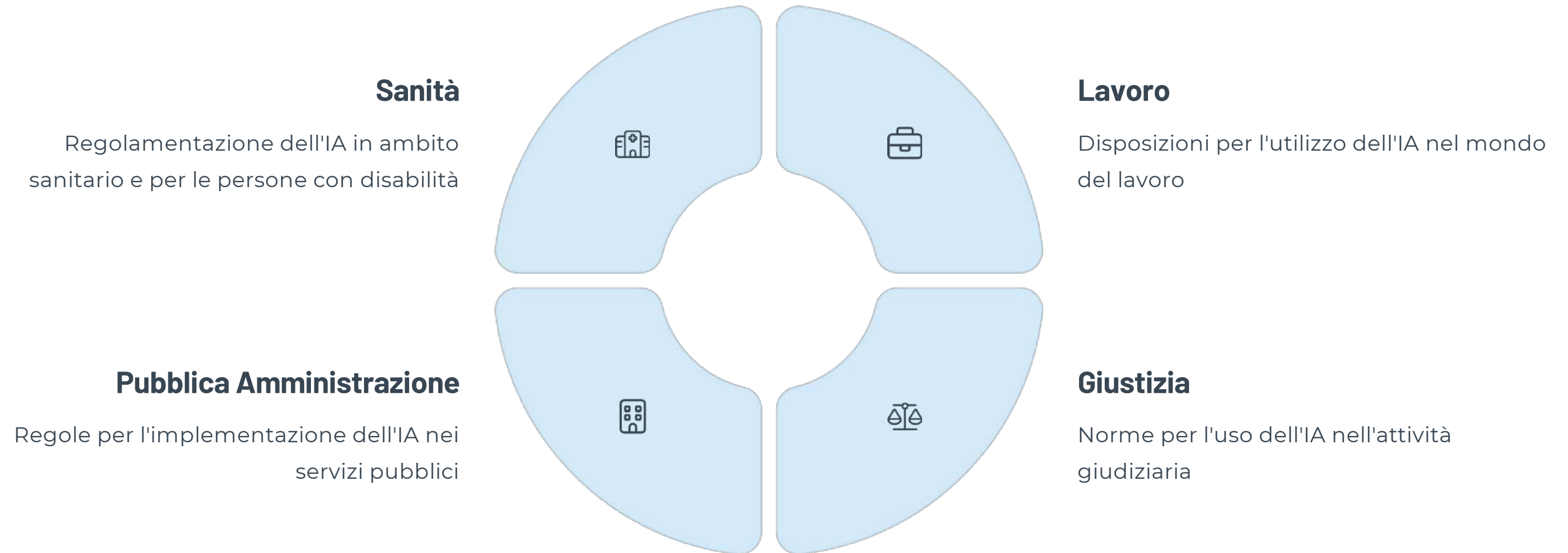
Stabilisce che l'uso dell'IA nell'informazione non deve pregiudicare la libertà e il pluralismo dei mezzi di comunicazione, la libertà di espressione, o l'obiettività, completezza, imparzialità e lealtà dell'informazione. Garantisce il trattamento lecito e trasparente dei dati personali, richiedendo un linguaggio chiaro e semplice per informare gli utenti sui rischi e sul diritto di opporsi al trattamento dei dati. Prevede il consenso per l'accesso alle tecnologie IA da parte di minori.

Art. 6 (Disposizioni in materia di sicurezza nazionale e difesa)

Esclude dall'ambito di applicazione della legge le attività connesse ai sistemi e modelli di intelligenza artificiale condotte a fini di **sicurezza nazionale, cybersicurezza e difesa nazionale**, le quali **restano regolate da normative specifiche**, pur dovendo rispettare i diritti fondamentali. La proposta di richiedere che i sistemi di intelligenza artificiale destinati all'uso in ambito pubblico fossero installati su server ubicati nel territorio nazionale, al fine di garantire la sovranità e la sicurezza dei dati sensibili dei cittadini, **è stata soppressa nel testo finale della Camera.**

2. Disposizioni Settoriali (Art. 7 – 18)

Questo capitolo introduce norme specifiche per l'applicazione dell'IA in diversi settori chiave.



Disposizioni Settoriali: Sanità



Art. 7 (Uso dell'intelligenza artificiale in ambito sanitario e di disabilità)

L'IA è concepita per migliorare il sistema sanitario, la prevenzione, la diagnosi e la cura, nel rispetto dei diritti individuali e della protezione dei dati. Vieta l'introduzione di sistemi IA che selezionino o condizionino l'accesso alle prestazioni sanitarie in modo discriminatorio. L'interessato ha diritto di essere informato sull'impiego di tecnologie IA. Promuove lo sviluppo di sistemi IA per migliorare le condizioni di vita delle persone con disabilità, facilitando accessibilità e inclusione sociale. I sistemi IA in sanità devono supportare, non sostituire, le decisioni mediche, che rimangono prerogativa esclusiva dei professionisti. Devono essere affidabili, verificati e aggiornati per minimizzare il rischio di errori.



Art. 8 (Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario)

Dichiara di rilevante interesse pubblico il trattamento di dati, anche personali, per la ricerca scientifica in IA in ambito sanitario, per lo sviluppo di farmaci, terapie e dispositivi medici. Autorizza l'uso secondario di dati personali anonimizzati per tali scopi. AGENAS può stabilire linee guida per l'anonimizzazione dei dati.



Art. 9 (Disposizioni in materia di trattamento dei dati personali)

Prevede che il trattamento semplificato dei dati personali per la ricerca e sperimentazione di IA e machine learning sarà regolato da un decreto del Ministro della Salute, riconoscendo l'importanza di bilanciare innovazione tecnologica e tutela della riservatezza.



Art. 10 (Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza e governance della sanità digitale)

Introduce disposizioni per l'IA nel settore sanitario, inclusa la creazione di una piattaforma nazionale di IA per la sanità digitale, gestita da AGENAS, per supportare medici, utenti e amministrazioni.

Disposizioni Settoriali: Lavoro e Professioni e P.A

Art. 11 (Disposizioni in materia di intelligenza artificiale in materia di lavoro)

L'IA deve essere impiegata per **migliorare le condizioni di lavoro, tutelare l'integrità psicofisica dei lavoratori, accrescere la qualità delle prestazioni** e la produttività, sempre nel rispetto dei diritti inviolabili del lavoratore e della privacy. I datori di lavoro devono informare i lavoratori sull'uso dell'IA.

Art. 12 (Osservatorio sull'adozione dell'intelligenza artificiale nel mondo del lavoro)

Istituisce un Osservatorio presso il Ministero del Lavoro e delle Politiche Sociali con l'obiettivo di definire una strategia per l'IA nel lavoro, monitorarne l'impatto sul mercato e promuovere la formazione, rafforzando trasparenza e responsabilità.

Art. 13 (Disposizioni in materia di professioni intellettuali)

L'uso dell'IA nelle professioni intellettuali è limitato a funzioni strumentali e di supporto all'attività professionale, mantenendo la prevalenza del lavoro intellettuale umano. Per preservare il rapporto fiduciario, i professionisti devono comunicare in modo chiaro e semplice al cliente le informazioni relative ai sistemi di IA utilizzati.

Art. 14 (Pubblica amministrazione e intelligenza artificiale)

Autorizza le pubbliche amministrazioni a impiegare sistemi di intelligenza artificiale per migliorare l'efficienza e la qualità dei servizi erogati, riducendo tempi e costi. Impone obblighi di tracciabilità e trasparenza nell'uso degli strumenti IA e richiede percorsi formativi e organizzativi per il personale, garantendo un impiego consapevole. Le PA devono rispettare i limiti normativi esistenti e operare con le risorse già disponibili. L'IA è uno strumento di supporto, con i decisori umani che rimangono gli unici responsabili il comma 2 è molto chiaro "L'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale "

Disposizioni Settoriali: Giustizia e Cybersicurezza

Art. 15 (Uso dei sistemi di intelligenza artificiale nell'attività giudiziaria)

Stabilisce che ogni decisione nel processo giudiziario rimane inderogabilmente riservata al magistrato. L'IA può supportare, ma non sostituire, l'interpretazione della legge, la valutazione delle prove o l'adozione di provvedimenti. L'uso dell'IA è ammesso per l'organizzazione dei sistemi relativi alla giustizia, la semplificazione del lavoro giudiziario e le attività amministrative accessorie. Ogni sperimentazione di sistemi di IA nei tribunali deve essere autorizzata. Promuove la formazione dei magistrati e del personale amministrativo per un uso consapevole e sicuro dell'IA.

Art. 17 (Modifica al codice di procedura civile)

Modifica l'Articolo 9, comma 2, del codice di procedura civile, inserendo la competenza esclusiva del tribunale per le cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale, escludendo i giudici di pace.

Art. 16 (Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento dell'intelligenza artificiale)

Delega il Governo ad adottare decreti legislativi per definire una disciplina organica sull'uso di dati, algoritmi e metodi matematici per l'addestramento dell'IA, includendo diritti, obblighi, senza possibilità di introdurre altri, e misure di protezione, nonché sanzioni per gli usi illeciti.

Art. 18 (Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale)

Promuove e sviluppa iniziative per valorizzare l'IA come risorsa per rafforzare la cybersicurezza nazionale, anche attraverso partenariati pubblico-privato.

3. Governance (Art. 19 - 24)

La terza parte del disegno di legge riguarda la governance:



Questa sezione definisce la struttura di governance per l'implementazione e la supervisione delle normative sull'intelligenza artificiale in Italia.

Governance: Strategia Nazionale e Autorità

Art. 19 (Strategia nazionale per l'intelligenza artificiale)

La **Presidenza del Consiglio**, in accordo con le autorità nazionali per l'IA, è incaricata di **elaborare e aggiornare la strategia nazionale sull'IA** con cadenza almeno biennale. Promuove la collaborazione tra pubblico e privato e coordina le attività della pubblica amministrazione.



Art. 20 (Autorità nazionali per l'intelligenza artificiale)

Designa **AgID (Agenzia per l'Italia Digitale)** e **ACN (Agenzia per la Cybersicurezza Nazionale)** come **Autorità Nazionali per l'IA**.

AgID è responsabile della **promozione dell'innovazione e dello sviluppo dell'IA**

ACN è incaricata della **vigilanza, ispezione e sanzionamento dei sistemi IA, e della promozione dell'IA in cybersicurezza**.

Entrambe gestiranno spazi di sperimentazione congiunti e collaboreranno con le autorità finanziarie (Banca d'Italia, CONSOB, IVASS).

Viene istituito un **Comitato di coordinamento presso la Presidenza del Consiglio** per garantire il raccordo tra le istituzioni, e restano ferme le competenze del Garante per la protezione dei dati personali.

Governance: Deleghe al Governo



Adeguamento Normativo

Delega il Governo ad adottare decreti legislativi per adeguare la legislazione nazionale al Regolamento (UE) 2024/1689.



Poteri di Vigilanza

Attribuzione di poteri di vigilanza e sanzionatori alle autorità nazionali designate.



Formazione

Promozione dell'alfabetizzazione e della formazione sull'intelligenza artificiale.



Uso Illecito

Definizione dei casi di realizzazione e uso illecito dell'IA, comprese le fattispecie penali e la responsabilità civile.

Art. 24 (Deleghe al Governo in materia di intelligenza artificiale): Delega il Governo ad adottare decreti legislativi per adeguare la legislazione nazionale al Regolamento (UE) 2024/1689, inclusa l'attribuzione di poteri di vigilanza e sanzionatori alle autorità nazionali, e la promozione dell'alfabetizzazione e della formazione sull'IA. Delega inoltre il Governo a definire i casi di realizzazione e uso illecito dell'IA, comprese le fattispecie penali e la responsabilità civile.



MODIFICHE AL CODICE PENALE E ALTRE DISPOSIZIONI PENALI

4. Nuove Fattispecie di Reato (Art. 26)

Circostanze Aggravanti

Nuove circostanze aggravanti comuni per i reati commessi mediante sistemi di intelligenza artificiale

1

Deepfake e Contenuti Alterati

Sanzioni per la diffusione illecita di contenuti generati o alterati dall'IA come deepfake e immagini pornografiche non consensuali

2

3

4

Frode mediante IA

Introduzione di nuovi reati specifici per la frode realizzata attraverso sistemi di intelligenza artificiale

Reati Societari

Modifiche alle leggi esistenti sui reati societari e l'intermediazione finanziaria per includere i reati legati all'IA

Le Linee Guida AGID per l'Adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione

L'integrazione dell'Intelligenza Artificiale (IA) nella Pubblica Amministrazione (PA) italiana rappresenta una frontiera strategica per l'innovazione e l'efficienza dei servizi pubblici. In questo contesto, l'Agenzia per l'Italia Digitale (AgID) ha elaborato un quadro di riferimento fondamentale attraverso le sue Linee Guida per l'adozione di sistemi di IA nella PA. Questo documento non è una mera raccolta di raccomandazioni, ma un provvedimento strutturato che mira a guidare le amministrazioni attraverso un percorso complesso, garantendo conformità normativa, tutela dei diritti fondamentali e promozione di un'innovazione responsabile.

IL documento, nella sua versione attuale, è in fase di consultazione pubblica.

La **consultazione** è stata avviata il **18 febbraio 2025** con la Determinazione n. 17/2025 ed è **terminata il 20 marzo 2025**.

Questa fase ha permesso a tutti gli interessati di inviare commenti, suggerimenti e proposte di modifica o integrazione tramite Forum Italia, contribuendo così alla definizione finale del testo.

Contesto e quadro normativo delle Linee Guida AGID sull'IA nella PA



D.P.C.M. 12 gennaio 2024

Piano Triennale per l'informatica nella pubblica amministrazione 2024-2026



Codice dell'Amministrazione Digitale

Articolo 2, comma 1 del CAD - pilastro della normativa italiana sulla digitalizzazione



Procedure di Emanazione

Articolo 71 del CAD e Determinazione AgID n. 160 del 17 maggio 2018

Le Linee Guida AGID sull'Intelligenza Artificiale nella Pubblica Amministrazione si inseriscono in un contesto normativo e strategico ben definito, riflettendo l'impegno dell'Italia verso la digitalizzazione del settore pubblico. Questo documento è stato emanato in conformità con il D.P.C.M. del 12 gennaio 2024, che stabilisce il "Piano Triennale per l'informatica nella pubblica amministrazione 2024-2026".

La sua genesi è altresì ancorata all'articolo 2, comma 1 del Codice dell'Amministrazione Digitale (CAD), un pilastro della normativa italiana sulla digitalizzazione. L'intero processo di emanazione ha seguito le procedure delineate dall'articolo 71 del CAD e ha rispettato la Determinazione AgID n. 160 del 17 maggio 2018, che regola l'adozione di linee guida per l'attuazione del CAD stesso.

Ambito di applicazione

Ambito Soggettivo

L'ambito di applicazione di queste Linee Guida si rivolge a tutti i soggetti indicati nell'articolo 2, comma 2, del CAD, i quali sono collettivamente identificati nel documento con l'acronimo "PA". Questo include un'ampia varietà di enti pubblici, dalle amministrazioni centrali a quelle locali.



Ambito Oggettivo

L'ambito oggettivo, invece, si concentra sulle modalità di adozione dei sistemi di Intelligenza Artificiale, con una particolare enfasi sulla conformità normativa e sull'impatto organizzativo che tali sistemi possono generare.



Struttura del documento

La struttura del documento è stata concepita per garantire un costante adattamento ai rapidi cambiamenti imposti dalla rivoluzione digitale. A tal fine, le Linee Guida sono corredate da 9 allegati, definiti "strumenti", i cui contenuti sono progettati per essere facilmente aggiornati in base all'evoluzione tecnologica.

Linee Guida Principali
Documento base con principi
fondamentali



9 Allegati "Strumenti"

Contenuti facilmente aggiornabili

Aggiornamenti Periodici

Adattamento all'evoluzione tecnologica

Gli allegati coprono aree cruciali

1 Valutazione del livello di maturità nell'adozione di IA

Allegato A fornisce strumenti per misurare quanto un'amministrazione è pronta ad implementare soluzioni di IA

2 Valutazione del rischio

Allegato B offre metodologie per identificare e mitigare i rischi associati all'implementazione dell'IA

3 Valutazione d'impatto

Allegato C presenta strumenti per analizzare le conseguenze dell'adozione dell'IA sui processi e servizi

4 Modello di codice etico

Allegato D propone linee guida etiche per l'utilizzo responsabile dell'IA nella PA

5 Norme tecniche rilevanti

Allegato E raccoglie gli standard tecnici applicabili ai sistemi di IA

6 Documentazione dei casi d'uso

Allegato F fornisce esempi pratici di implementazione dell'IA nella PA

7 Classificazione delle funzionalità dell'IA

Allegato G categorizza le diverse capacità e applicazioni dell'IA

8 Procedure di governance

Allegato H delinea i processi decisionali e di supervisione per i sistemi di IA

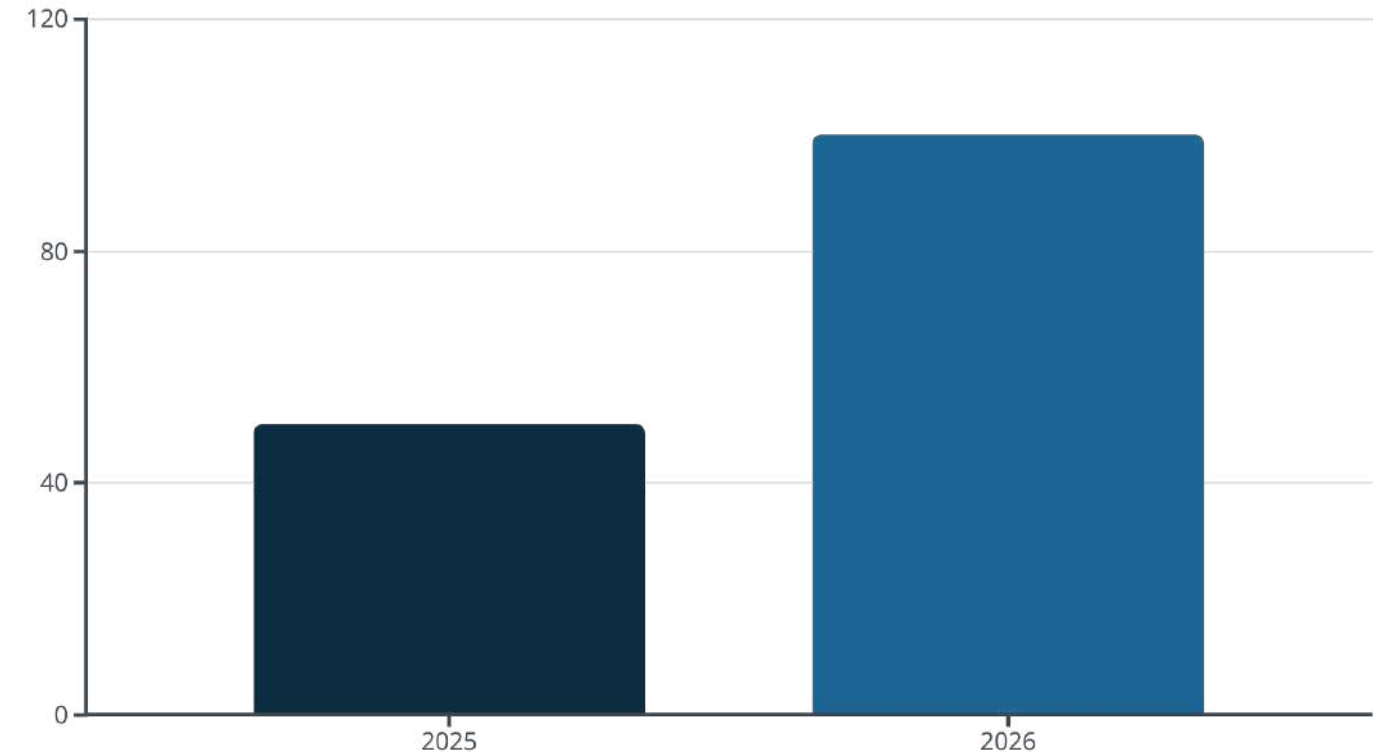
9 Indicatori di prestazione

Allegato I presenta metriche per valutare l'efficacia dei sistemi di IA implementati

Questa metodologia è in linea con quanto previsto dall'articolo 14-bis, comma 2, lettera a) del CAD, che promuove un approccio flessibile alla regolamentazione digitale.

Natura dinamica e adattiva della regolamentazione dell'IA nella PA

La **natura dinamica** e adattiva della regolamentazione dell'IA nella PA è un aspetto fondamentale di questo provvedimento. Il fatto che le linee guida siano ancora una bozza e soggette a consultazione pubblica, insieme alla progettazione degli allegati come strumenti aggiornabili, rivela una filosofia regolatoria che riconosce la rapida evoluzione della tecnologia IA. L'AgID **non** sta cercando di creare un **regolamento statico e rigido**, ma piuttosto un quadro agile capace di evolvere. Questo implica che **per le PA**, la conformità non è un traguardo da raggiungere una volta per tutte, ma un **processo continuo di monitoraggio degli aggiornamenti e di adattamento delle procedure interne**. Offre inoltre agli stakeholder l'opportunità di influenzare il testo finale, promuovendo un ambiente regolatorio più collaborativo.



Obiettivi per progetti IA nel Piano Triennale

Inoltre, l'IA nella PA è chiaramente posizionata come una parte integrante della strategia nazionale di digitalizzazione.

Il collegamento diretto delle Linee Guida con il "Piano Triennale per l'informatica nella pubblica amministrazione 2024-2026", che fissa obiettivi ambiziosi per i progetti di IA (ad esempio, almeno 50 progetti avviati nel 2025 e 100 nel 2026), dimostra che l'adozione dell'IA non è un'iniziativa isolata ma una componente centrale dell'agenda di trasformazione digitale italiana.

Terminologia delle Linee Guida

Termini Chiave Adottati

Linee Guida adottano i termini chiave: «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUÒ», «POSSONO» e «OPZIONALE», definiti dalle norme ISO/IEC Directives, Part 2 "Principles and rules for the structure and drafting of ISO and IEC documents" per la stesura dei documenti tecnici.

Questi termini tecnici sono fondamentali per comprendere il livello di obbligatorietà o discrezionalità delle disposizioni contenute nelle Linee Guida, seguendo gli standard internazionali per la redazione di documenti tecnici.



L'interpretazione di tali termini

L'interpretazione di tali termini:

La corretta interpretazione della terminologia è essenziale per comprendere il grado di vincolatività delle disposizioni contenute nelle Linee Guida e per garantire un'implementazione conforme ai requisiti stabiliti.



Technical Terminology



Significato dei Termini Chiave



DEVE o DEVONO

Indicano un requisito obbligatorio



NON DEVE o NON DEVONO o NON PUÒ o NON POSSONO

Indicano un assoluto divieto



DOVREBBE o NON DOVREBBE

Indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi



PUÒ o POSSONO o l'aggettivo OPZIONALE

Indica che l'operatore può scegliere di applicare o meno la specifica

Questa classificazione dei termini permette alle amministrazioni di distinguere chiaramente tra requisiti obbligatori, divieti assoluti, raccomandazioni che richiedono attenta valutazione e disposizioni opzionali, facilitando così l'implementazione conforme delle Linee Guida.

Principi generali per l'adozione dell'IA nella Pubblica Amministrazione

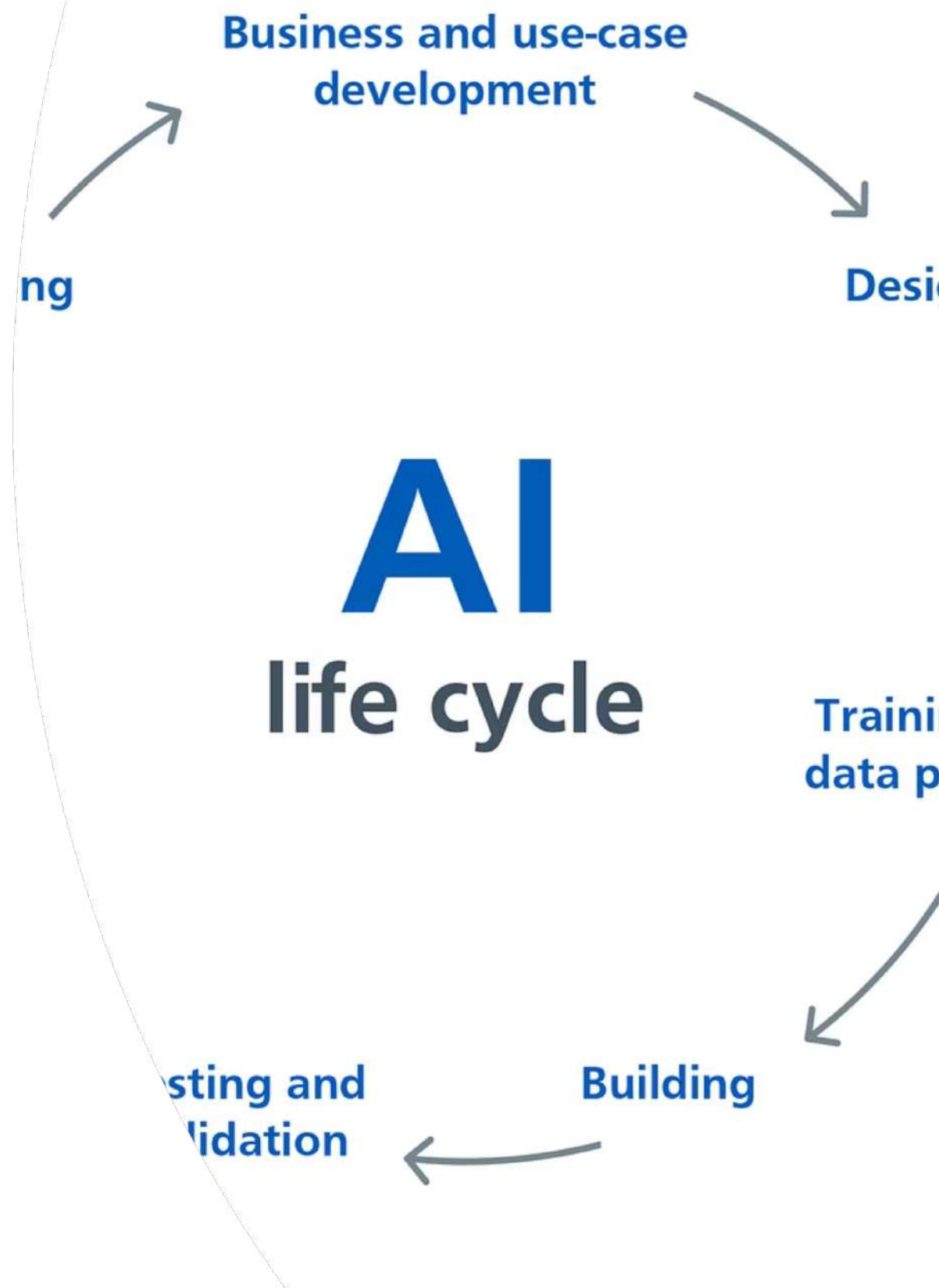
Il Capitolo 3 delle Linee Guida AGID stabilisce un insieme di principi fondamentali che devono guidare le Pubbliche Amministrazioni nell'adozione, nell'acquisto e nello sviluppo di sistemi di Intelligenza Artificiale. Questi principi sono stati formulati per assicurare che l'IA sia impiegata in modo etico, responsabile e conforme alle normative vigenti, massimizzando al contempo i benefici per i cittadini e per l'efficienza amministrativa.



Il Ciclo di Vita

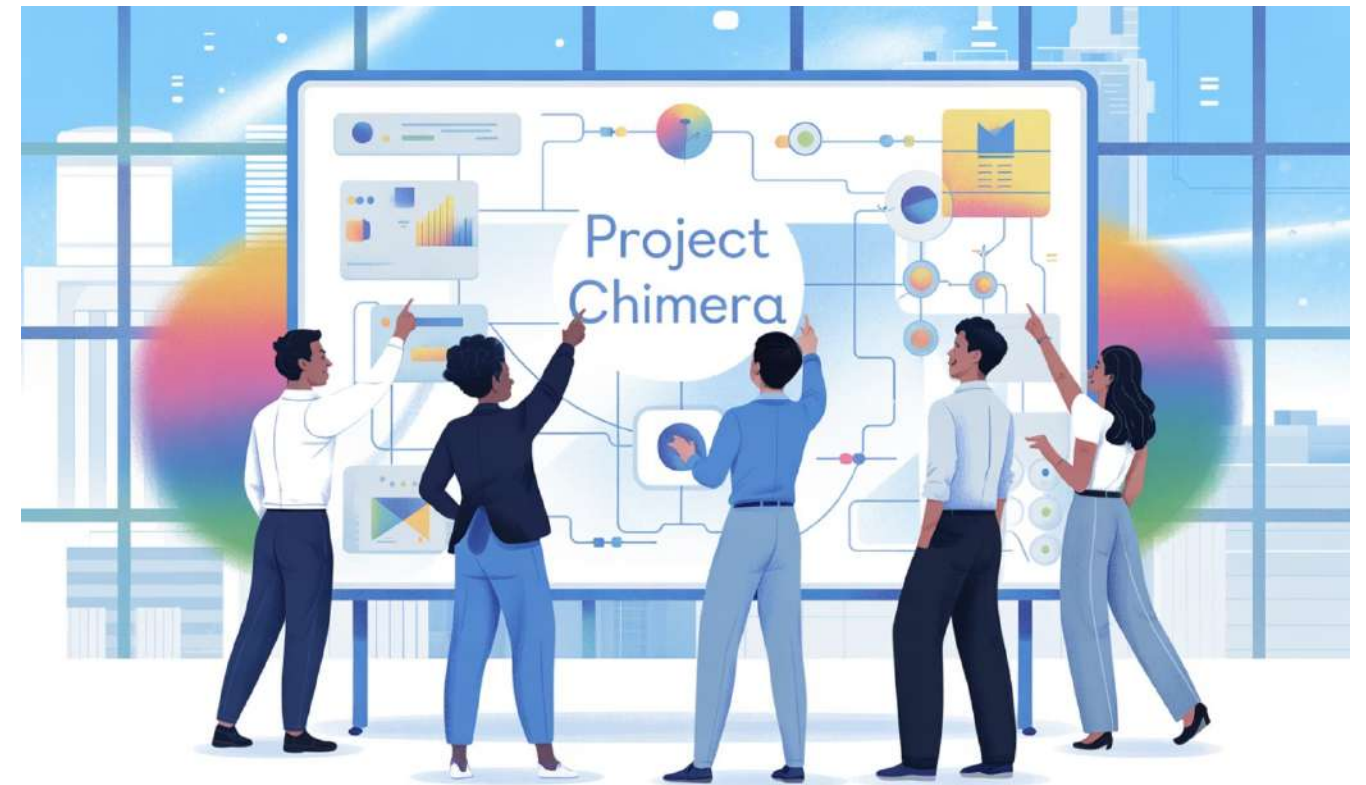
Le Linee Guida per l'adozione dell'Intelligenza Artificiale (IA) nella Pubblica Amministrazione (PA) adottano come modello di riferimento il ciclo di vita di un sistema di IA definito dall'OCSE. Questo ciclo descrive le diverse fasi che un sistema di IA attraversa, dalla pianificazione iniziale fino alla sua dismissione.

Le fasi principali del ciclo di vita di un sistema di IA:



Pianificazione e design

In questa fase, l'organizzazione (PA) **identifica l'obiettivo** che il sistema di IA deve raggiungere, comprendendo il contesto operativo e i dati necessari. Include la **definizione dei bisogni** e requisiti degli stakeholder, la loro traduzione in requisiti tecnici misurabili e la progettazione dell'architettura e del design del sistema.



Raccolta e processamento dei dati

Acquisizione

I dati (strutturati e non) e i metadati vengono acquisiti da varie fonti

Analisi

Verifica dell'adattamento a distribuzioni statistiche

Pulizia

Integrazione e trasformazione secondo le esigenze

Selezione

Identificazione delle caratteristiche più rilevanti, scartando quelle non pertinenti

È fondamentale seguire le indicazioni sulla gestione e qualità dei dati. Le caratteristiche più rilevanti del dataset vengono identificate e selezionate, scartando quelle non pertinenti, per ridurre le dimensioni del dataset.



Costruzione e/o addestramento dei modelli



Selezione del modello

L'organizzazione costruisce o seleziona un modello di IA appropriato per l'obiettivo e i dati disponibili.

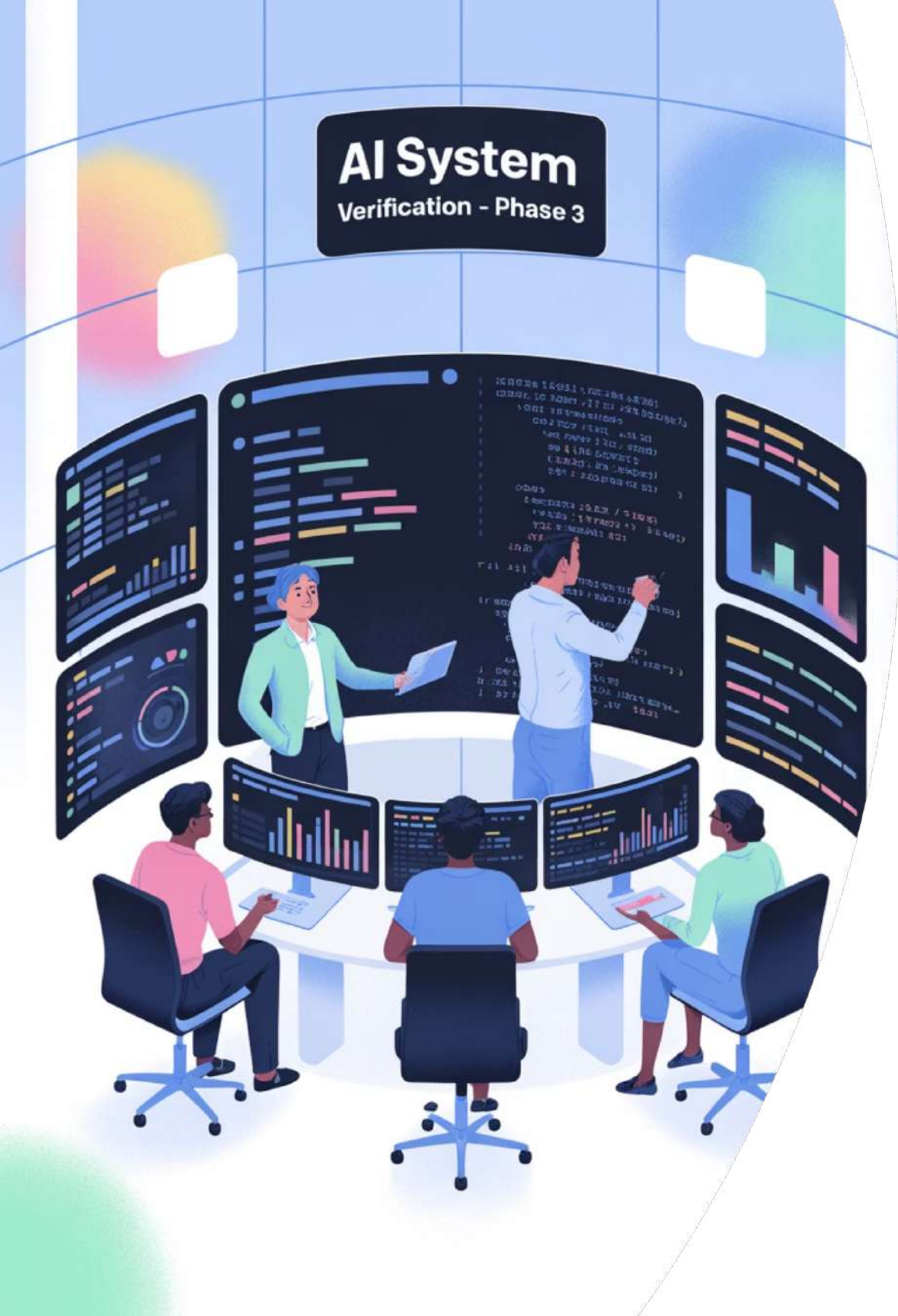
Scelta degli algoritmi

Questa scelta include quella degli algoritmi di apprendimento (supervisionato, non supervisionato, con rinforzo).

Addestramento e tuning

Il modello viene poi addestrato sui dati con l'algoritmo scelto, seguito da una fase di "tuning" per regolare gli iperparametri basandosi su un dataset di convalida.

In alternativa, si può optare per il "trasferimento dell'apprendimento", acquisendo un modello IA già addestrato e configurato, specialmente se non si dispone di dati sufficienti per l'addestramento⁶.



Testing, valutazione, verifica e validazione



Test rigorosi

Il sistema di IA è sottoposto a test rigorosi per garantire che soddisfi i requisiti e le aspettative degli stakeholder.



Risoluzione anomalie

Si identificano e risolvono anomalie, verificando che il modello operi correttamente nel contesto previsto.



Verifica conformità

Si verifica che il sistema rispetti i criteri di conformità e qualità stabiliti.

Messa a disposizione per l'utilizzo o il dispiegamento

Il sistema di IA addestrato viene reso disponibile agli utenti e integrato nei processi operativi, assicurando compatibilità con altri sistemi e accessibilità per tutti gli utenti previsti.



Integrazione

Collegamento con i sistemi esistenti



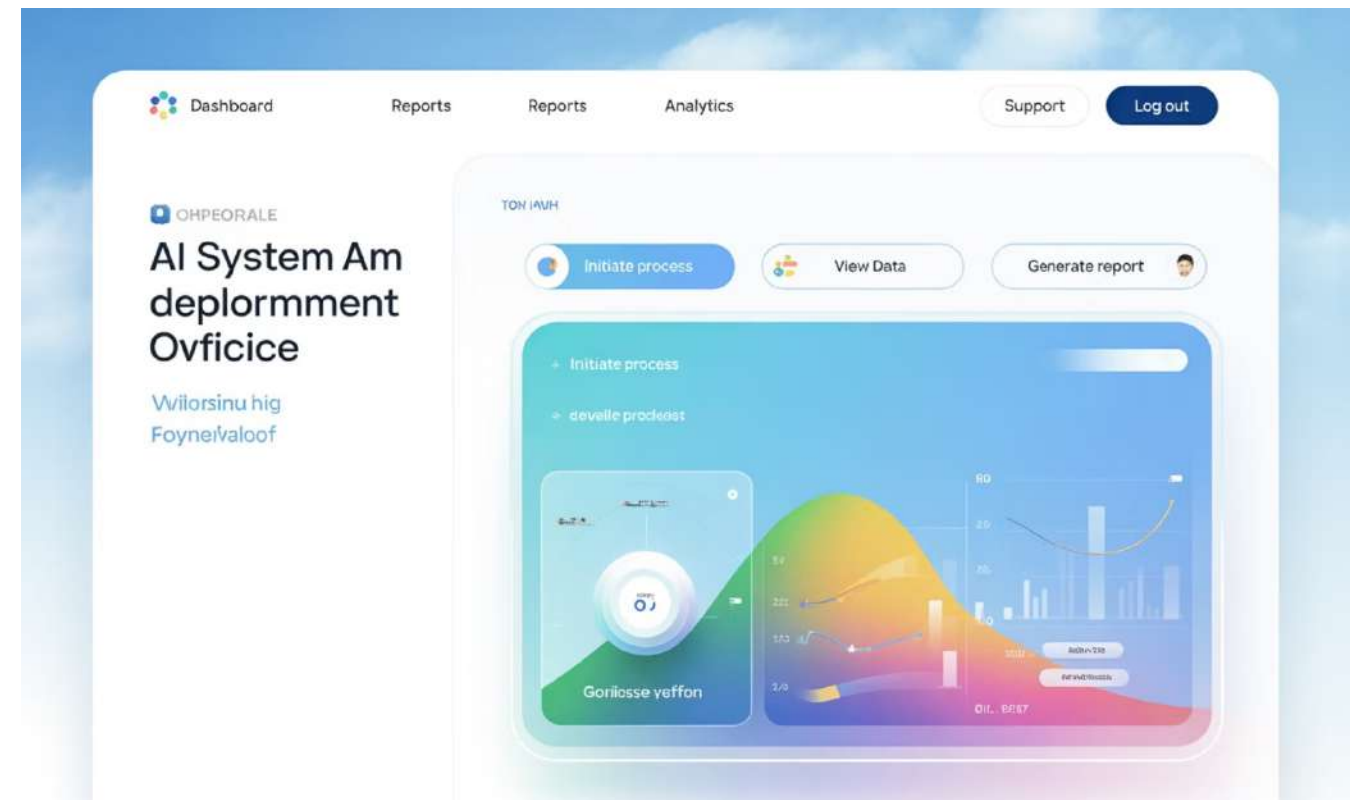
Accessibilità

Disponibilità per tutti gli utenti previsti



Operatività

Funzionamento nei processi di lavoro





Operatività e monitoraggio

Il sistema di IA e i dati in ingresso sono monitorati continuamente per rilevare variazioni nei pattern operativi, anomalie nei dati o l'insorgenza di bias che potrebbero compromettere l'affidabilità delle decisioni.

1

Monitoraggio continuo

Controllo costante del sistema e dei dati in ingresso

2

Manutenzione

Attività di manutenzione e ottimizzazione del modello

3

Riaddestramento

Aggiornamento del modello con nuovi dati quando necessario

4

Valutazione

Verifica costante del raggiungimento degli obiettivi e dell'efficacia operativa

Ritiro/Disattivazione

Quando il sistema di IA non è più necessario, viene ritirato o disattivato in modo controllato. Questa fase include la gestione sicura dei dati, la documentazione delle operazioni finali e la pianificazione di eventuali sostituzioni o alternative.



Gestione sicura dei dati

Archiviazione o eliminazione sicura di tutti i dati sensibili

Documentazione finale

Registrazione completa delle operazioni di disattivazione

Pianificazione alternative

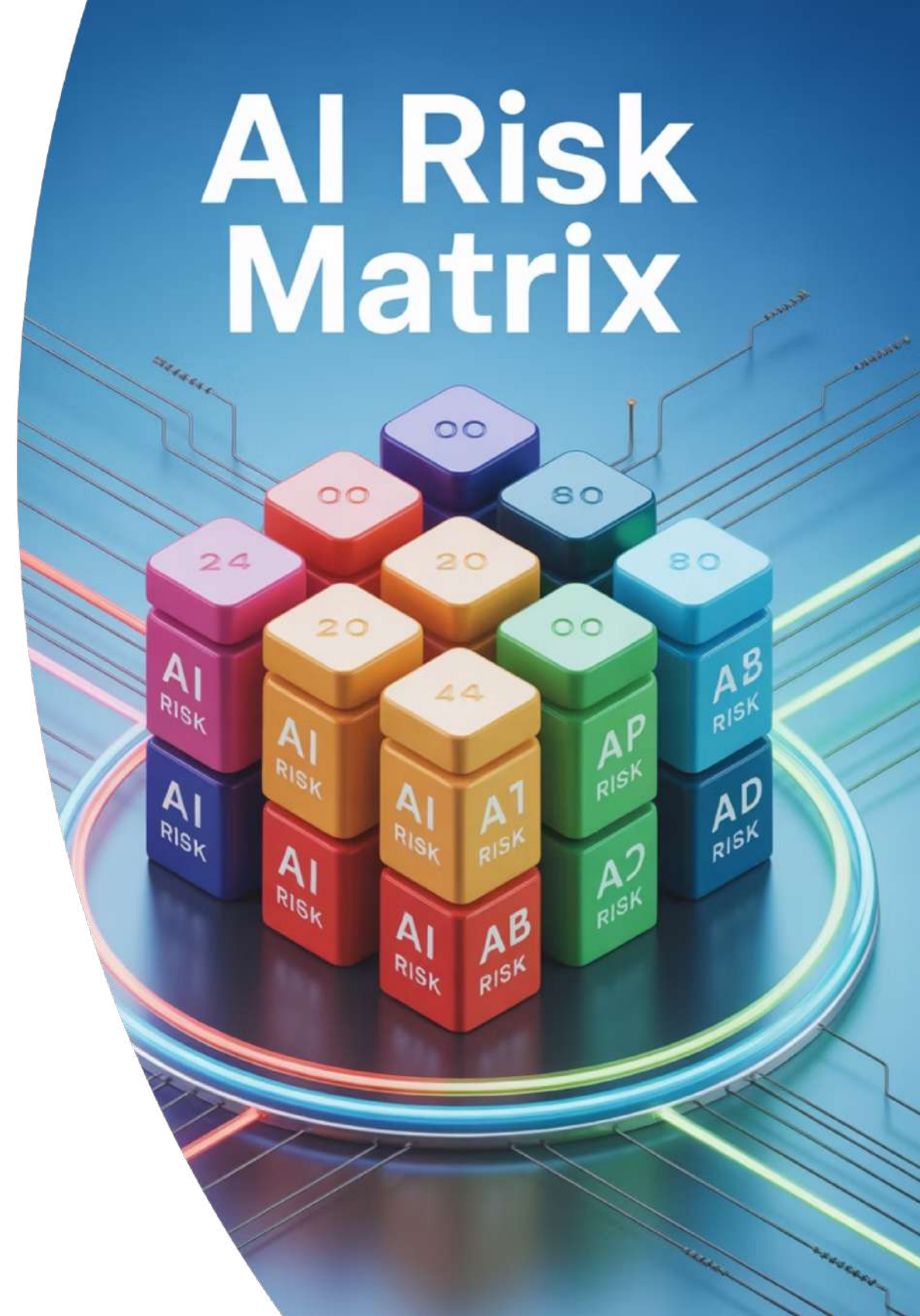
Preparazione di sistemi sostitutivi o soluzioni alternative

CLASSIFICAZIONE DEI SISTEMI AI SULLA BASE DEL RISCHIO

Le Linee Guida per l'adozione di Intelligenza Artificiale (IA) nella Pubblica Amministrazione (PA) classificano i sistemi di IA sulla base del rischio, un approccio adottato dall'AI Act, poiché l'IA, pur offrendo notevoli benefici, può comportare rischi per gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione.

Le PA DEVONO tenere in considerazione questa classificazione.

Il documento distingue i sistemi di IA nei seguenti livelli di rischio:



Sistemi di IA vietati



Gli obblighi relativi agli usi vietati dell'IA sono entrati in vigore il 2 febbraio 2025, e la Commissione europea ha pubblicato apposite linee guida in merito.

Sono considerati sistemi a rischio inaccettabile e, pertanto, sono vietati. L'articolo 5 dell'AI Act fornisce un elenco di tali sistemi. Esempi includono IA che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole, tecniche volutamente manipolative o ingannevoli volte a distorcere il comportamento delle persone, meccanismi di sfruttamento delle persone vulnerabili o sistemi di IA che introducano meccanismi di "social scoring".



Tecniche subliminali

IA che agiscono senza che una persona ne sia consapevole



Tecniche manipolative

Sistemi volutamente ingannevoli volti a distorcere il comportamento delle persone



Sfruttamento vulnerabilità

Meccanismi che sfruttano persone vulnerabili



Social scoring

Sistemi di IA che introducono meccanismi di valutazione sociale

Sistemi di IA ad alto rischio

Questi sistemi pongono elevati rischi. In caso di malfunzionamento, possono causare una rilevante dannosità, con un'alta compromissione di interessi pubblici e diritti fondamentali.

Le PA DEVONO fare riferimento al sistema di classificazione delineato dall'AI Act, in particolare all'articolo 6 e all'Allegato III, per qualificare un sistema come ad alto rischio.

Le PA DOVREBBERO inoltre considerare che la Commissione europea ha il potere di adottare atti delegati per aggiungere o modificare i casi d'uso dei sistemi di IA ad alto rischio di cui all'Allegato III dell'AI Act.



Carta dei diritti fondamentali dell'UE

Rispettare i principi della Carta, valutando l'impatto dei sistemi di IA sui diritti tutelati



Dichiarazione europea sui diritti digitali

Considerare la Dichiarazione per il Digital Decade, assicurando l'allineamento delle applicazioni IA ai valori europei

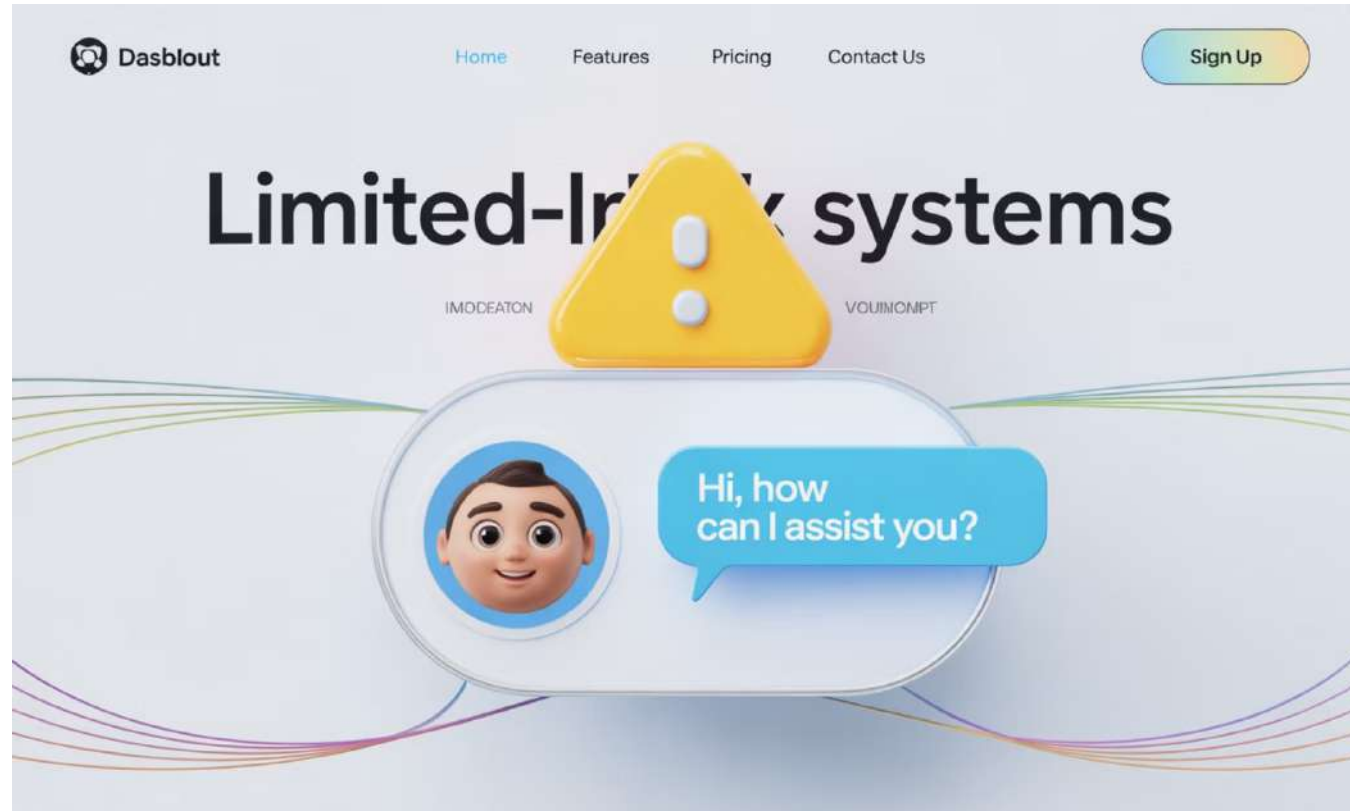


Orientamenti etici AI HLEG

Seguire gli Orientamenti etici per un'IA affidabile dell'AI HLEG, promuovendo trasparenza, equità e responsabilità nell'uso dell'IA

Per i sistemi di IA ad alto rischio, oltre agli obblighi previsti dall'AI Act, le PA DEVONO garantire un costante ed elevato livello di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali.

Sistemi di IA a rischio limitato



Sono sistemi con un rischio minore. In caso di malfunzionamento, si contraddistinguono per una potenziale dannosità limitata (ad esempio, chatbot generici) e un impatto limitato su interessi pubblici e diritti fondamentali.



Chatbot generici

Assistenti virtuali con funzionalità limitate



Impatto limitato

Effetti contenuti su diritti fondamentali

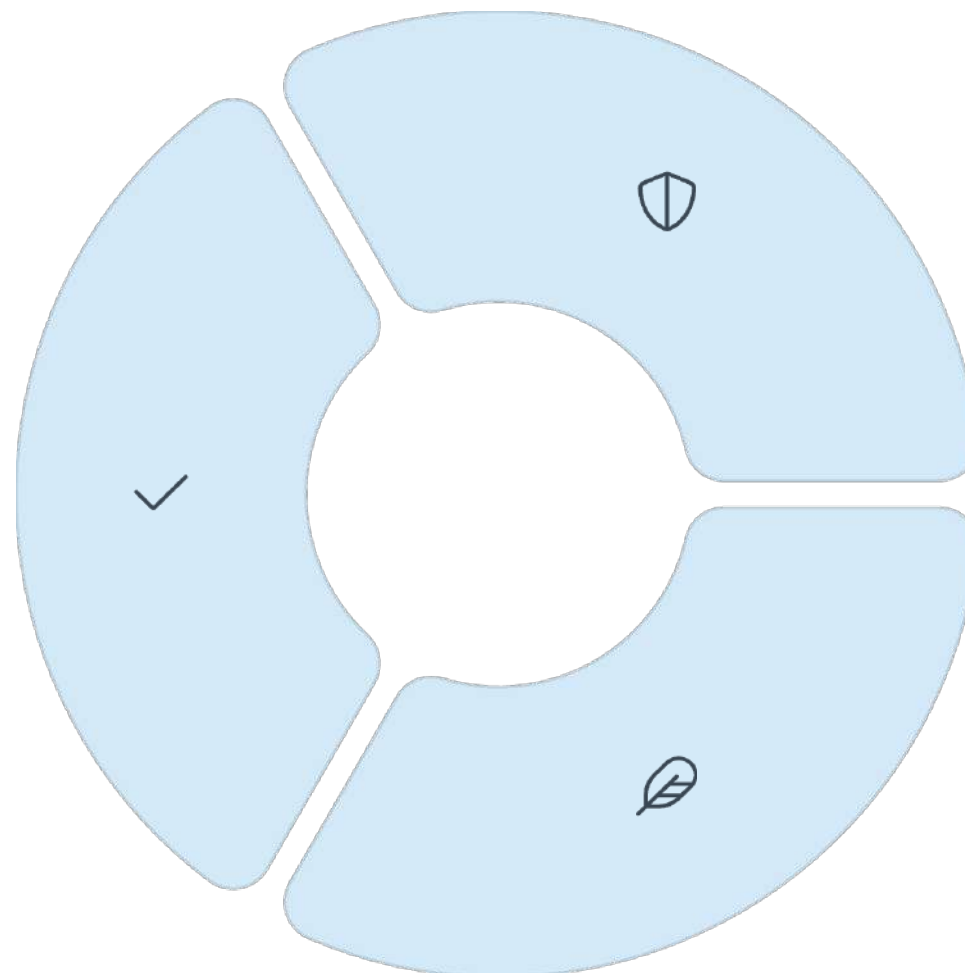


Dannosità ridotta

Conseguenze minori in caso di malfunzionamento

Sistemi di IA a rischio minimo o nullo

Rischio irrilevante
Questi sistemi presentano un rischio praticamente nullo per gli utenti



Dannosità molto limitata

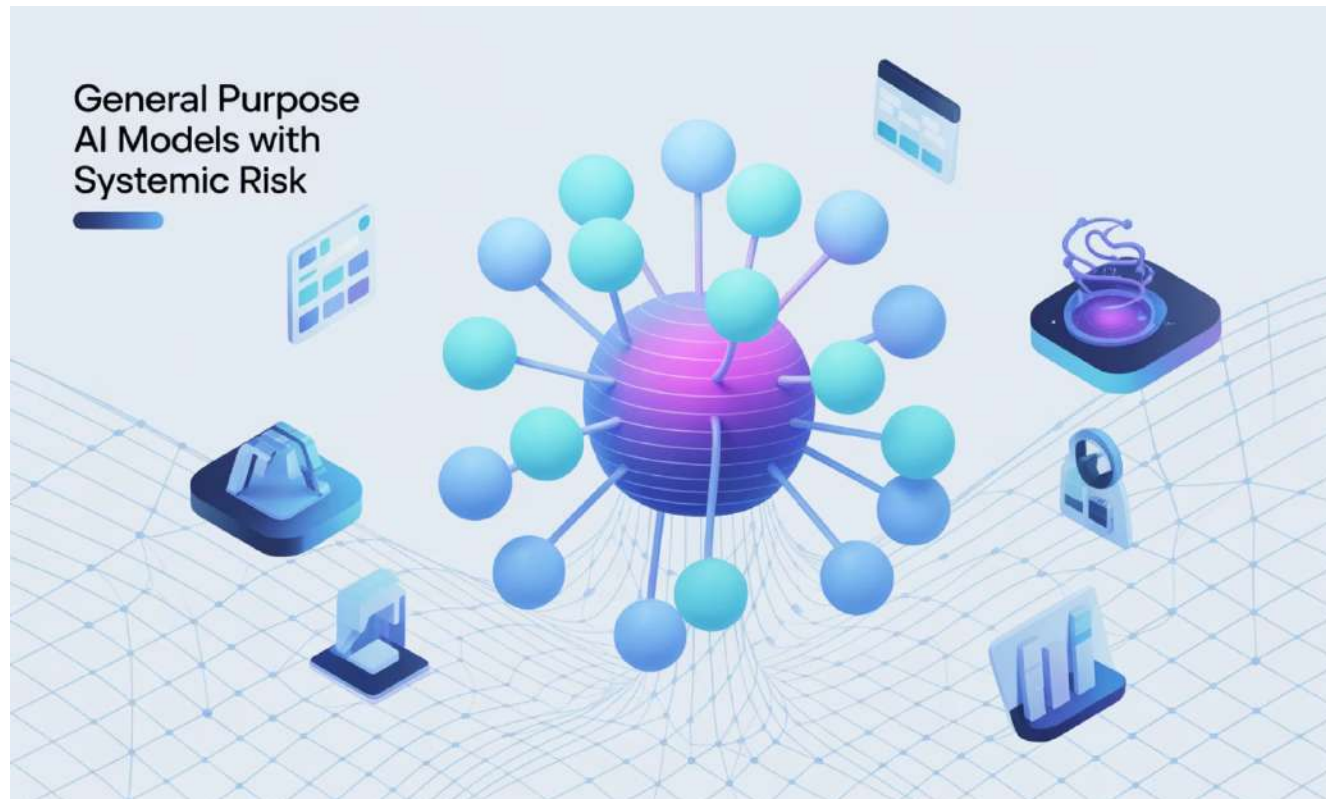
In caso di malfunzionamento, le conseguenze sono minime

Impatto trascurabile

Effetti quasi nulli su interessi pubblici e diritti fondamentali

Questi sistemi presentano un rischio irrilevante. La loro dannosità, in caso di malfunzionamento, è molto limitata, potendo avere un impatto del tutto trascurabile su interessi pubblici e diritti fondamentali.

Modelli di IA per finalità generali (GPAI)



Regolamentazione specifica

È inoltre specificato che il Capo V dell'AI Act definisce una regolamentazione specifica per i modelli di IA per finalità generali (GPAI) con rischio sistemico, che possono avere effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica.



Rischio sistemico

Modelli che possono avere impatti su larga scala



Effetti sulla salute pubblica

Conseguenze prevedibili sul benessere collettivo



Capo V dell'AI Act

Sezione dedicata alla regolamentazione di questi modelli

PRINCIPI PER L'ADOZIONE DELL'AI NELLA PA



Finalità dell'IA nella Pubblica Amministrazione

Le PA sono chiamate ad adottare l'IA con obiettivi chiari e misurabili, che si concentrano su quattro finalità principali:

 **Automatizzare attività semplici e ripetitive**

L'IA deve liberare il personale da compiti di ricerca e analisi delle informazioni che sono di natura ripetitiva, consentendo ai dipendenti di dedicarsi ad attività a maggior valore aggiunto e migliorando l'efficienza operativa complessiva.

 **Supportare la personalizzazione dei servizi**

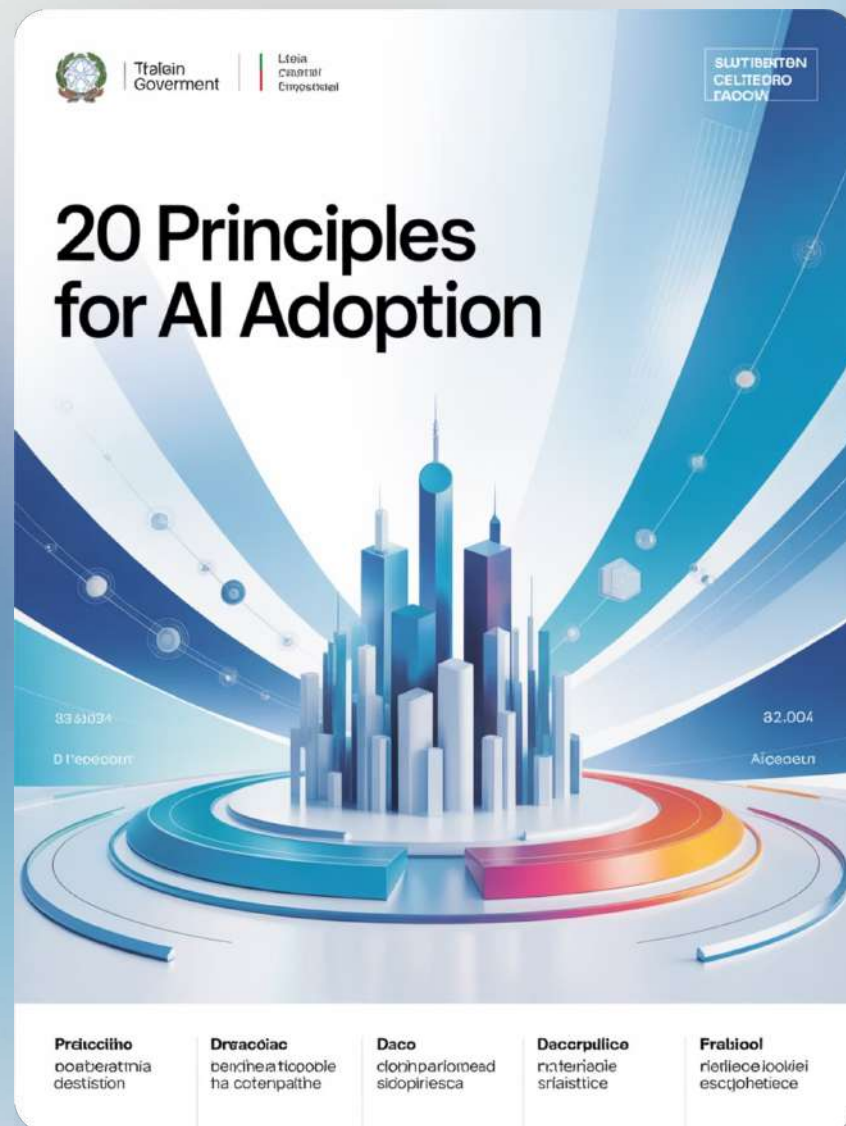
L'IA deve contribuire a rendere i servizi pubblici più efficaci, efficienti e tempestivi, personalizzandoli in base alle esigenze dell'utente e introducendo meccanismi di proattività.

 **Aumentare le capacità predittive**

L'utilizzo dell'IA mira a migliorare i processi decisionali, rendendoli più informati e basati sui dati, attraverso l'analisi predittiva.

 **Promuovere l'innovazione**

L'adozione dell'IA è vista come un motore per l'innovazione continua sia nei servizi pubblici offerti che nei processi amministrativi interni.



Principi Guida per l'Adozione dell'IA

Per raggiungere questi obiettivi, le Linee Guida delineano 20 principi guida, raggruppati in diverse aree tematiche:

Conformità e Governance



1 Conformità normativa

Le PA devono adottare sistemi di IA nel pieno rispetto delle normative nazionali ed europee, tra cui l'AI Act, il GDPR e la Direttiva NIS2, monitorando costantemente l'evoluzione legislativa per garantire la conformità.

2 Rispetto dei valori fondamentali dell'UE

L'adozione dell'IA deve sempre garantire il rispetto dei principi definiti dalla Carta dei diritti fondamentali dell'Unione Europea.

3 Gestione del rischio

Le PA sono tenute ad adottare politiche adeguate di gestione del rischio, analizzando a fondo i rischi associati all'IA per prevenire violazioni dei diritti fondamentali o altri danni.

4 Protezione dei dati personali

L'utilizzo dei sistemi di IA deve avvenire nel rispetto delle norme unionali e nazionali sulla protezione dei dati personali, assicurando elevati standard di qualità e integrità dei dati.

Etica e Inclusione



Responsabilità

L'IA è concepita come uno strumento di supporto all'attività umana, e la responsabilità ultima delle decisioni prese con il supporto dei sistemi di IA rimane sempre in capo all'essere umano. È essenziale identificare chiaramente le responsabilità di tutti gli attori coinvolti nel ciclo di vita dei sistemi di IA.



Accessibilità, inclusività, non discriminazione

Le PA devono garantire un trattamento equo per tutti i soggetti e gruppi, promuovendo parità di accesso, uguaglianza di genere e diversità culturale. Devono essere adottate misure preventive per evitare la riproduzione o l'amplificazione di bias sociali.



Trasparenza

I sistemi di IA adottati dalle PA devono garantire la trasparenza e la comprensibilità delle loro decisioni e del loro funzionamento. È fondamentale assicurare un'adeguata spiegabilità dei risultati, rendendo comprensibili le motivazioni delle decisioni e delle azioni intraprese dai sistemi di IA.



Informazione

Le PA devono informare gli utenti sull'interazione con sistemi di IA, rendendoli consapevoli delle capacità e dei limiti di tali sistemi.

Qualità e Affidabilità dei Sistemi di IA

I principi da P.9 a P.15 si concentrano sulla qualità tecnica e l'affidabilità dei sistemi di IA implementati nella Pubblica Amministrazione:



Qualità dei dati

Le PA devono adottare sistemi di IA garantendo una gestione etica, trasparente e conforme dei dati. Ciò implica l'utilizzo di dati di alta qualità, affidabili e aggiornati, e la definizione di politiche chiare per l'accesso, l'uso e la conservazione dei dati.



Affidabilità

È necessario garantire che i risultati e le decisioni prodotte dai sistemi di IA siano affidabili e coerenti con gli obiettivi prefissati, attraverso un monitoraggio continuo delle prestazioni.



Robustezza

Le PA devono assicurare la robustezza dei sistemi di IA, garantendo che operino correttamente anche in condizioni avverse o in presenza di guasti.



Sicurezza cibernetica

La sicurezza cibernetica dei sistemi di IA è cruciale per prevenire tentativi di alterazione, compromissione o uso illecito da parte di terzi. Le PA devono adottare misure di protezione adeguate.



Supervisione umana

Le PA devono garantire un livello adeguato di supervisione umana dei sistemi di IA, assicurando che siano progettati e implementati in modo da consentirne la verifica, la correzione o la sostituzione da parte di personale umano.



Registrazioni (logging)

I sistemi di IA devono essere dotati di adeguati meccanismi di registrazione per tracciare e conservare nel tempo le operazioni svolte, garantendo la tracciabilità.



Adozione di standard tecnici

Le PA devono considerare le norme tecniche nazionali, europee e internazionali per garantire interoperabilità, manutenibilità, sicurezza e conformità dei sistemi di IA.

Innovazione e Sostenibilità

Efficienza e qualità dei servizi

Le PA adottano l'IA per incrementare l'efficienza operativa e migliorare la qualità dei servizi per cittadini e imprese, automatizzando compiti ripetitivi e implementando soluzioni innovative e proattive.



Innovazione e miglioramento continuo

È promosso un approccio all'IA orientato all'innovazione e al miglioramento continuo, che include la collaborazione con altre PA, enti di ricerca, università e imprese per sperimentare e integrare soluzioni basate sull'IA.

Sostenibilità ambientale

Le PA devono adottare sistemi di IA secondo un approccio sostenibile, attento alla tutela ambientale e in linea con i principi di sostenibilità energetica.

Formazione e Organizzazione



Formazione e sviluppo delle competenze

Le PA devono investire nella formazione del proprio personale per garantire le competenze necessarie a utilizzare, gestire e sviluppare sistemi di IA in modo efficace e responsabile. È altresì promossa l'alfabetizzazione digitale per cittadini e imprese.

- Formazione tecnica per il personale IT
- Competenze di base per tutti i dipendenti
- Programmi di alfabetizzazione digitale per cittadini
- Collaborazione con università e centri di ricerca

Rafforzamento Organizzativo e Approccio Human-in-the-Loop

Rafforzamento dell'organizzazione e delle infrastrutture

Nell'adozione di sistemi di IA, le PA devono ottimizzare il proprio assetto organizzativo e le infrastrutture tecnologiche per agevolare la trasformazione digitale e migliorare i livelli di sicurezza e resilienza.

È fondamentale sottolineare che per i sistemi di IA classificati ad alto rischio, questi principi sono rafforzati da requisiti specifici definiti dall'AI Act.

Approccio "Human-in-the-Loop"

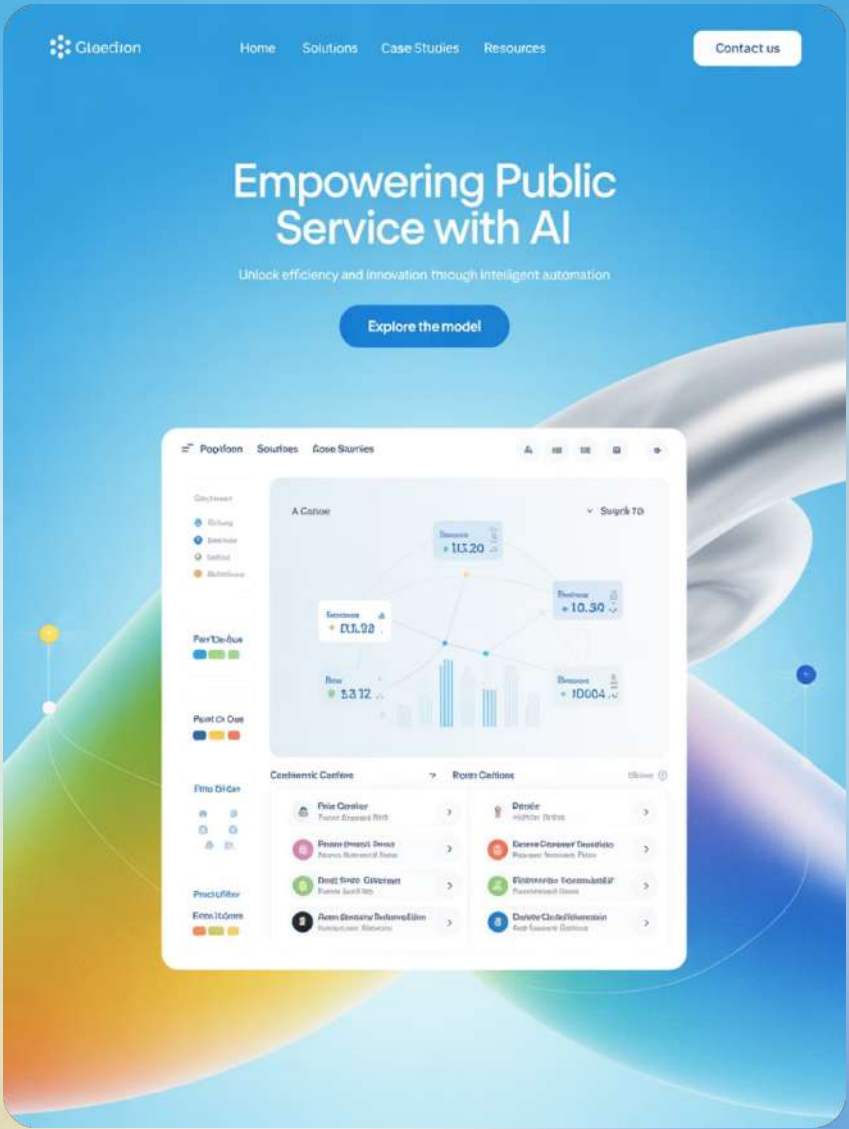
L'approccio "Human-in-the-Loop" emerge come un pilastro etico e operativo centrale. Il Principio P.5 sulla "Responsabilità" stabilisce esplicitamente che l'IA è un "strumento di supporto all'attività umana, mantenendo la responsabilità ultima delle decisioni prese dai sistemi di IA". Questo concetto è ulteriormente rafforzato dal Principio P.13 ("Supervisione umana") e dagli obblighi previsti dall'AI Act e dall'Articolo 22 del GDPR, che impongono il "diritto a un intervento umano su decisioni automatizzate".

Questa impostazione indica che la normativa e le linee guida non mirano a una completa automazione decisionale nella PA. Al contrario, enfatizzano la necessità di mantenere un controllo umano significativo, specialmente per le decisioni che possono avere un impatto sui diritti fondamentali dei cittadini. Ciò richiede la progettazione di sistemi IA che siano interpretabili, modificabili e, se necessario, reversibili, oltre alla formazione del personale per esercitare questa supervisione in modo efficace, trovando un equilibrio tra l'efficienza algoritmica e la garanzia dei diritti individuali.

Qualità dei Dati come Fattore Critico

Un altro aspetto critico è la qualità dei dati, riconosciuta come fattore determinante per il successo e la conformità. Il Principio P.9 ("Qualità dei dati") richiede esplicitamente "dati di alta qualità, affidabili e aggiornati". Questa esigenza è ulteriormente rafforzata dall'Articolo 10 dell'AI Act, che "esplicitamente manda l'uso di dataset di alta qualità per l'addestramento, la validazione e il test dei sistemi di IA ad alto rischio. La quantità dei dati è altresì cruciale per l'accuratezza dei modelli. Questo implica che la disponibilità e la qualità dei dati non sono solo requisiti tecnici per l'efficacia dell'IA, ma un imperativo legale ed etico. Dati di scarsa qualità o viziati da bias possono portare a decisioni discriminatorie o errate, con gravi conseguenze legali e sociali. Le PA devono quindi investire in modo significativo nella governance, nella pulizia, nell'arricchimento e nella validazione dei propri dataset, considerandoli infrastrutture strategiche per lo sviluppo e l'adozione dell'IA.

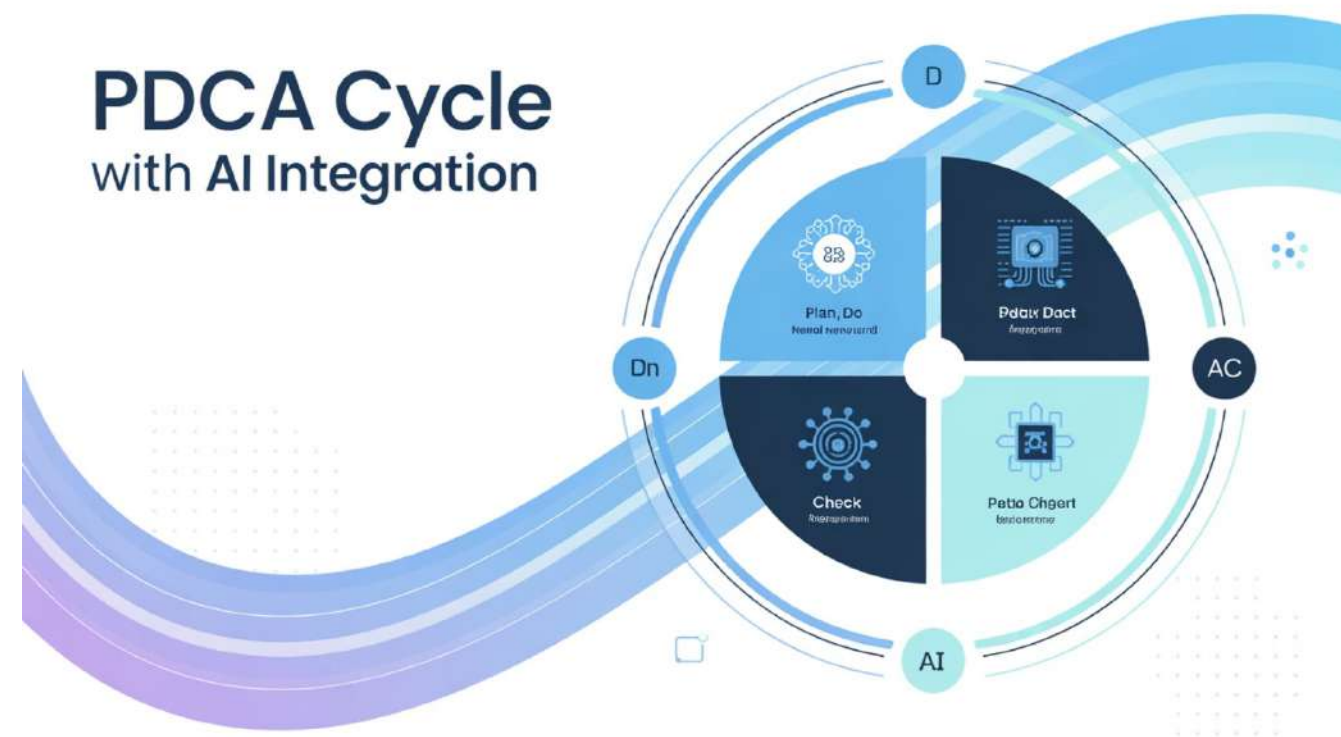
MODELLO DI ADOZIONE DELL'AI



Introduzione al Modello di Adozione

Il Capitolo 4 delle Linee Guida AGID introduce un modello strutturato per l'adozione dell'IA da parte delle Pubbliche Amministrazioni, basato sul ciclo di miglioramento continuo **Plan-Do-Check-Act (PDCA)** e sulle pratiche gestionali dello standard ISO/IEC 42001:2023.

Questo modello è proposto come un approccio sistematico che le PA DOVREBBERO adottare, adattandolo alle proprie specificità e al ruolo ricoperto (fornitore o deployer di sistemi di IA). Per i sistemi a rischio limitato, minimo o nullo, le fasi possono essere accorpate per adeguarsi alla minore complessità.



L'adozione di un approccio interattivo e basato sul rischio emerge come il modello operativo standard.

Il modello di adozione dell'IA è esplicitamente basato sul ciclo PDCA e sullo standard ISO/IEC 42001:2023. Le fasi di "Gestione del rischio" (4.7), "Valutazione d'impatto" (4.8), "Monitoraggio e valutazione" (4.12) e "Miglioramento continuo" (4.13) sono integrate e interconnesse, con una forte enfasi sulla classificazione del rischio secondo l'AI Act. Questo indica che le PA sono chiamate ad abbandonare un approccio lineare e ad adottare un modello operativo dinamico e ciclico per l'IA. La valutazione dei rischi e degli impatti non è un'attività una tantum, ma un processo continuo che si adatta all'evoluzione del sistema IA e del contesto. L'allocazione di risorse e la pianificazione operativa devono riflettere questa natura ciclica e basata sul rischio, richiedendo flessibilità e capacità di adattamento costanti.

Strategia per l'IA



Sviluppo della Strategia

Le PA DEVONO sviluppare una strategia per l'IA che sia coerente con il proprio contesto e allineata alla propria missione istituzionale.



Coerenza con i Piani Esistenti

La strategia DEVE essere coerente con il Piano Integrato di Attività e Organizzazione (PIAO), la strategia sui dati e il Piano Triennale per l'informatica nella PA.



Definizione degli Obiettivi

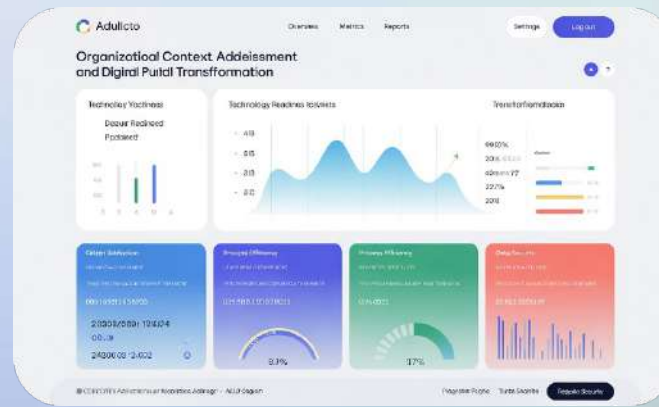
Questa strategia DEVE definire gli obiettivi dell'utilizzo dell'IA e le azioni concrete per conseguirli, promuovendo un approccio condiviso e collaborativo all'interno dell'ente.



Coordinamento

Il coordinamento di questa strategia DEVE essere affidato al Responsabile per la Transizione al Digitale (RTD) e al suo ufficio (UTD), con il coinvolgimento del Responsabile della Protezione dei Dati (RPD).

Le azioni chiave includono il miglioramento della qualità dei dati, l'incremento delle competenze del personale, l'individuazione di casi d'uso benefici, la valutazione di esperienze pregresse, l'avvio di sperimentazioni (anche in collaborazione con altre PA) e la promozione di sinergie.



Analisi del Contesto e delle Caratteristiche della PA



Fattori Esterni

Requisiti normativi derivanti da CAD, AI Act, DGA, GDPR, NIS2 e aspettative degli stakeholder esterni



Fattori Interni

Struttura organizzativa, stakeholder interni, ambiti operativi, contesto territoriale, capacità tecnologiche



Obiettivo dell'Analisi

Definire una strategia e un modello di adozione adeguati

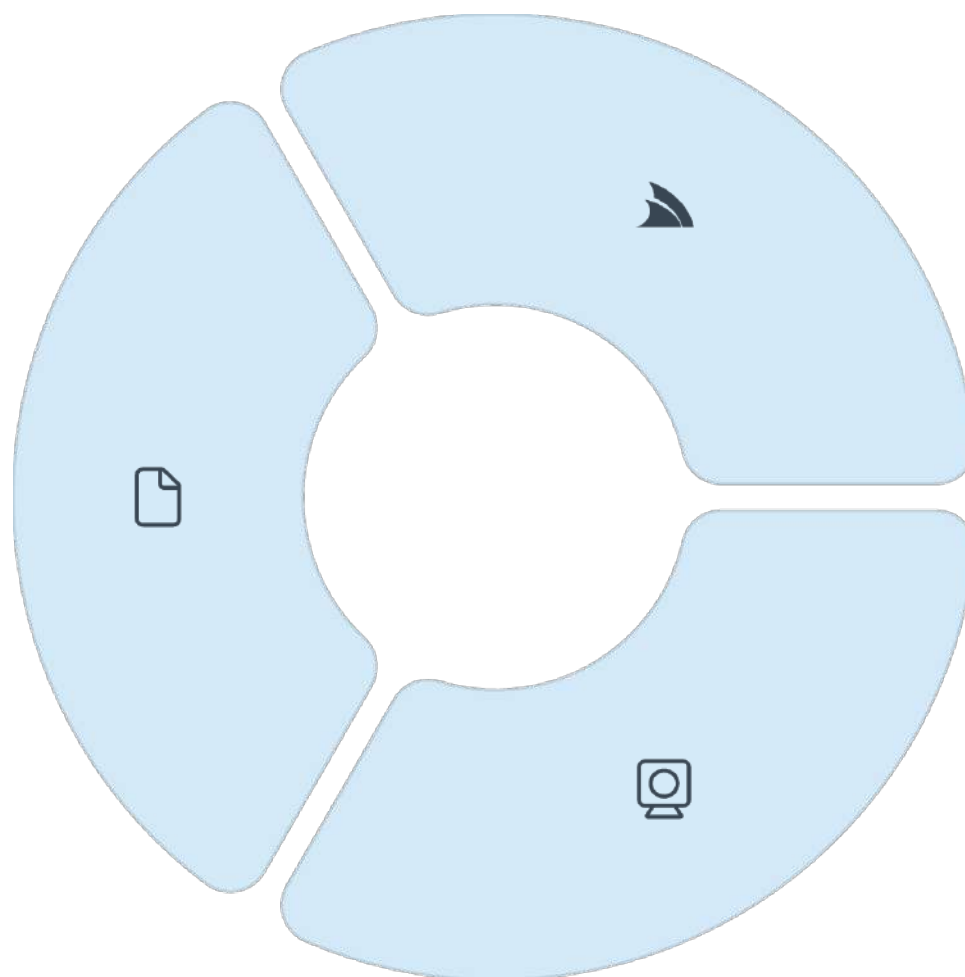
Le PA DEVONO condurre un'analisi approfondita dei fattori esterni e interni che possono influenzare la capacità dell'ente di raggiungere i risultati attesi dall'uso dell'IA. L'Allegato A fornisce uno strumento pratico per determinare il livello di maturità organizzativa e tecnologica delle PA in relazione all'IA.

Obiettivi e ambiti prioritari di applicazione

Le PA DEVONO identificare preliminarmente gli obiettivi e gli ambiti prioritari per l'adozione dell'IA, basandosi sull'analisi del proprio contesto. È comunque possibile condurre sperimentazioni in ambiti non prioritari e a minor rischio.

Miglioramento dell'efficienza operativa

- Supporto alle decisioni
- Ottimizzazione dell'allocazione delle risorse
- Miglioramento della gestione documentale
- Supporto giuridico e procedure di acquisto



Miglioramento dei servizi ai cittadini e alle imprese

- Personalizzazione
- Proattività
- Trasparenza
- Accessibilità
- Inclusione

Sicurezza e protezione dei dati

Garantire la sicurezza delle informazioni e la protezione dei dati personali nell'implementazione dei sistemi di IA

Norme Tecniche

Le PA DEVONO considerare le norme tecniche nazionali, europee e internazionali nell'acquisizione, sviluppo e adozione dei sistemi di IA. L'AI Act, in particolare, definisce i requisiti per i sistemi di IA ad alto rischio.

L'Allegato E fornisce un elenco delle principali norme tecniche sull'IA da considerare.



Norme Nazionali

1

Standard e linee guida sviluppate a livello nazionale per l'implementazione dell'IA nella pubblica amministrazione

2

Norme Europee

Regolamenti e direttive dell'Unione Europea, con particolare riferimento all'AI Act e ai suoi requisiti per i sistemi ad alto rischio

3

Norme Internazionali

Standard ISO/IEC e altre norme tecniche internazionali relative all'implementazione e gestione dei sistemi di IA

Casi d'Uso

Il modello di adozione dell'IA prevede che le PA individuino i casi d'uso che offrono il massimo beneficio, basandosi sulla propria strategia IA, sull'analisi del contesto e sulle caratteristiche dell'organizzazione. Le PA DEVONO raccogliere, documentare e aggiornare le informazioni fondamentali sui casi d'uso e sulle soluzioni IA che li implementano, per l'intero ciclo di vita.

L'Allegato F fornisce un modello di documentazione di un caso d'uso. Le PA DEVONO trasmettere periodicamente all'AgID un estratto della documentazione descrittiva dei casi d'uso.

4.5.1. Funzionalità dell'IA

A partire dai casi d'uso, le PA definiscono le funzionalità dei sistemi di IA che li implementano. L'Allegato G riporta una classificazione non esaustiva delle funzionalità dei sistemi di IA.

4.5.2. Requisiti

Nelle fasi di sviluppo e gestione dei sistemi di IA, le PA DEVONO identificare i requisiti (normativi, tecnici, etici e operativi) tenendo conto delle aspettative delle parti interessate. Oltre ai Principi delle Linee Guida, le PA DEVONO considerare requisiti di conformità all'AI Act, gestione e qualità dei dati, protezione dei dati personali e sicurezza cibernetica.

4.5.3. Indicatori di prestazione

Le PA DEVONO definire, per ciascun caso d'uso, indicatori chiave di prestazione (KPI) per misurare l'efficacia del sistema di IA nel raggiungere gli obiettivi. I KPI DEVONO essere monitorati durante il ciclo di vita del caso d'uso.

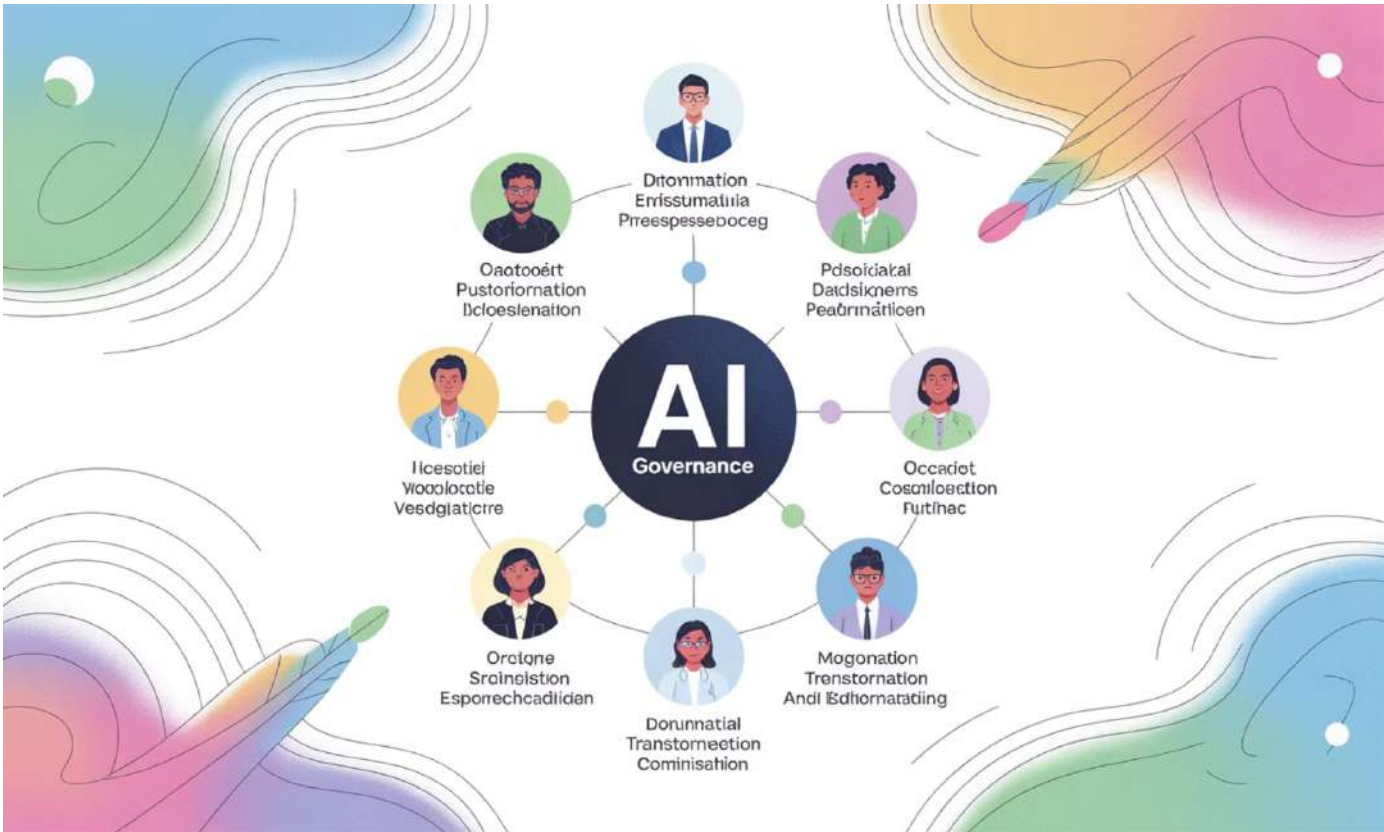
L'Allegato I fornisce uno strumento operativo per l'individuazione dei KPI e riguardano: prestazioni del modello; qualità dei dati; robustezza e affidabilità; efficienza computazionale; usabilità e accessibilità; impatto etico e conformità normativa; costo e sostenibilità.

Governance

Gli organi direttivi della PA sono responsabili dell'approvazione della strategia per l'IA dell'ente.

La responsabilità della gestione dell'IA DEVE essere affidata al RTD e al suo ufficio (UTD), e gli organi direttivi DEVONO garantire questa assegnazione e comunicarla internamente.

Le PA DOVREBBERO definire procedure di governance per lo sviluppo e l'utilizzo dei sistemi di IA, coerenti con la strategia IA e il PIAO.



Procedure di Governance

L'Allegato H fornisce un elenco di possibili procedure di governance che le PA possono implementare per gestire efficacemente i sistemi di IA.



Codice Etico

Le PA DEVONO adottare un codice etico per l'IA, che diventi uno strumento di governance vincolante, allineato al quadro normativo e integrato nei processi decisionali e operativi.

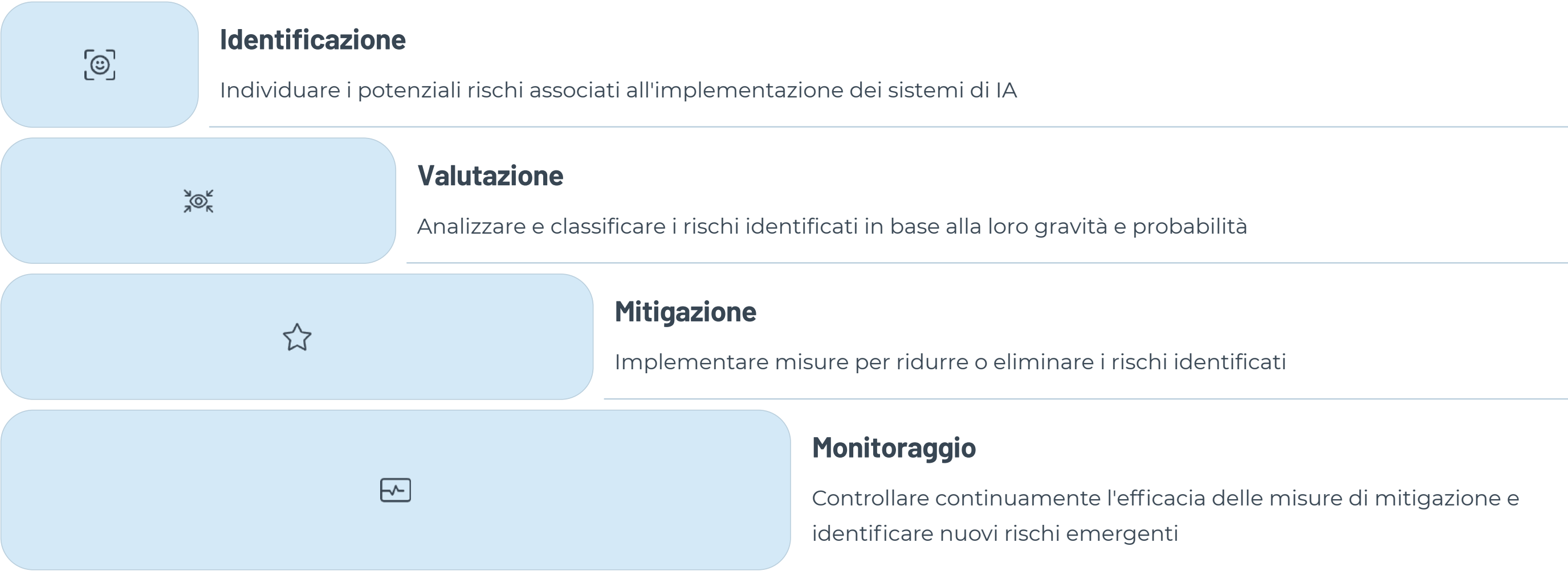


Responsabilità

Il Responsabile per la Transizione al Digitale (RTD) e il suo ufficio (UTD) devono assumere la responsabilità della gestione dell'IA all'interno dell'organizzazione.

Gestione del Rischio

Le PA DEVONO adottare un approccio alla gestione del rischio conforme all'AI Act, che definisce requisiti rigorosi per l'identificazione, valutazione e mitigazione dei rischi associati ai sistemi di IA "ad alto rischio".



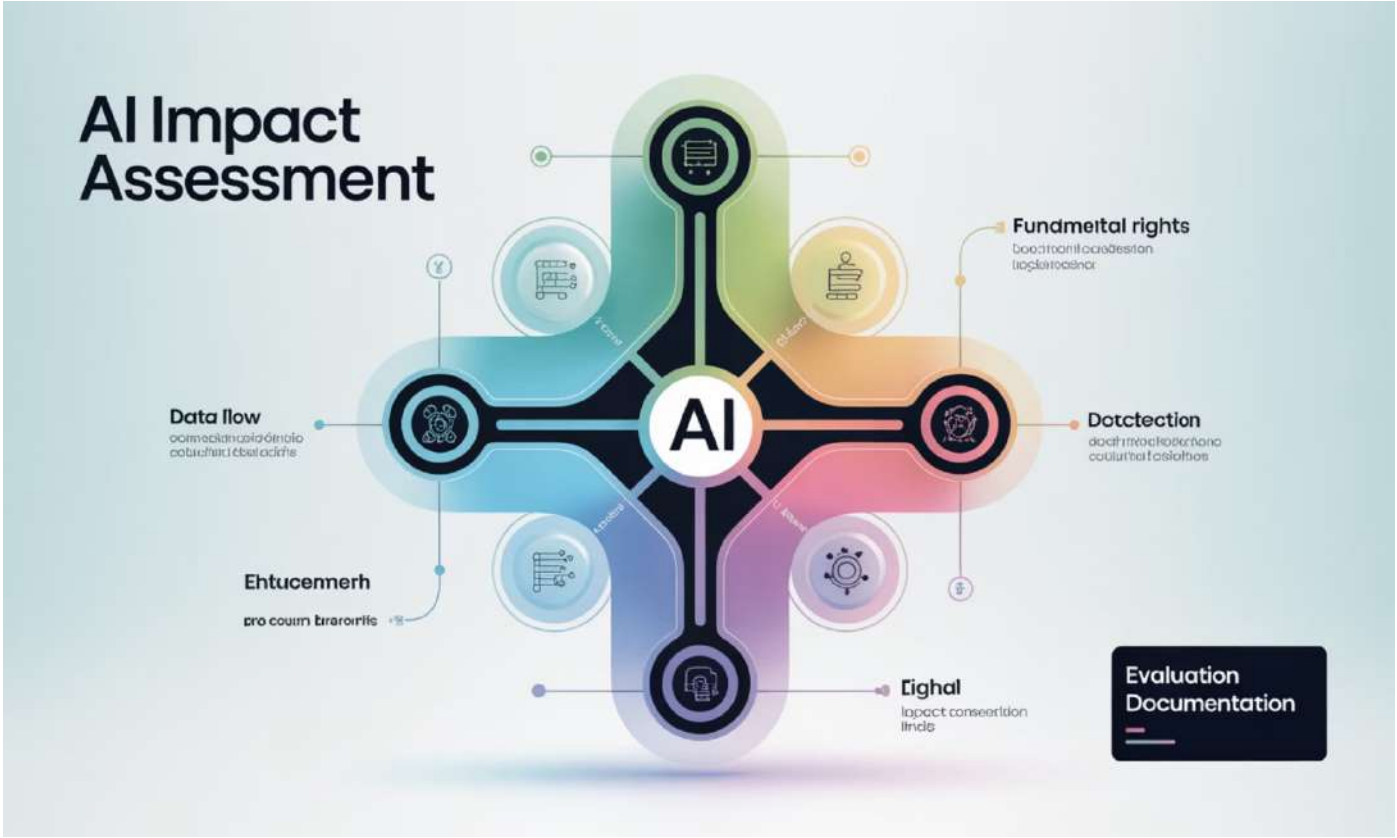
In attesa delle norme tecniche armonizzate, le PA PUÒ fare riferimento a standard come UNI ISO 31000 e ISO/IEC 23894. L'Allegato B propone uno strumento operativo per la gestione del rischio per i sistemi IA "ad alto rischio".

Valutazione d'Impatto

L'AI Act definisce requisiti rigorosi per la valutazione d'impatto dei sistemi IA "ad alto rischio", che DEVE includere la valutazione d'impatto sui diritti fondamentali (FRIA) e la valutazione d'impatto sulla protezione dei dati personali (DPIA).

I risultati di queste valutazioni DEVONO essere documentati e condivisi. Le PA DOVREBBERO definire un processo per valutare le potenziali conseguenze sui diritti fondamentali anche per i sistemi IA di "rischio minimo o nessun rischio", pur mantenendo la necessità della DPIA.

- **FRIA**
Valutazione d'impatto sui diritti fondamentali
- **DPIA**
Valutazione d'impatto sulla protezione dei dati personali
- **Documentazione**
Registrazione e condivisione dei risultati delle valutazioni
- **AIIA**
L'Allegato C fornisce uno strumento di supporto per le PA per effettuare la valutazione d'impatto (AIIA)



Piano Operativo

1 Definizione degli Obiettivi

Le PA DEVONO definire obiettivi operativi chiari per l'adozione e l'uso dell'IA, assicurandone la coerenza con la strategia IA e il rispetto dei requisiti normativi.

2 Misurazione e Monitoraggio

Gli obiettivi DEVONO essere misurabili, monitorati e aggiornati regolarmente per garantire il loro raggiungimento.

3 Approccio di Project Management

Per il raggiungimento degli obiettivi, la PA DEVE adottare un approccio sistematico e documentato di project management, definendo un piano operativo che includa attività, risorse, tempi, responsabilità e criteri di valutazione.

Il piano operativo rappresenta la traduzione concreta della strategia IA in azioni specifiche, con una chiara definizione delle responsabilità e delle tempistiche per ciascuna attività prevista.

TEMPLATE

MID TERM

ONE
dolor sit amet,
adipiscing elit



MILESTONE
Lorem ipsum dolor sit amet,
consectetur adipiscing elit



MILESTONE
Lorem ipsum dolor sit amet,
consectetur adipiscing elit



MILESTONE
Lorem ipsum dolor sit
consectetur adipiscing



E
it amet,
elit



MILESTONE
Lorem ipsum dolor sit amet,
consectetur adipiscing elit



MILESTONE
Lorem ipsum dolor sit amet,
consectetur adipiscing elit



MILESTONE
Lorem ipsum dolor sit an
consectetur adipiscing eli

Risorse, Competenze, Comunicazione



Allocazione delle Risorse

Le PA DEVONO determinare e allocare risorse finanziarie, tecnologiche e umane adeguate per sviluppare, mantenere e migliorare i sistemi di IA.

Sviluppo delle Competenze

Le PA DEVONO determinare le competenze necessarie per il personale coinvolto nei sistemi di IA e garantirne l'acquisizione tramite formazione, istruzione o esperienza, documentando le competenze acquisite.

Promozione dell'Uso Responsabile

Le PA DEVONO promuovere un uso responsabile ed efficace dell'IA, assicurando che il personale sia consapevole dei principi, obiettivi, strategia IA e codice etico.

Le PA DEVONO definire il piano di comunicazione interno ed esterno relativo ai sistemi di IA. Le PA DEVONO documentare e conservare le informazioni necessarie per assicurare conformità normativa, trasparenza e tracciabilità dei sistemi di IA, applicando le Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Implementazione

In questa fase, le PA DEVONO attuare il piano operativo definito nella fase di pianificazione.

Le PA DEVONO condurre, a intervalli pianificati o in caso di modifiche significative, la valutazione dei rischi legati all'IA e mantenere una documentazione adeguata sui risultati. Analogamente, le PA DEVONO condurre la valutazione dell'impatto del sistema di IA e mantenere una documentazione adeguata.



Attuazione del Piano

Implementazione delle attività definite nel piano operativo secondo le tempistiche stabilite

1

Valutazione dell'Impatto

Esecuzione della valutazione dell'impatto del sistema di IA e mantenimento di una documentazione adeguata

3

Valutazione dei Rischi

Conduzione periodica della valutazione dei rischi legati all'IA e documentazione dei risultati

2

Documentazione

Registrazione di tutte le attività svolte e dei risultati ottenuti per garantire trasparenza e tracciabilità

4

Monitoraggio, valutazione e miglioramento continuo

Monitoraggio e Valutazione

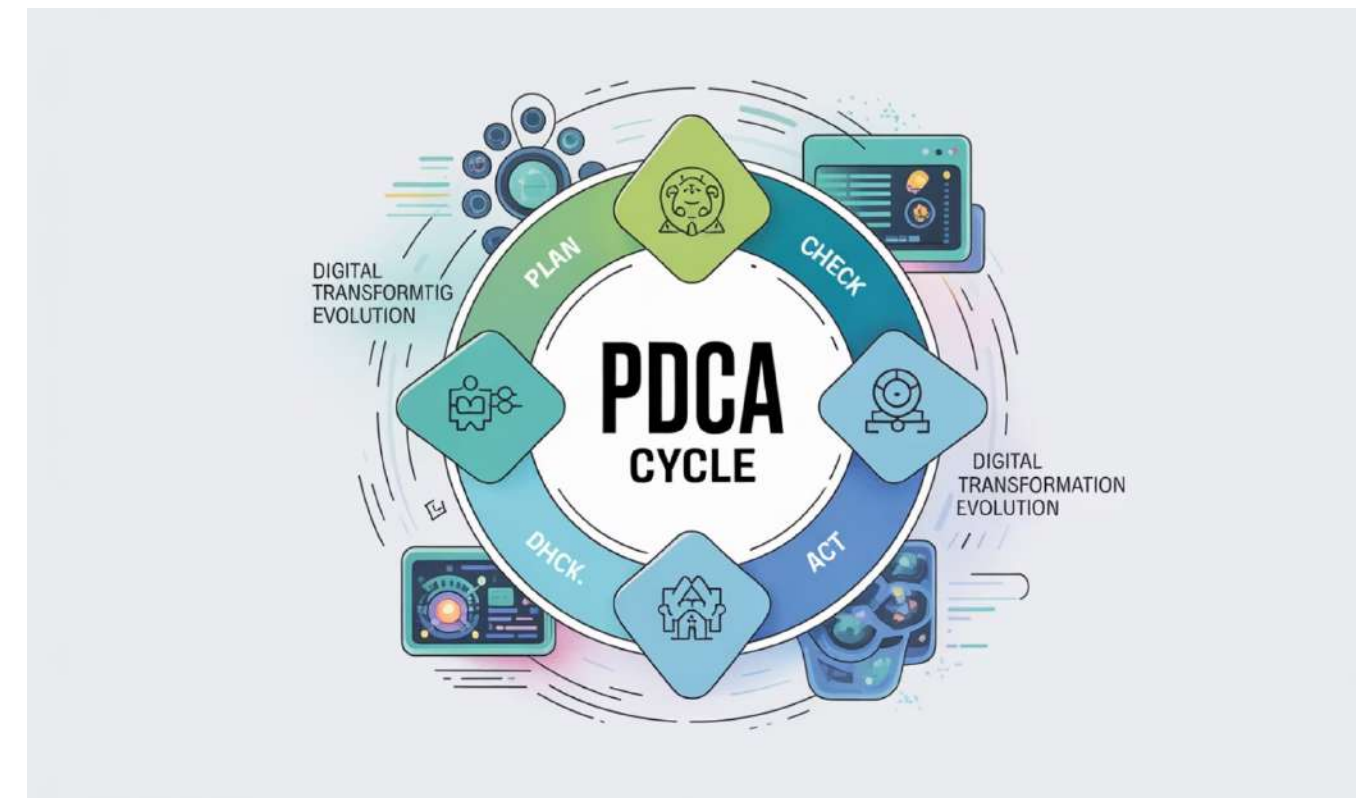
Le PA DEVONO definire e monitorare regolarmente i KPI per misurare:

- misurare l'efficacia delle misure organizzative e tecniche
- le prestazioni tecniche dei sistemi di IA
- l'impatto sui processi interni e sui diritti fondamentali
- Il valore aggiunto per la PA.

I risultati del monitoraggio DEVONO essere conservati.

Miglioramento Continuo

Le PA DEVONO garantire nel tempo l'idoneità, l'adeguatezza e l'efficacia dei sistemi di IA adottati e delle misure tecniche e organizzative per la gestione dell'IA tramite un processo di "miglioramento continuo".





Ruoli e responsabilità chiave nella Governance dell'IA nella PA

Organi Direttivi della PA



Gli **organi direttivi della Pubblica Amministrazione** rappresentano il **vertice decisionale nell'implementazione dell'Intelligenza Artificiale** all'interno dell'ente.

Responsabilità Principali nell'IA

- Approvazione della strategia per l'IA dell'ente
- Garanzia dell'assegnazione delle responsabilità IA al RTD
- Supervisione dell'implementazione complessiva
- Allocazione delle risorse necessarie

Riferimento nelle Linee Guida

4.6 Governance

La sezione stabilisce il ruolo fondamentale degli organi direttivi nel garantire una governance efficace dell'IA, attraverso l'approvazione formale delle strategie e l'assegnazione chiara delle responsabilità.

Ruoli Chiave nella Governance dell'IA

Ruolo	Responsabilità Principali nell'IA	Riferimento nelle Linee Guida
Responsabile per la Transizione al Digitale (RTD)	Coordinamento e responsabilità della strategia IA; assicurare la conformità dei sistemi IA alle Linee Guida; riferire agli organi direttivi sulle prestazioni e attività di controllo; affidatario della sorveglianza umana per i sistemi IA ad alto rischio.	4.1 Strategia per l'IA, 4.6 Governance, 5.2 Misure di sorveglianza
Ufficio per la Transizione al Digitale (UTD)	Supporto al RTD nella gestione e coordinamento dell'IA; partecipazione a percorsi tecnico-specialistici.	4.1 Strategia per l'IA, 4.6 Governance, 5.2 Misure di sorveglianza, 8.1 Indicazioni operative
Responsabile della Protezione dei Dati (RPD)	Coinvolgimento nella definizione della strategia IA; garanzia del rispetto delle norme sulla protezione dei dati personali; conduzione della DPIA.	4.1 Strategia per l'IA, 10. Protezione dei dati personali

La centralità del Responsabile per la Transizione al Digitale

La centralità del Responsabile per la Transizione al Digitale (RTD) nella governance dell'IA è un elemento distintivo di questo modello.

Le sezioni 4.1 sulla "Strategia per l'IA" e 4.6 sulla "Governance" assegnano esplicitamente al RTD e al suo Ufficio (UTD) il coordinamento e la responsabilità della gestione dell'IA, inclusa la conformità alle Linee Guida.

L'analisi degli impatti di precedenti linee guida AgID ha dimostrato che la nomina del RTD *"ha sicuramente contribuito a semplificare il rapporto del cittadino e dell'impresa con la P.A. velocizzando i processi e la standardizzazione delle procedure"*.



Questo posiziona il **RTD come la figura chiave** per l'implementazione dell'IA nella PA, non solo a livello tecnico ma anche strategico e di governance. Ciò richiede che il RTD possieda non solo competenze digitali, ma anche una profonda comprensione delle implicazioni legali, etiche e organizzative dell'IA. La sua efficacia è cruciale per la trasformazione digitale complessiva della PA, fungendo da ponte tra la visione strategica e l'implementazione operativa.

Personale coinvolto nei sistemi IA



Responsabilità Principali

- Acquisizione delle competenze necessarie
- Consapevolezza dei principi, obiettivi e codice etico
- Partecipazione a programmi formativi

Riferimento nelle Linee Guida

- 4.10 Risorse, competenze, comunicazione
- 8. Formazione e sviluppo delle competenze

Formazione Base

Acquisizione delle conoscenze fondamentali sui sistemi di IA e sul loro impatto nei processi della PA.

Specializzazione

Sviluppo di competenze specifiche in base al ruolo ricoperto nell'implementazione e utilizzo dei sistemi IA.

Aggiornamento Continuo

Partecipazione a programmi di formazione continua per mantenersi al passo con l'evoluzione delle tecnologie IA.

Conformità delle Soluzioni di IA

Il Capitolo 5 delle Linee Guida AGID si concentra sulla conformità delle soluzioni di Intelligenza Artificiale, sottolineando l'imperativo per le Pubbliche Amministrazioni di operare nel pieno rispetto della normativa nazionale ed europea, con particolare riferimento all'AI Act. Le PA DEVONO fare riferimento alla definizione di "sistema di IA" contenuta nell'articolo 3, n. 1) dell'AI Act per determinare se una tecnologia rientra nell'ambito di applicazione del regolamento.

Successivamente, è essenziale procedere alla classificazione del sistema di IA, stabilendone il livello di rischio (inaccettabile, alto, limitato, minimo o nullo).

È altresì fondamentale che le PA riconoscano chiaramente il ruolo che ricoprono nel ciclo di vita dell'IA, sia come fornitori (ad esempio, erogando sistemi di IA tramite servizi cloud ad altri soggetti o sviluppando soluzioni per il riuso) sia come deployer (utilizzatori finali).

Monitoraggio del ciclo di vita delle soluzioni di IA



Monitoraggio Continuo

Le PA, sia che agiscano come fornitori sia come deployer, DEVONO monitorare i propri sistemi di IA e il relativo impatto sui diritti fondamentali per tutto il ciclo di vita del sistema. Il tipo di monitoraggio richiesto dipende dal livello di rischio del sistema.



Conformità dei Dati

Per tutti i sistemi di IA, inclusi quelli a rischio limitato o minimo, le PA DEVONO verificare che i dati siano trattati in conformità alle normative e garantire la presenza e l'eshaustività della documentazione tecnica, che DEVE essere costantemente aggiornata.



Valutazione d'Impatto

Per i sistemi di IA ad alto rischio, le PA che agiscono come deployer DEVONO effettuare una valutazione dell'impatto sui diritti fondamentali (FRIA) prima dell'utilizzo, considerando processi, periodo e frequenza d'uso, categorie di persone interessate, dati trattati, rischi specifici e misure di sorveglianza umana.



Documentazione Tecnica

Se una PA è fornitore di sistemi di IA ad alto rischio, DEVE documentare il sistema di monitoraggio post-immissione sul mercato, monitorare il sistema di gestione dei rischi, mettere a disposizione informazioni comprensibili e assicurare la registrazione automatica degli eventi rilevanti e la conservazione della documentazione tecnica.

5.2. Misure di sorveglianza

Le PA DEVONO adempiere agli obblighi riguardanti le misure di supervisione umana dei sistemi IA ad alto rischio, come previsto dall'articolo 14 dell'AI Act, in funzione del proprio ruolo.

La PA fornitore DEVE progettare e sviluppare i sistemi di IA in modo da garantire un'efficace supervisione umana.

La PA deployer, d'altra parte, DEVE adottare procedure e strumenti per assicurare il monitoraggio, l'interpretazione e l'intervento umano sulle decisioni generate dall'IA.



Human-On-The-Loop

Intervento sui parametri durante il funzionamento del sistema



Human-In-The-Loop

Capacità di influenzare l'output del sistema



Human-In-Command

Determinazione dell'uso nei processi decisionali

La responsabilità della sorveglianza umana è affidata al RTD e al suo Ufficio (UTD), assicurando che il personale incaricato possieda le competenze necessarie.

Auditing e controlli nei confronti dei fornitori esterni

Verifica Preliminare

Le PA che si avvalgono di un sistema IA prodotto esternamente (come deployer) DEVONO verificare preliminarmente il rispetto delle norme previste dall'AI Act per i fornitori, a seconda del rischio del sistema.

Controllo Sistemi ad Alto Rischio

Per i sistemi di IA ad alto rischio, le PA deployer DEVONO verificare la conformità dei sistemi ai requisiti dell'AI Act e chiedere ai fornitori di dimostrare e garantire, anche tramite certificazioni, i requisiti previsti dall'articolo 16 dell'AI Act (ad esempio, conformità ai requisiti della sezione II, esistenza di un sistema di gestione della qualità, espletamento della valutazione di conformità, redazione della documentazione pertinente, istituzione di un sistema di monitoraggio post-immissione sul mercato).

Verifica Modelli Generali

Le PA DEVONO inoltre verificare che i fornitori di modelli di IA per finalità generali con rischi sistemici abbiano assolto agli obblighi previsti dall'articolo 53 dell'AI Act, inclusa la documentazione relativa a test e verifiche condotte da soggetti esterni.

La sezione 5.3 ("Auditing e controlli nei confronti dei fornitori esterni") impone alle PA deployer di "verificare preliminarmente il rispetto delle norme previste dall'AI Act per i fornitori" e di "chiedere ai fornitori di dimostrare e garantire, anche tramite certificazioni, i requisiti previsti". Questo concetto è ulteriormente rafforzato dal fatto che "Le PA titolari dei dati, anche se l'IA è fornita da terzi. Questo significa che resta in capo all'ente pubblico la responsabilità di garantire il rispetto dei diritti dei cittadini e la sicurezza dei dati trattati".

Conservazione della documentazione e responsabilità

Le PA DEVONO garantire la corretta conservazione della documentazione relativa all'impiego dei sistemi di IA ad alto rischio, in conformità con la normativa italiana ed europea sulla gestione documentale. Ciò include la conservazione dei dati e metadati necessari per assicurare la tracciabilità dei processi decisionali automatizzati, nel rispetto della normativa sulla protezione dei dati personali. L'AI Act stabilisce l'obbligo di conservare la documentazione tecnica sui sistemi di IA ad alto rischio per un periodo congruo, al fine di garantire audit e verifiche.

Le PA DEVONO gestire e conservare la documentazione dei sistemi di IA secondo le disposizioni del CAD e le linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

La non-delegabilità della responsabilità della PA, anche in presenza di fornitori esterni, è un principio cardine.

ETHICAL AI
GOVERNANCE

Digital
ethics

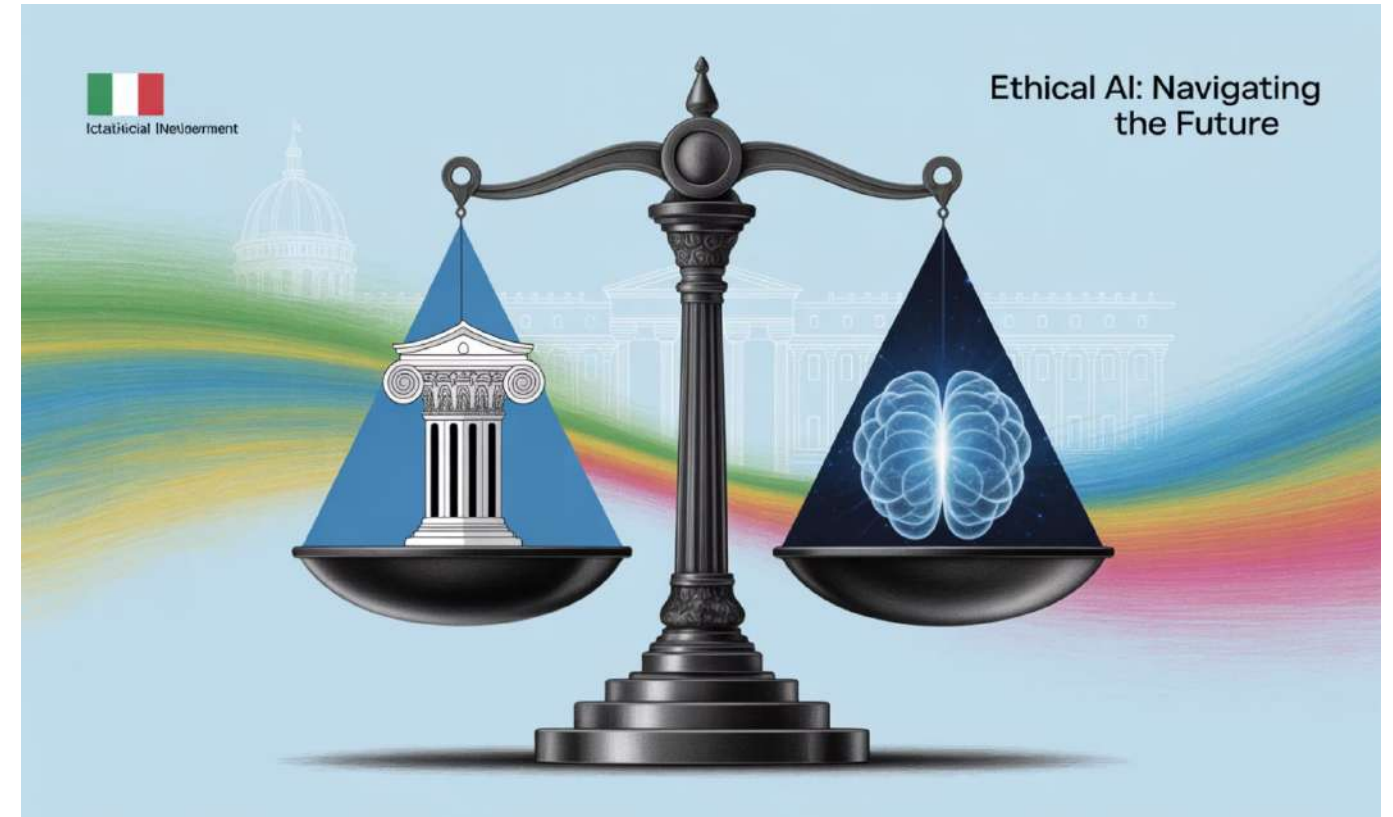
A futuristic digital cityscape with classical buildings, a glowing globe labeled 'Digital ethics', and a network of glowing lines and nodes.

Governance Etica dell'IA

Etica e Normativa nell'IA

Il Capitolo 6 delle Linee Guida AGID affronta la dimensione etica dell'Intelligenza Artificiale nella Pubblica Amministrazione, riconoscendo che la conformità normativa, sebbene fondamentale, non esaurisce la complessità delle implicazioni etiche legate all'uso di queste tecnologie.

Il capitolo chiarisce che i codici etici sono "volontari" ma "non possono comportare un abbassamento delle tutele o il venir meno degli obblighi normativi". Questo significa che l'etica non sostituisce la legge, ma la integra, fornendo un livello di guida superiore e più flessibile per affrontare le sfumature e le aree grigie che la normativa, per sua natura, non può coprire in dettaglio.



Le PA sono incoraggiate a sviluppare una "cultura etica" dell'IA che vada oltre la mera conformità legale. Questo è particolarmente rilevante in un campo in rapida evoluzione come l'IA, dove la legislazione spesso segue l'innovazione. L'adozione di codici etici può migliorare la fiducia pubblica e guidare decisioni responsabili in situazioni complesse non esplicitamente regolate, promuovendo un uso dell'IA che sia non solo legale ma anche giusto e socialmente accettabile.



L'Etica come Complemento alla Compliance



Conformità Normativa

L'etica è qui intesa come un complemento essenziale alla compliance normativa.



Collaborazione tra PA

Fermo restando il rispetto degli obblighi di conformità all'AI Act e a ogni altra normativa vigente, le PA POSSONO dotarsi di codici etici e di comportamento, anche in collaborazione con altre amministrazioni.

Codici Etici: Scopo e Limiti

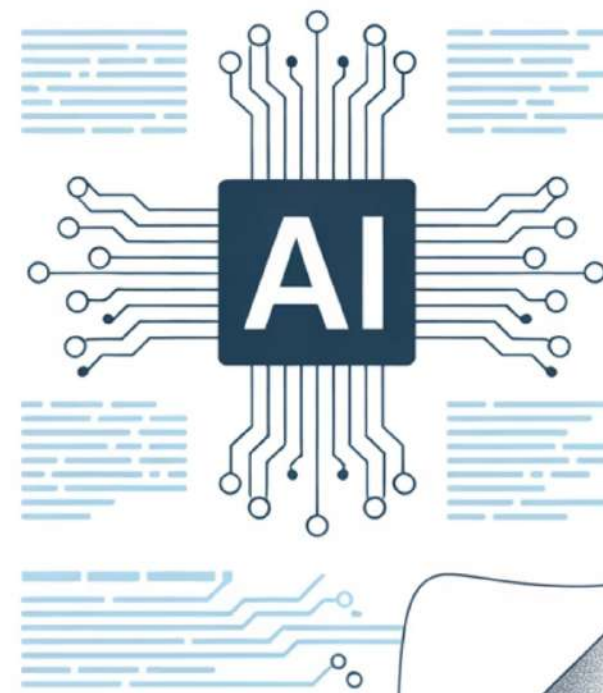
Adozione Volontaria

Questi codici, la cui adozione è su base volontaria, mirano a coadiuvare le PA nella selezione e nell'uso dei sistemi di IA e a introdurre regole di utilizzo per i dipendenti, promuovendo un approccio consapevole e responsabile.

Mantenimento delle Tutele

È cruciale sottolineare che questi codici etici e di condotta NON POSSONO comportare un abbassamento delle tutele o il venir meno degli obblighi normativi già stabiliti.

Ethical Code for Artificial Intelligence



Sviluppo dei Codici Etici



Le PA POSSONO sviluppare tali codici favorendo il coinvolgimento degli stakeholder, garantendo così una prospettiva ampia e inclusiva. Il contenuto di questi codici può prevedere elementi e requisiti supplementari rispetto alla normativa, incentivando l'applicazione volontaria dei requisiti dell'AI Act anche ai sistemi non classificati ad alto rischio, promuovendo così un livello di protezione e responsabilità più elevato.

Fonti Autorevoli per i Codici Etici

Per la stesura e l'implementazione di questi codici, le PA DEVONO tenere in adeguata considerazione gli Orientamenti etici per un'IA affidabile dell'AI HLEG (High-Level Expert Group on AI) e altre fonti europee e internazionali autorevoli (ad esempio, IEEE, OECD, UNESCO, ONU, Stato della Città del Vaticano).



AI HLEG

Orientamenti etici per un'IA affidabile dell'High-Level Expert Group on AI



Organizzazioni Internazionali

IEEE, OECD, UNESCO, ONU



Altre Fonti

Stato della Città del Vaticano



Scopi Fondamentali dei Codici Etici

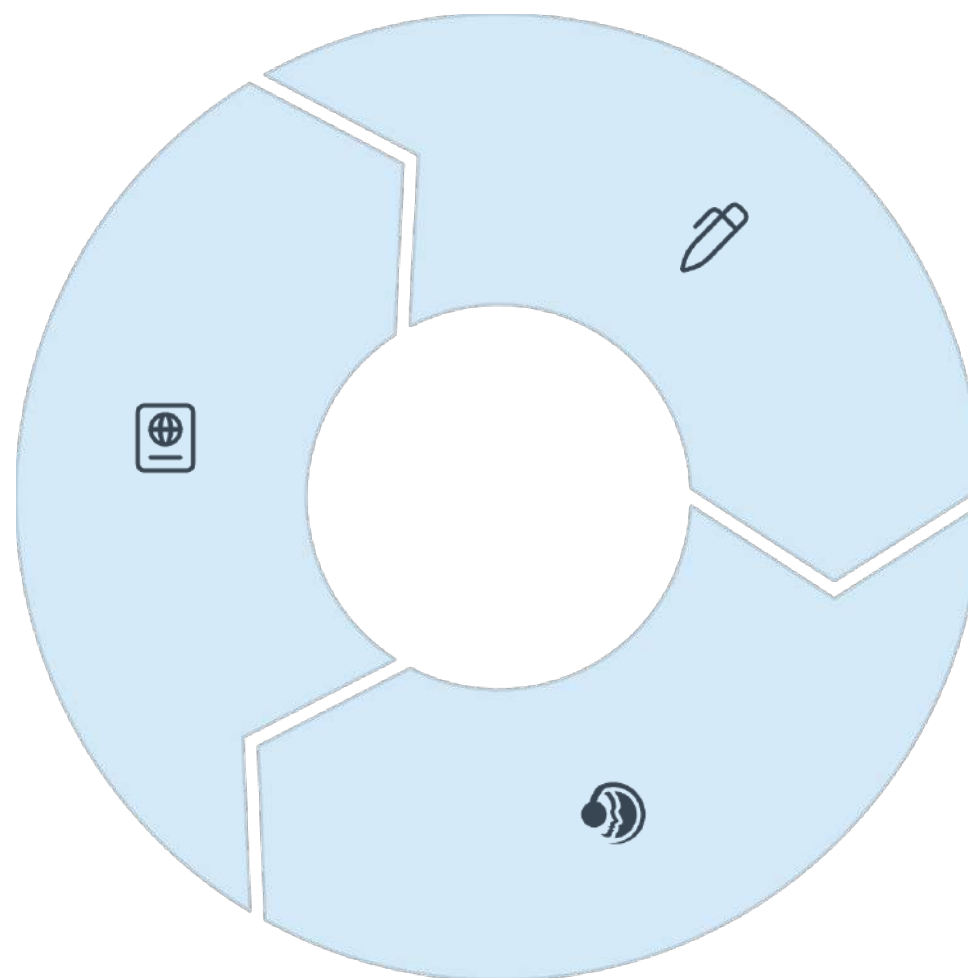
I codici etici DOVREBBERO perseguire una serie di scopi fondamentali, tra cui:

-  Garantire elevati standard professionali nell'uso dell'IA.
-  Promuovere la formazione continua e la consapevolezza pubblica sull'IA.
-  Incentivare l'uso dell'IA per il bene pubblico.
-  Stimolare l'investimento nella ricerca per mitigare i rischi associati all'IA.
-  Favorire lo sviluppo di standard tecnici internazionali che supportino un'IA responsabile.

Revisione periodica dei Codici Etici

Codice Etico

Le PA DEVONO garantire che i codici etici siano revisionati periodicamente



Aggiornamento

Per essere sempre aggiornati rispetto all'evoluzione tecnologica e normativa

Consultazione

Questa revisione DEVE avvenire in consultazione con esperti e stakeholder

Modello di Codice Etico



L'**Allegato D** delle Linee Guida fornisce un modello di codice etico e di comportamento, offrendo un punto di partenza pratico per le amministrazioni.



Comunicazione

Importanza della Comunicazione e Trasparenza

Il Capitolo 7 delle Linee Guida AGID si concentra sull'importanza della comunicazione e della trasparenza nell'adozione e nell'uso dei sistemi di Intelligenza Artificiale da parte della Pubblica Amministrazione. La comunicazione è vista come un elemento chiave per costruire e mantenere la fiducia dei cittadini e degli utenti nei confronti delle soluzioni basate sull'IA.

La trasparenza è il fondamento della fiducia pubblica nell'IA. Le sezioni 7.1 e 7.2 enfatizzano ripetutamente la "trasparenza" e gli "obblighi di informativa" come requisiti fondamentali, con riferimenti espliciti all'AI Act e al GDPR. L'obiettivo è che gli utenti siano "consapevoli del loro utilizzo e dell'impatto sui processi decisionali" e abbiano il "diritto di ottenere una spiegazione comprensibile delle decisioni IA".



Ciò significa che la fiducia dei cittadini nell'IA della PA è direttamente proporzionale alla trasparenza e alla comprensibilità dei sistemi. Le PA non devono solo implementare l'IA, ma anche "demistificarla" per il pubblico, spiegando come funziona, quali dati usa e come le decisioni vengono prese. Questo richiede l'uso di un linguaggio chiaro, la disponibilità di canali di comunicazione accessibili e la proattività nell'informare gli utenti, anche quando interagiscono con un chatbot, per esempio chiarendo quando non è in grado di rispondere e attivando canali umani.

Misure di Trasparenza

Consapevolezza dell'Interazione con l'IA

Le PA che adottano sistemi di IA DEVONO implementare misure di trasparenza per garantire che gli utenti siano consapevoli del loro utilizzo e dell'impatto sui processi decisionali. L'AI Act, in particolare, prevede requisiti stringenti di trasparenza per i sistemi ad alto rischio e per determinati sistemi di IA (articolo 50).

Requisiti di Trasparenza

Le PA, sia come fornitori che come deployer, DEVONO applicare o verificare l'applicazione di tali requisiti, che includono:

- Informazioni sull'interazione con l'IA: Gli utenti devono essere consapevoli quando comunicano con una macchina.
- Indicazione dei contenuti generati artificialmente: È necessario segnalare chiaramente i contenuti creati o manipolati dall'IA (ad esempio, i deepfake).
- Documentazione tecnica: La documentazione tecnica deve essere disponibile per le autorità competenti.
- Obblighi specifici per sistemi ad alto rischio: Questi includono istruzioni dettagliate e la tracciabilità delle decisioni.

Protezione dei Dati Personali

Le PA DEVONO essere trasparenti nell'utilizzo di sistemi di IA che trattano dati personali, fornendo informative adeguate, esaustive e accessibili agli interessati, nel rispetto del GDPR.

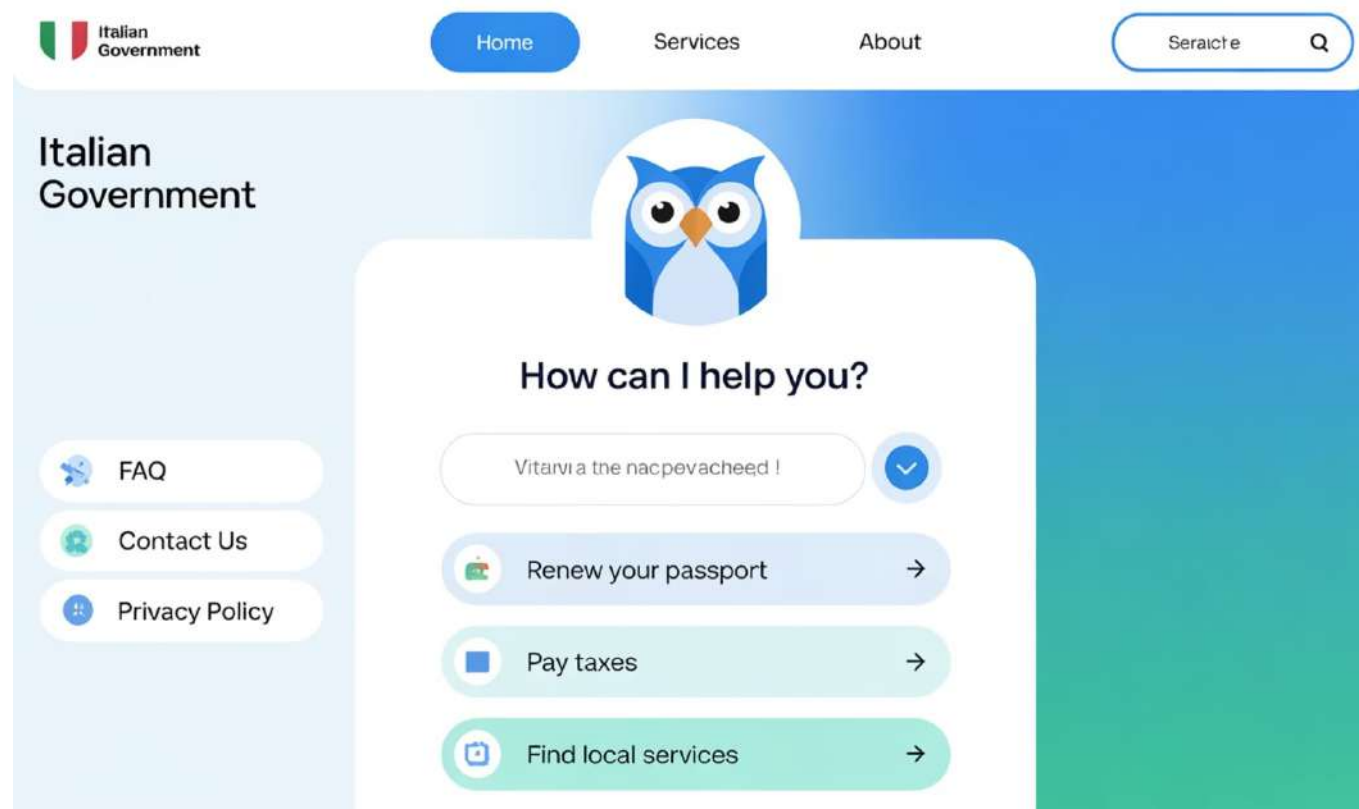
Obblighi di Informativa

		
Descrizione del Sistema	Criteri di Decisione	Diritto di Opposizione
Nel rispetto del GDPR e dell'AI Act, le PA DEVONO garantire un elevato livello di trasparenza e chiarezza nell'impiego di sistemi di IA, specialmente quando questi impattano sui diritti e interessi degli utenti. L'informativa fornita DEVE essere chiara, esaustiva e accessibile, includendo la descrizione del sistema di IA e delle sue finalità.	Spiegazione dei criteri e parametri delle decisioni automatizzate e dei possibili impatti sui cittadini. I cittadini DEVONO essere informati della facoltà di ottenere una spiegazione comprensibile delle decisioni IA, con trasparenza del processo decisionale e descrizione dei dati utilizzati.	Le PA DEVONO informare gli utenti della possibilità di opporsi a decisioni automatizzate e di richiedere l'intervento umano, specificando le modalità per l'esercizio di tale diritto e garantendo l'accesso a un riesame umano.

Le PA DOVREBBERO elaborare informative dettagliate e personalizzate per ogni sistema di IA, per massimizzare la comprensione da parte degli utenti.

Adottare l'IA nella Comunicazione Istituzionale

L'IA può migliorare significativamente l'efficacia, l'accessibilità e l'interattività delle comunicazioni istituzionali, ad esempio tramite l'uso di chatbot e assistenti virtuali.



Ottimizzazione

Ottimizzazione dei processi creativi e personalizzazione dei messaggi



Automazione

Automazione delle risposte e rapidità nell'erogazione delle informazioni



Accessibilità

Aumento dell'accessibilità per diverse fasce di utenti



Costi

Potenziale riduzione dei costi operativi

Approccio Responsabile all'IA nella Comunicazione

Percorso Graduale

Le PA che adottano sistemi di IA per la comunicazione DEVONO seguire un percorso graduale e pianificato, come descritto nel Capitolo 4.

1

2

Formazione Adeguata

I dipendenti coinvolti DEVONO ricevere una formazione adeguata sull'utilizzo dei sistemi di IA.

3

Trasparenza

Le PA DEVONO informare i cittadini sull'uso dell'IA e sulla gestione dei dati, garantire la protezione dei dati personali.

4

Segnalazione Esplicita

È necessario segnalare esplicitamente l'uso di strumenti IA nelle comunicazioni istituzionali.

5

Accessibilità

Assicurare la massima accessibilità e comprensione delle comunicazioni per tutti i cittadini.

Limiti e supervisione umana



È altresì importante che le PA NON DEVONO sviluppare una dipendenza eccessiva dall'IA o affidarsi completamente ad essa, garantendo sempre una supervisione umana e mantenendo un tono umano ed empatico nella comunicazione.

Evitare la Dipendenza Eccessiva

Le PA non devono diventare troppo dipendenti dai sistemi di IA per la comunicazione istituzionale.

Garantire la Supervisione Umana

È fondamentale mantenere sempre un controllo umano sui processi automatizzati.

Mantenere l'Empatia

La comunicazione deve conservare un tono umano ed empatico, anche quando supportata da tecnologie IA.



Formazione e sviluppo delle Competenze

Il Digital Divide nella Pubblica Amministrazione

Il Capitolo 8 delle Linee Guida AGID sottolinea l'importanza cruciale della formazione e dello sviluppo delle competenze per un'adozione efficace e responsabile dell'Intelligenza Artificiale nella Pubblica Amministrazione.

Il "digital divide interno" emerge come una barriera significativa all'adozione efficace dell'IA. Questo capitolo sottolinea la necessità di "acquisire e sviluppare competenze adeguate" e di ampliare le "competenze digitali di base di tutti i dipendenti pubblici, includendo l'AI literacy".



Documenti esterni evidenziano la "scarsa supervisione" e la "mancanza di competenze tecniche tra il personale amministrativo" come sfide concrete. La Direttiva NIS2, inoltre, integra l'IA nella formazione sulla cybersecurity, suggerendo una lacuna esistente nella preparazione del personale pubblico.

Questo significa che la mancanza di competenze interne è una delle sfide più significative per l'adozione dell'IA nella PA. Senza un investimento massiccio e continuo in formazione (dalla AI literacy di base alle competenze specialistiche), le PA non saranno in grado di governare, implementare e gestire efficacemente i sistemi IA, né di sfruttarne appieno il potenziale. Ciò richiede un approccio strategico alla gestione delle risorse umane e alla formazione, con percorsi differenziati per i vari livelli e ruoli all'interno dell'amministrazione.



Acquisizione di Competenze Adeguate

Obbligo di acquisizione competenze

La PA DEVE acquisire e sviluppare competenze adeguate sia a livello individuale che organizzativo per cogliere appieno i vantaggi offerti dall'IA.

Comprensione delle potenzialità

È fondamentale che il personale comprenda le potenzialità e le implicazioni dell'IA per migliorare i servizi pubblici e sviluppi competenze specifiche per governare e regolamentare il suo utilizzo, garantendo il rispetto dei principi etici, la protezione dei dati e la trasparenza.

Standard e normative

L'AI Act e lo standard ISO/IEC 42001 evidenziano la necessità di interventi formativi differenziati e di una mappatura delle figure professionali per definire piani formativi mirati.



AI Literacy per i Dipendenti Pubblici

Ampliamento competenze digitali



La diffusione dell'IA richiede un ampliamento delle competenze digitali di base di tutti i dipendenti pubblici, includendo l'AI literacy, ovvero la consapevolezza sull'IA e la comprensione degli aspetti normativi, operativi e di dominio.

Formazione su etica e sicurezza



I dipendenti pubblici DEVONO essere formati sui principi etici e sulla gestione dei rischi di sicurezza legati all'IA.

Competenze specialistiche



È altresì opportuno identificare e rafforzare competenze tecniche di dominio e specialistiche, anche tramite reclutamento e upskilling.

Figure Professionali Critiche per l'IA



Tra le figure professionali critiche per l'IA nella PA vengono citate, ad esempio, data engineer, machine learning engineer, prompt engineer, data scientist, AI ethicist, giurista informatico, change manager ed esperti umanisti.



Definizione dei profili

È necessario definire profili professionali e percorsi di carriera per dirigenti e specialisti AI.



Competenze dirigenziali

I dirigenti pubblici, in particolare, DEVONO avere competenze adeguate per prendere decisioni consapevoli sull'adozione dell'IA, comprendendo opportunità, implicazioni e impatti, e sviluppando capacità di gestione del cambiamento.

Indicazioni operative per le PA

Le Linee Guida forniscono indicazioni operative concrete per supportare le amministrazioni nell'implementazione di strategie efficaci per lo sviluppo delle competenze necessarie all'adozione dell'IA.



Indicazioni Operative 1



Promozione AI literacy

Le PA DEVONO promuovere l'AI literacy di tutti i dipendenti pubblici, definendo obiettivi di performance individuali e favorendo la fruizione di programmi formativi specifici sull'IA.



Diffusione Linee Guida

DEVONO garantire la massima diffusione delle Linee Guida sull'IA di AgID all'interno delle proprie strutture.



Learning communities

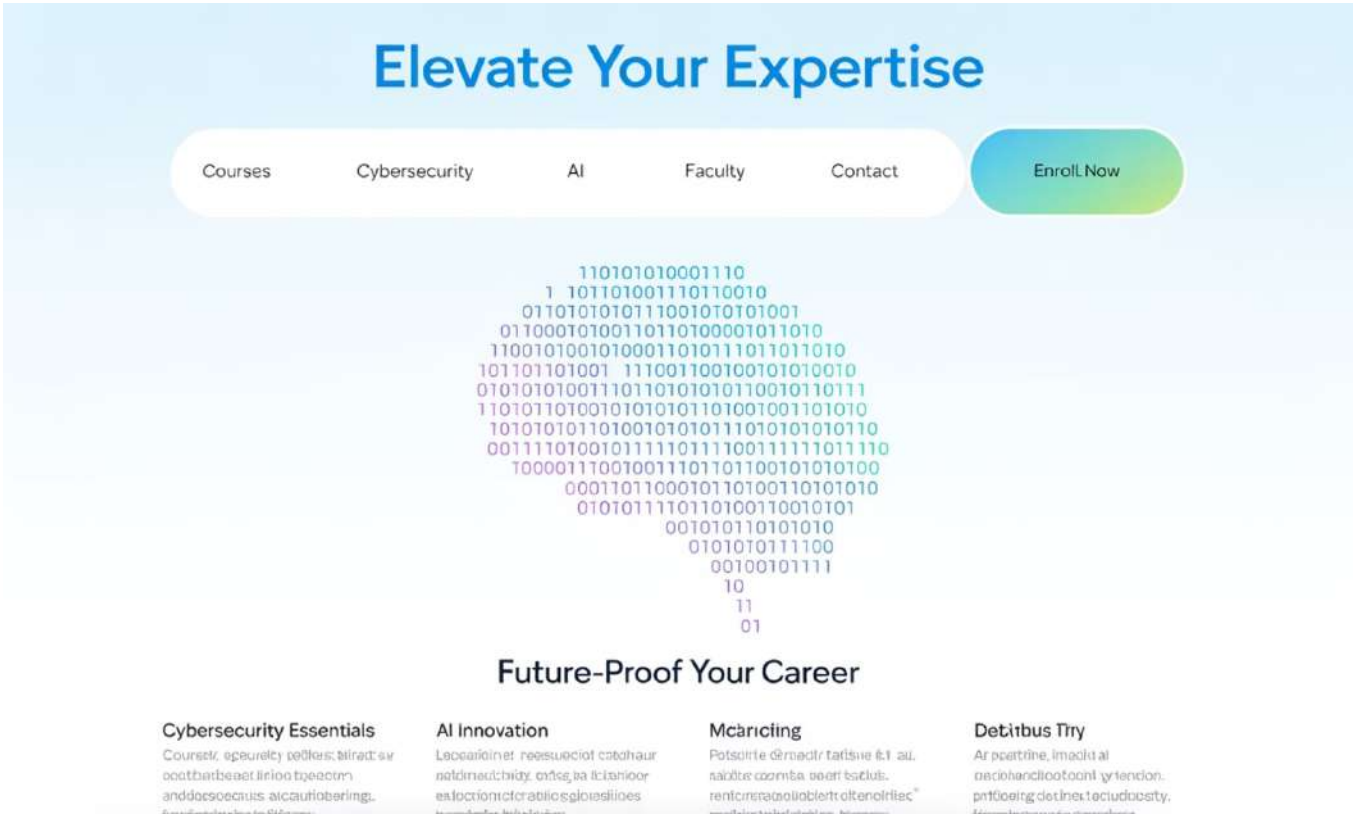
DEVONO promuovere e favorire la partecipazione degli RTD, UTD e altri attori chiave a learning communities sull'adozione dell'IA, per facilitare lo scambio di conoscenze e best practice.



Obiettivi di performance

Le PA che adottano progetti IA DEVONO promuovere e favorire la definizione di obiettivi di performance dei dirigenti connessi alla partecipazione a percorsi formativi a supporto del decision making e della guida dei processi di adozione dell'IA.

Indicazioni Operative 2



- Le PA che realizzano progetti di trasformazione digitale basati sull'AI DEVONO promuovere la realizzazione di programmi formativi mirati e contestualizzati alle specifiche esigenze del progetto.
- Le PA coinvolte in attività di sviluppo, acquisizione e gestione dell'IA DEVONO favorire l'accesso a percorsi tecnico-specialistici per UTD e professionisti IT, con una rilevazione sistematica dei fabbisogni di competenze e la collaborazione con Università e centri di competenza.
- DEVONO prevedere percorsi formativi specifici sulla sicurezza cibernetica dell'IA, data la sua crescente importanza.
- DEVONO dare evidenza degli interventi formativi nel PIAO, integrando la strategia di sviluppo delle competenze nella pianificazione generale dell'ente.
- Le PA DOVREBBERO promuovere una cultura dell'apprendimento continuo, incoraggiando la crescita professionale costante.

Indicazioni Operative 3



Attrazione di talenti

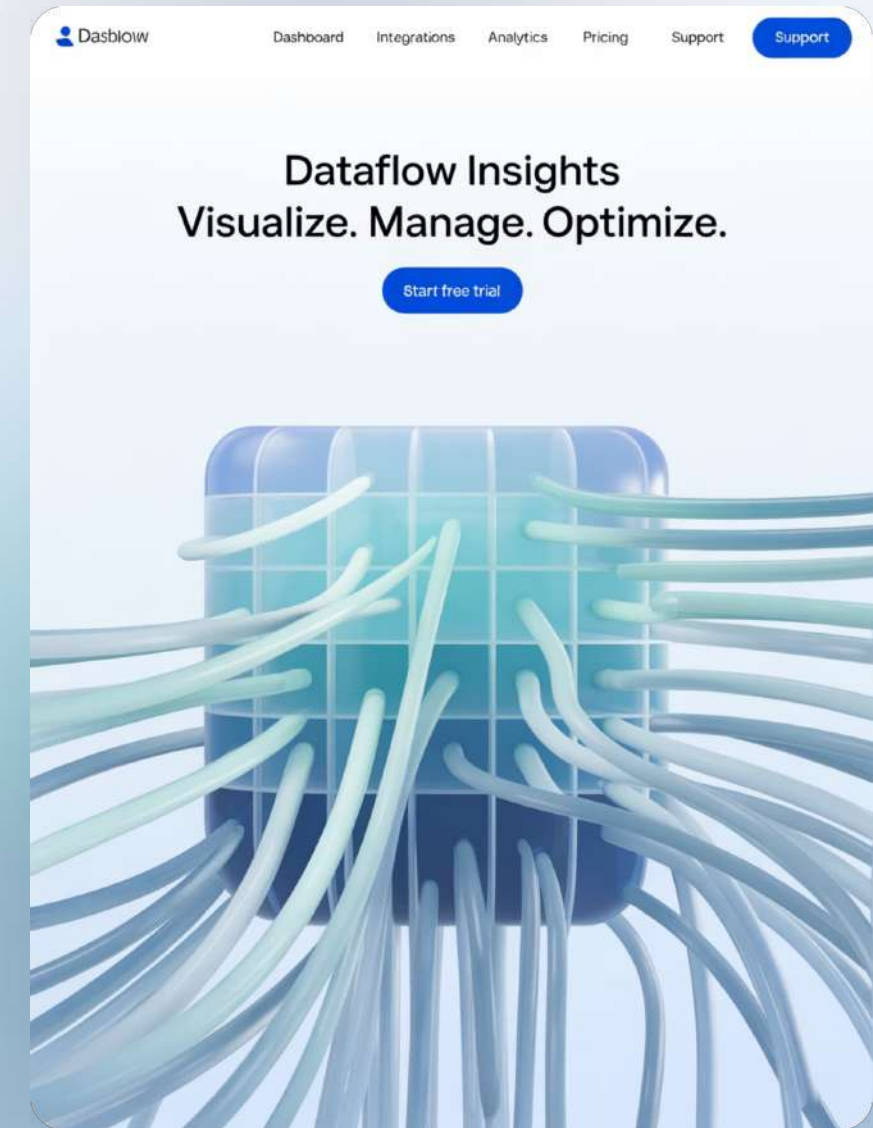
POSSONO intraprendere azioni per favorire l'attrazione di talenti e giovani specialisti (ad esempio, hackathon, tirocini, dottorati) e promuovere attività di ricerca interdisciplinare.



AI awareness per i cittadini

Infine, le amministrazioni POSSONO contribuire a promuovere l'AI awareness e AI literacy dei cittadini, affinché interagiscano in modo efficace, consapevole e sicuro con le soluzioni di IA.

Gestione e Qualità dei Dati



Importanza della Gestione dei Dati

Il Capitolo 9 delle Linee Guida AGID pone un'enfasi cruciale sulla gestione e la qualità dei dati, riconoscendoli come il prerequisito fondamentale per l'affidabilità e l'efficacia dei sistemi di Intelligenza Artificiale nella Pubblica Amministrazione. L'AI Act stesso evidenzia l'importanza della qualità dei dati come elemento essenziale per sistemi di IA affidabili. La governance e la corretta gestione dei dati sono propedeutici a garantire la disponibilità e la qualità dei dati stessi.

L'Unione Europea ha definito un quadro normativo (come il Data Governance Act - DGA) per favorire la circolazione dei dati, garantendo al contempo protezione, diritti fondamentali, sicurezza e cybersicurezza.



La gestione dei dati nel contesto pubblico NON PUÒ prescindere da un coordinamento con le politiche europee e nazionali sui dati e dati aperti. In questo contesto, le strategie di licensing per l'acquisizione, l'elaborazione, il rilascio/pubblicazione e il riutilizzo dei dataset pubblici assumono un'importanza cruciale.

Tipologie di Dati

9.1. Tipologie di dati:

I dati rappresentano l'aspetto più rilevante e critico nell'adozione dell'IA. Ai fini della costruzione del modello e del deployment del sistema di IA, l'AI Act identifica tre tipologie principali:

1 **Dati di addestramento**

Utilizzati per addestrare un sistema di IA.

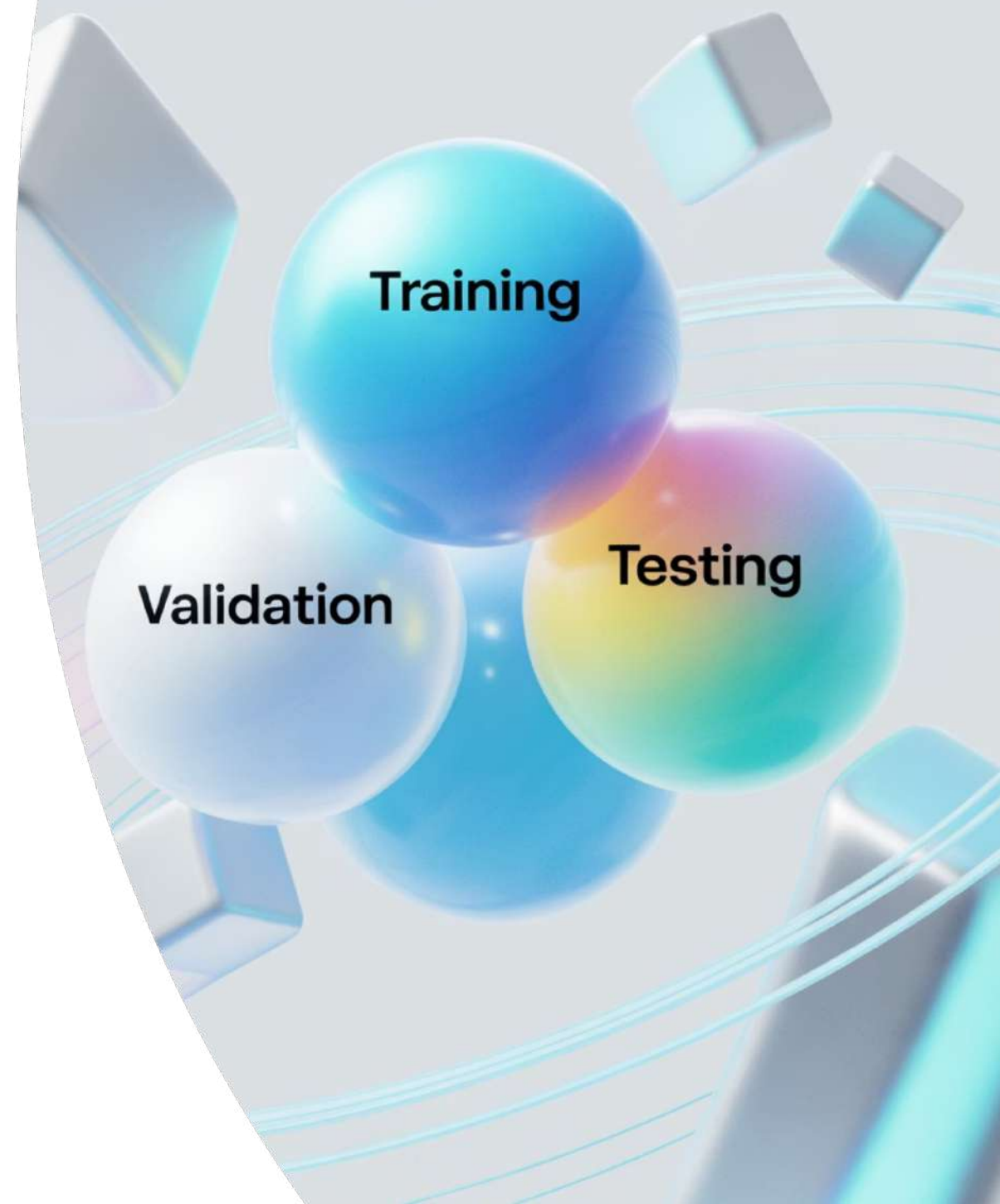
2 **Dati di convalida**

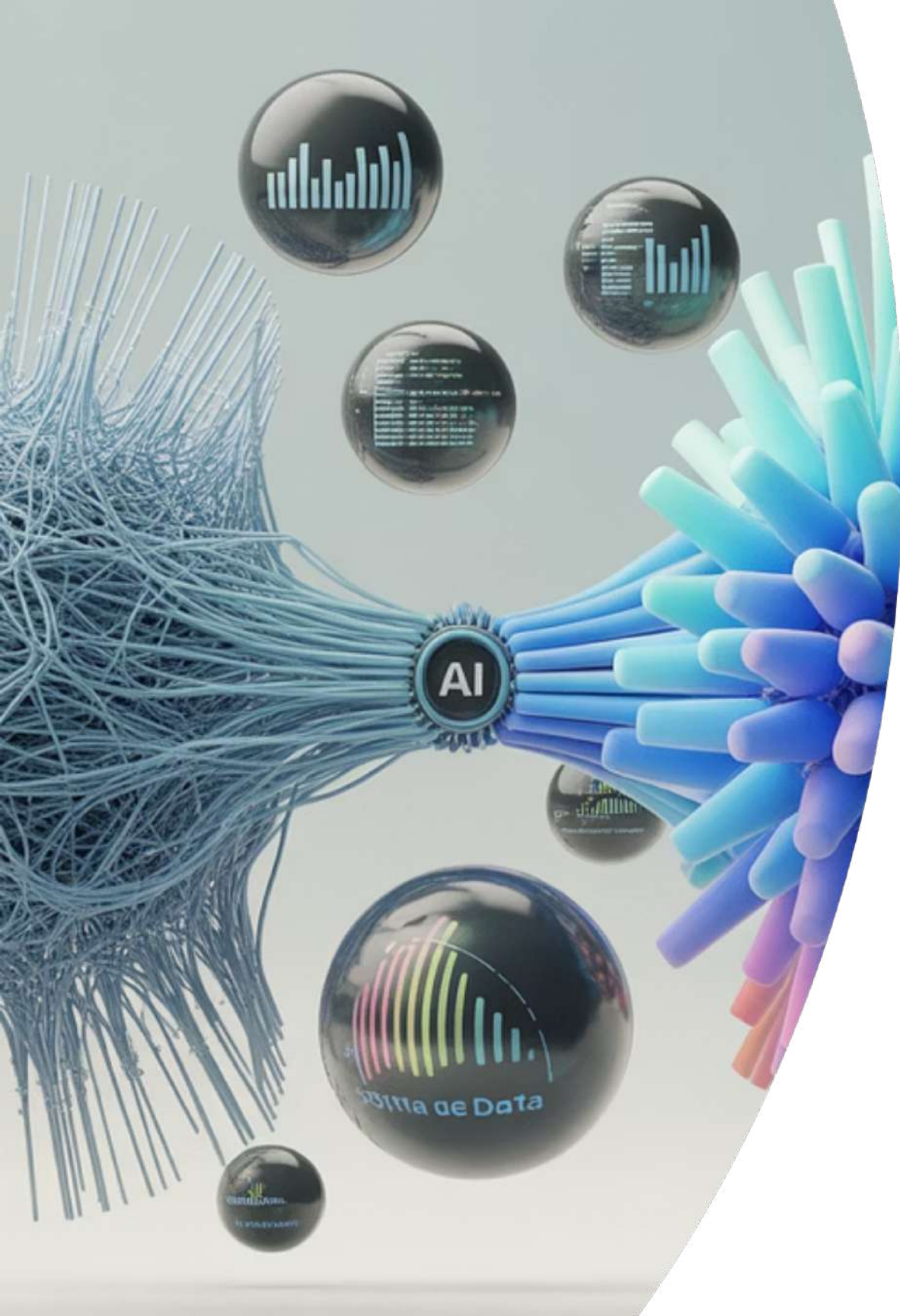
Utilizzati per valutare il sistema di IA addestrato e metterne a punto i parametri.

3 **Dati di prova**

Utilizzati per una valutazione indipendente del sistema di IA prima dell'immissione sul mercato.

AI Data Types





Classificazione dei Dati



Per Fonte

Con riferimento alle fonti, si distinguono dati interni alla PA e dati esterni alla PA.



Per Struttura

Per la struttura, si hanno dati strutturati, non strutturati e semi-strutturati.

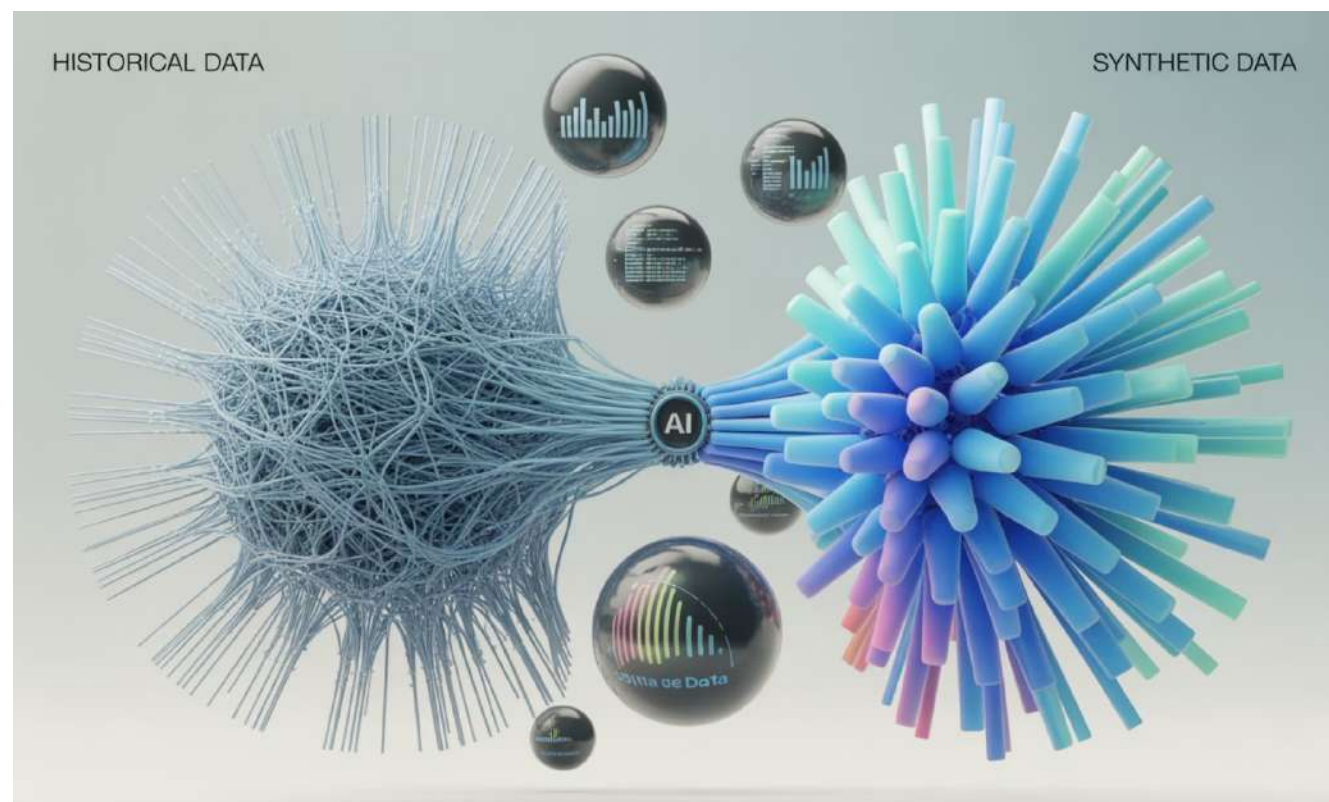


Per Fase

A seconda della fase di utilizzo/produzione, si distinguono dati di input (per addestramento, convalida, prova o pre-elaborazione) e dati di output (generati dal modello, di performance, predizioni).

Si considerano anche i dati del sistema di IA stesso (parametri del modello, metadati, codice sorgente, dati di performance, dati di log, dati di stato, dati temporanei).

Dati Storici e Sintetici



L'impiego di tecniche di IA predittiva è spesso associato all'utilizzo di dati storici, che possono presentare distorsioni.

I dati sintetici, creati artificialmente per l'addestramento, sono efficaci quando i dati reali sono difficili da raccogliere o da trattare nel rispetto dei requisiti di privacy. Gli spazi comuni di dati europei (ad esempio, in agricoltura, salute, PA) possono facilitare la condivisione di dati affidabili e sicuri.

Caratteristiche dei Dati

I dataset sono considerati **infrastrutture essenziali** per lo sviluppo dell'IA nella PA.



Qualità dei Dati nella PA



Analisi Sistemática

Le PA DOVREBBERO condurre un'analisi sistematica sullo stato e la qualità dei propri dataset, aggiornando e pubblicando i dati pubblicabili come open data secondo le linee guida Open Data.



Framework Sicuro

È fondamentale costruire un framework sicuro e comune per attuare le disposizioni del Data Governance Act per i dataset non pubblicabili come open data.



Qualità Elevata

I sistemi di IA apprendono e producono analisi affidabili solo se hanno a disposizione una quantità adeguata di dati di elevata qualità, nel rispetto delle normative sulla protezione e sicurezza dei dati.

Le linee guida Open Data forniscono indicazioni sulla qualità dei dati, facendo riferimento agli Standard UNI CEI ISO/IEC 25012:2014 e UNI CEI ISO/IEC 25024:2016.

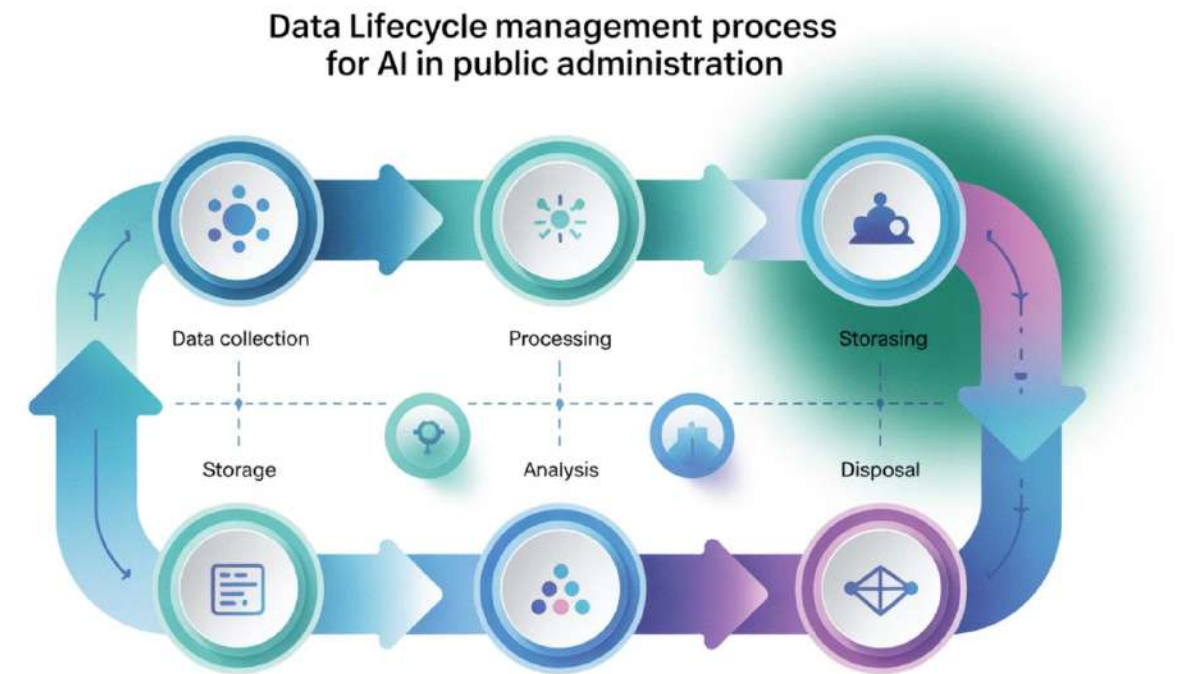
Per i sistemi di IA DOVREBBERO essere garantite caratteristiche di qualità come rappresentatività, bilanciamento, tracciabilità, disponibilità e credibilità.

La quantità dei dati è importante per addestrare efficacemente i sistemi di IA, specialmente nel contesto dei Big Data (caratterizzati da volume, varietà, velocità, variabilità). È rilevante fornire informazioni chiare e comprensibili sulle fonti dei dati e sulla logica che ha portato alla previsione o decisione. L'IA può anche migliorare la qualità dei dati stessi, armonizzando classificazioni, standardizzando, bonificando e migliorando l'accuratezza degli archivi, ed estraendo termini chiave.

Processi e Governance dei Dati

Processi e governance dei dati:

Per una corretta gestione dei dati nell'adozione di soluzioni di AI nella PA, è necessario delineare un processo strutturato e responsabile che copra l'intero ciclo di vita del dato, garantendo sicurezza e conformità.



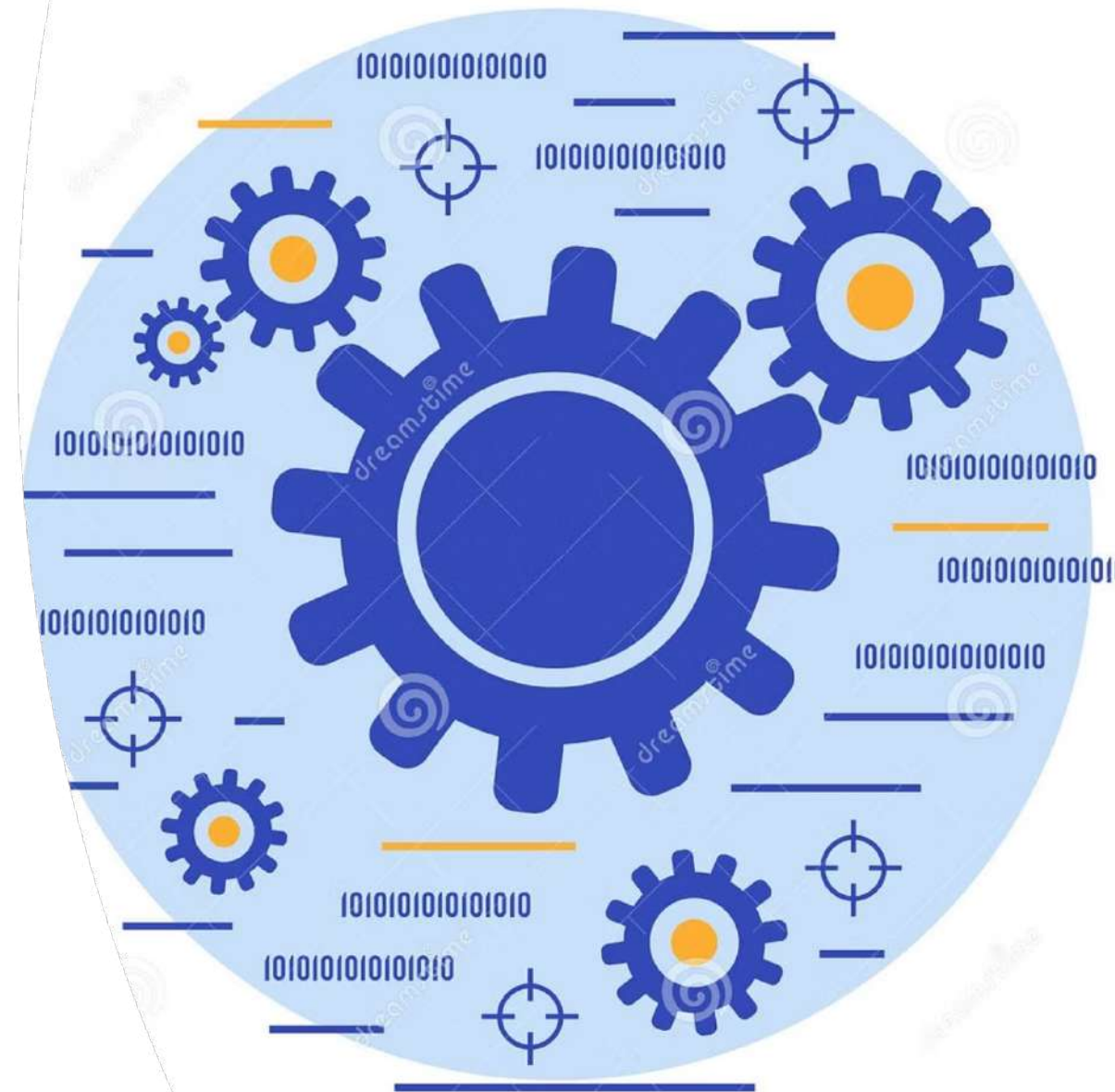
Integrazione dei Processi



Questo processo NON DOVREBBE prefigurare nuovi processi di gestione dei dati per l'IA separati dalle procedure esistenti, ma integrare le procedure e pratiche relative al contesto dell'IA.

Le Linee guida Open Data includono una sezione sugli aspetti organizzativi e un percorso di preparazione dei dati. Un modello di processo di gestione complessiva dei dati, adattato dalle linee guida Open Data con integrazioni dall'AI Act e dagli Standard ISO.

Fasi del Processo di Gestione dei Dati



DATA PROCE

Fasi Iniziali: Identificazione e Analisi

Identificazione

Pianificazione della raccolta e gestione dei dati, ricognizione di dati interni ed esterni, analisi dei vincoli.

Analisi

Verifica della qualità originaria dei dati, pulizia/bonifica, analisi del processo organizzativo.



Fasi Intermedie: Preparazione e Validazione

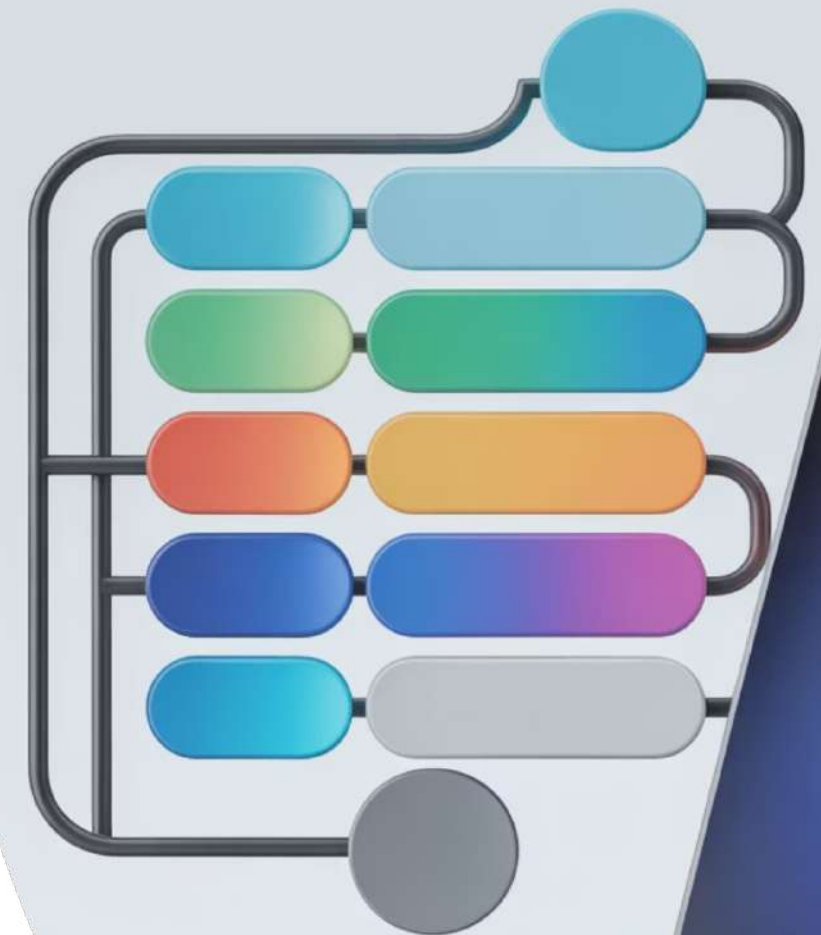
Preparazione

Arricchimento, modellazione e documentazione, operazioni di pre-processing (trasformazione, ricampionamento, etichettatura, codifica, anonimizzazione/pseudonimizzazione).

Validazione

Valutazione della qualità, verifica dell'integrità, valutazione di possibili distorsioni.

Dataflow AI





Fasi Finali: Utilizzazione e Monitoraggio

Utilizzazione

Pubblicazione, conservazione dei dati, addestramento-implementazione e funzionamento del sistema.

Monitoraggio

Monitoraggio costante della qualità e freschezza dei dati, revisioni e aggiornamenti periodici, dismissione dei dati.

Governance e collaborazione

La governance dei dati richiede l'individuazione chiara di ruoli e responsabilità, con la raccomandazione di costituire un gruppo di lavoro dedicato all'apertura dei dati. È auspicabile che la governance dei dati sia ricondotta a un'unica struttura di coordinamento. La collaborazione istituzionale è fondamentale, con amministrazioni che possono svolgere un ruolo di coordinamento (hub nazionali/regionali) e intermediazione verso gli enti locali.



Opportunità e Rischi

Opportunità

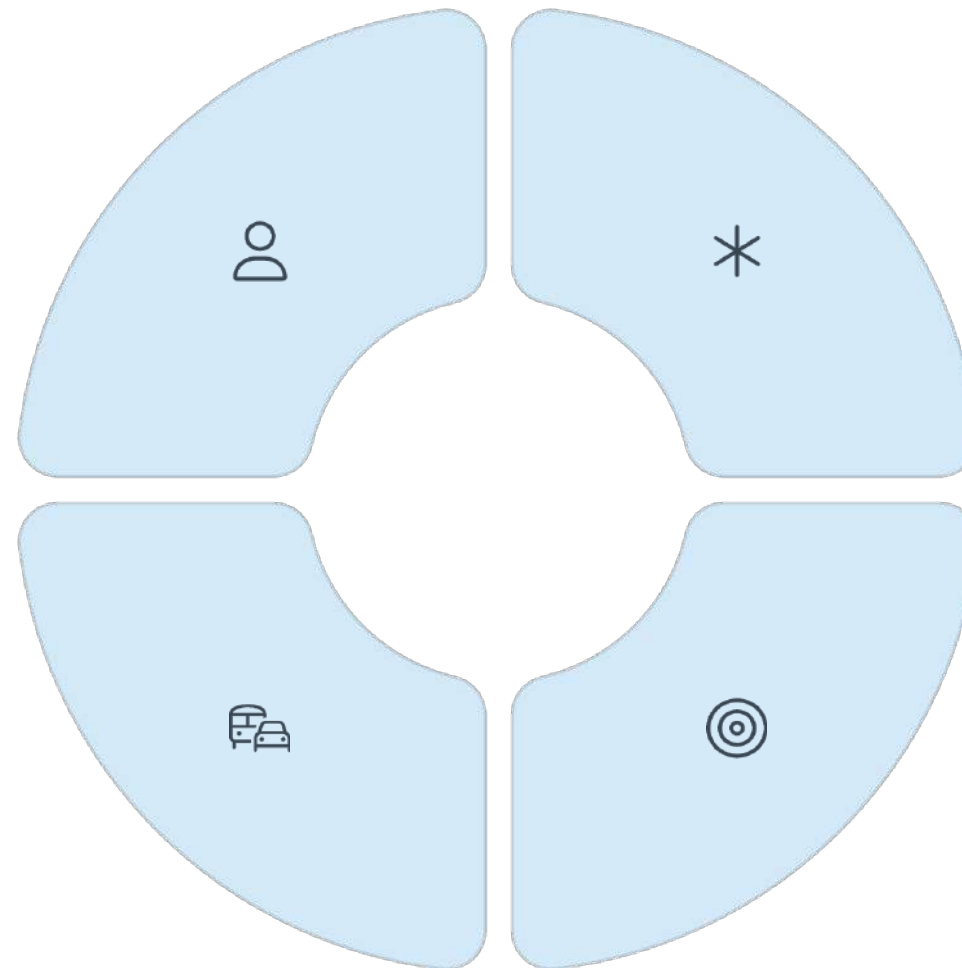
I dati rappresentano la più grande opportunità per l'IA nella PA.

L'AI Act richiede "high-quality data sets", e il Data Governance Act mira a "facilitare il riutilizzo e la condivisione dei dati".

Trasformazione

Le PA devono affrontare la sfida di trasformare i loro vasti archivi di dati in risorse utilizzabili per l'IA.

Investire in infrastrutture, competenze di data governance e metodologie per la bonifica e l'anonimizzazione.



Rischi

I dati rappresentano il più grande rischio per l'IA nella PA.

I dati storici possono presentare "distorsioni", e la "quantità" è cruciale per l'accuratezza.

Strategia

La disponibilità di dati di alta qualità, rappresentativi e non distorti è fondamentale per l'accuratezza e l'equità dei sistemi IA.

La gestione del ciclo di vita del dato diventa un processo strategico e non solo tecnico.

La sezione enfatizza che "I dati sono l'aspetto più rilevante e critico nell'adozione dell'IA".

Ciclo di Vita del Dato e Pratiche di Gestione

Fase del Ciclo di Vita del Dato	Descrizione delle Attività Chiave per l'IA	Obiettivi di Qualità/Conformità
Identificazione	Pianificazione della raccolta dati, ricognizione dati interni/esterni, analisi dei vincoli (normativi, etici, tecnici).	Definizione chiara delle finalità, liceità della raccolta, identificazione delle fonti affidabili.
Analisi	Verifica della qualità originaria dei dati, pulizia e bonifica, analisi del processo organizzativo di generazione.	Accuratezza, completezza, coerenza, identificazione e mitigazione di bias iniziali.
Preparazione	Arricchimento, modellazione e documentazione dei dati; operazioni di pre-processing (trasformazione, ricampionamento, etichettatura, codifica, anonimizzazione/pseudonimizzazione).	Rappresentatività, bilanciamento, tracciabilità, disponibilità, credibilità, minimizzazione dei dati, privacy by design.
Validazione	Valutazione della qualità dei dati preparati, verifica dell'integrità, valutazione di possibili distorsioni indotte dal pre-processing.	Conformità agli standard di qualità (UNI CEI ISO/IEC 25012/25024), assenza di bias residui, integrità.
Utilizzazione	Pubblicazione (se open data) e conservazione dei dati per l'addestramento, convalida e test dei modelli IA.	Accessibilità, riusabilità, sicurezza della conservazione, rispetto dei periodi di conservazione.
Monitoraggio	Monitoraggio costante della qualità e freschezza dei dati, revisioni e aggiornamenti periodici, dismissione dei dati non più necessari.	Mantenimento della qualità nel tempo, adattamento ai cambiamenti, conformità al principio di limitazione della conservazione.

Protezione dei Dati Personali (Capitolo 10)



Rispetto del Diritto Fondamentale

Il Capitolo 10 delle Linee Guida AGID sottolinea in modo esplicito che l'adozione di sistemi di Intelligenza Artificiale da parte delle Pubbliche Amministrazioni DEVE avvenire nel pieno rispetto del diritto fondamentale alla protezione dei dati personali.

Questo principio non è negoziabile e richiede una profonda attenzione alla valutazione e verifica della conformità normativa del sistema di IA e all'impatto sui diritti degli interessati.

Le PA sono chiamate ad adeguare il proprio modello organizzativo e le misure di sicurezza per garantire tale protezione.





Applicazione del GDPR all'IA nella PA

Il capitolo 10 chiarisce che il GDPR si applica "integralmente anche all'utilizzo dell'IA da parte della PA", con un'attenzione particolare ai principi di liceità, trasparenza, minimizzazione e integrità, oltre all'obbligo di DPIA per trattamenti ad alto rischio.

Privacy
by Design



Data.
protected.
Italia.



Privacy come prerequisito per l'Innovazione



Prerequisito Fondamentale

La protezione dei dati personali non è quindi un ostacolo all'innovazione AI, ma un prerequisito fondamentale per la sua adozione responsabile e legale nella PA.



Privacy by Design

Ogni sistema IA che tratta dati personali deve essere progettato con la privacy in mente (privacy by design) e sottoposto a una rigorosa DPIA.

Competenze Specializzate



Questo impone alle PA di avere competenze legali specializzate in protezione dati e di integrare il RPD nel ciclo di vita dell'IA, assicurando che le innovazioni tecnologiche non compromettano i diritti fondamentali dei cittadini.



Competenze Legali

Necessità di personale con conoscenze specifiche sulla normativa privacy



Integrazione del RPD

Il Responsabile Protezione Dati deve essere coinvolto in tutto il ciclo di vita dell'IA



Verifica dei Principi Fondamentali

In particolare, la PA DEVE verificare il rispetto dei principi fondamentali stabiliti dall'articolo 5 del GDPR, che si applicano integralmente anche all'utilizzo dell'IA.

Principi Fondamentali del GDPR

Liceità, Correttezza e Trasparenza

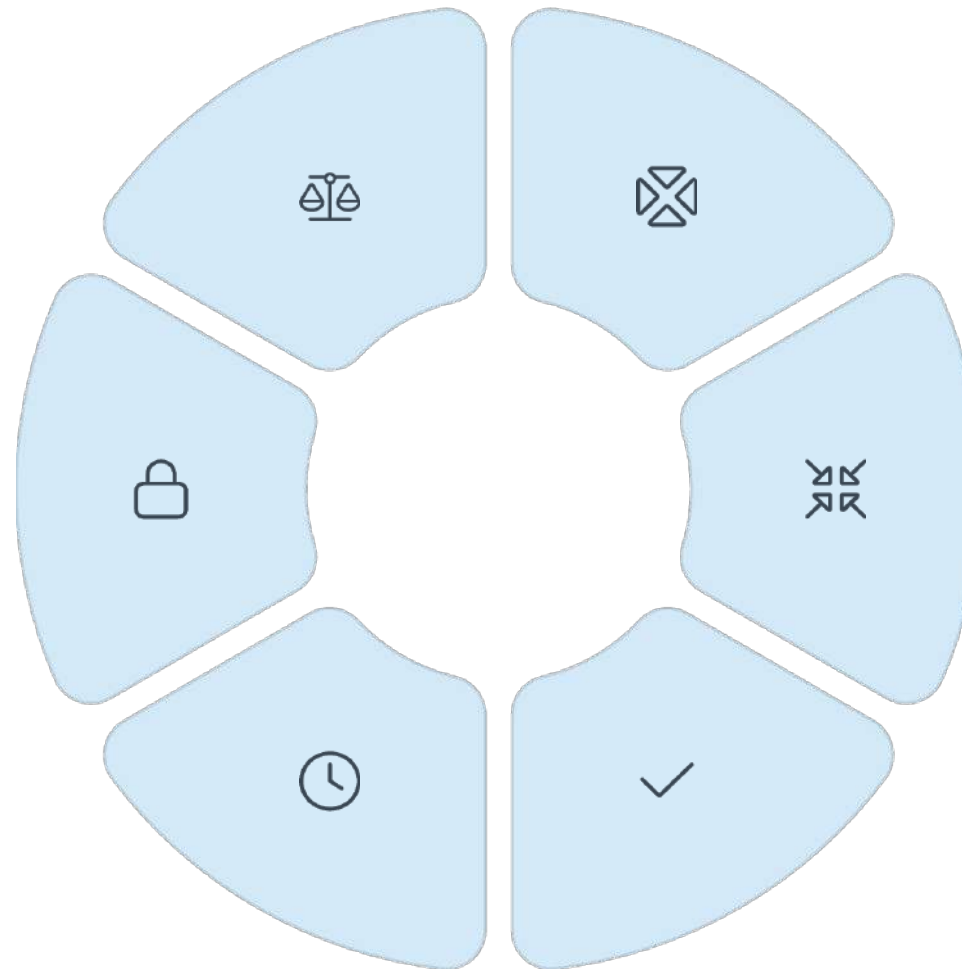
Il trattamento dei dati deve essere lecito, corretto e trasparente nei confronti dell'interessato.

Integrità e Riservatezza

I dati devono essere trattati in modo da garantire un'adeguata sicurezza, inclusa la protezione da trattamenti non autorizzati o illeciti.

Limitazione della Conservazione

I dati devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità.



Limitazione della Finalità

I dati devono essere raccolti per finalità determinate, esplicite e legittime, e non possono essere trattati in modo incompatibile con tali finalità.

Minimizzazione dei Dati

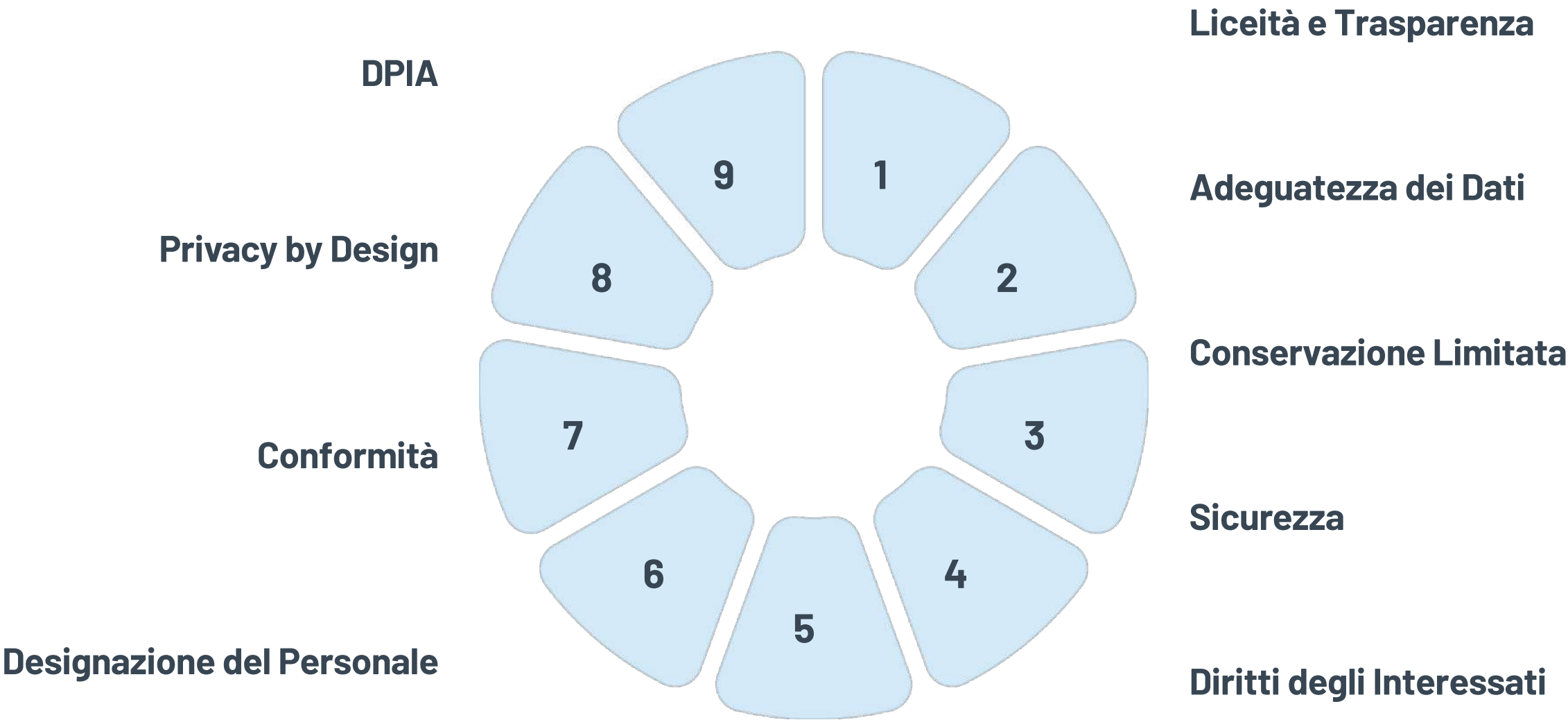
I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati.

Adempimenti Fondamentali

Se il sistema di IA comporta il trattamento di dati personali, la PA DEVE effettuare un'analisi specifica per garantire una serie di adempimenti fondamentali:



Principi Cardine del Garante Privacy

Il Garante per la protezione dei dati personali ha evidenziato tre principi cardine che devono guidare l'uso dell'IA nella PA:



Conoscibilità

L'interessato ha il diritto di conoscere la logica sottostante al trattamento automatizzato dei propri dati.



Non esclusività della decisione algoritmica

È necessaria la presenza di un intervento umano di controllo e validazione sulle decisioni generate dall'algoritmo.

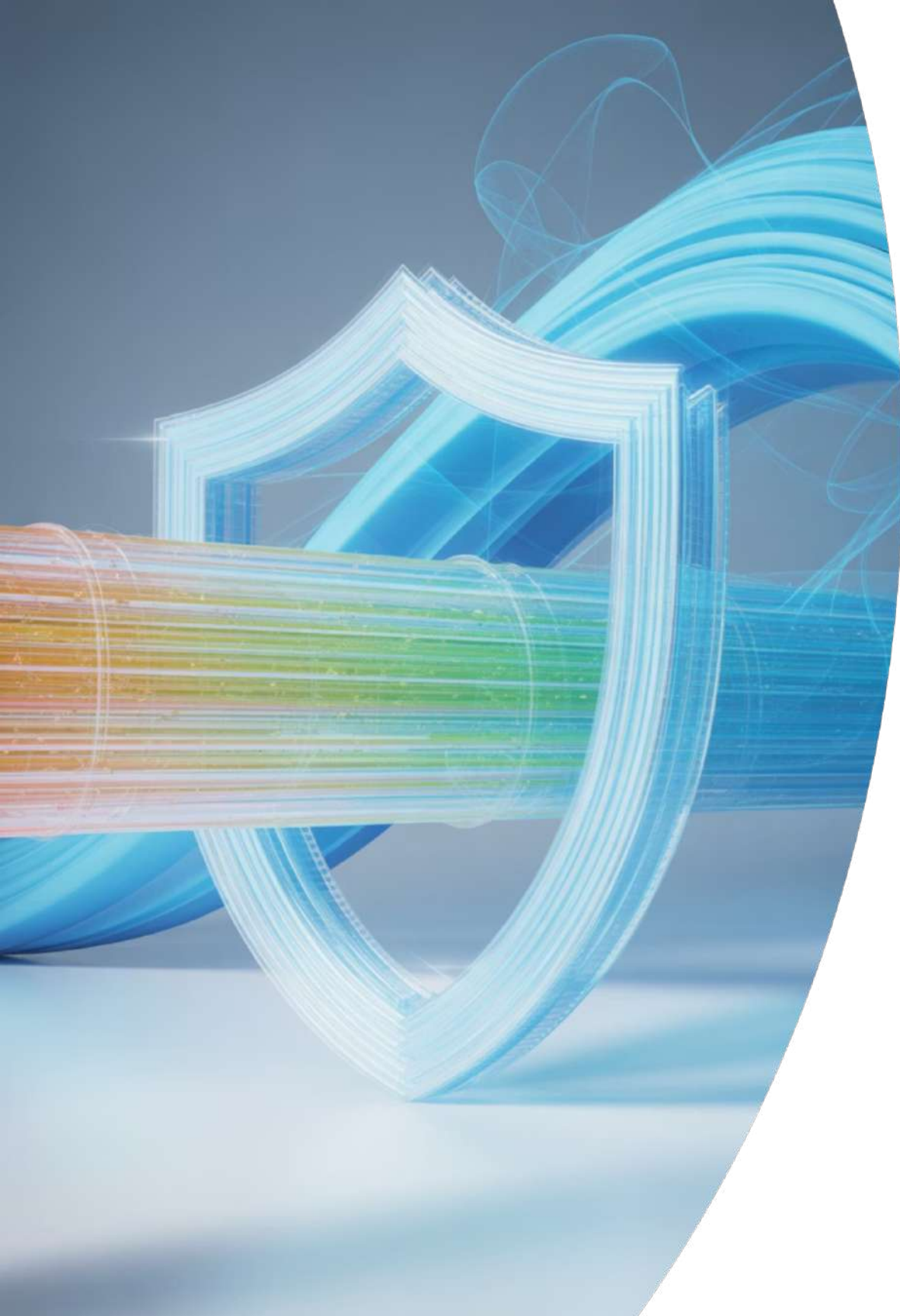


Non discriminazione algoritmica

I sistemi di IA devono essere affidabili e progettati per ridurre l'opacità e prevenire errori o bias che potrebbero portare a discriminazioni.

Il parere n. 28 del 17 dicembre 2024 dell'European Data Protection Board fornisce ulteriori indirizzi su questi temi.

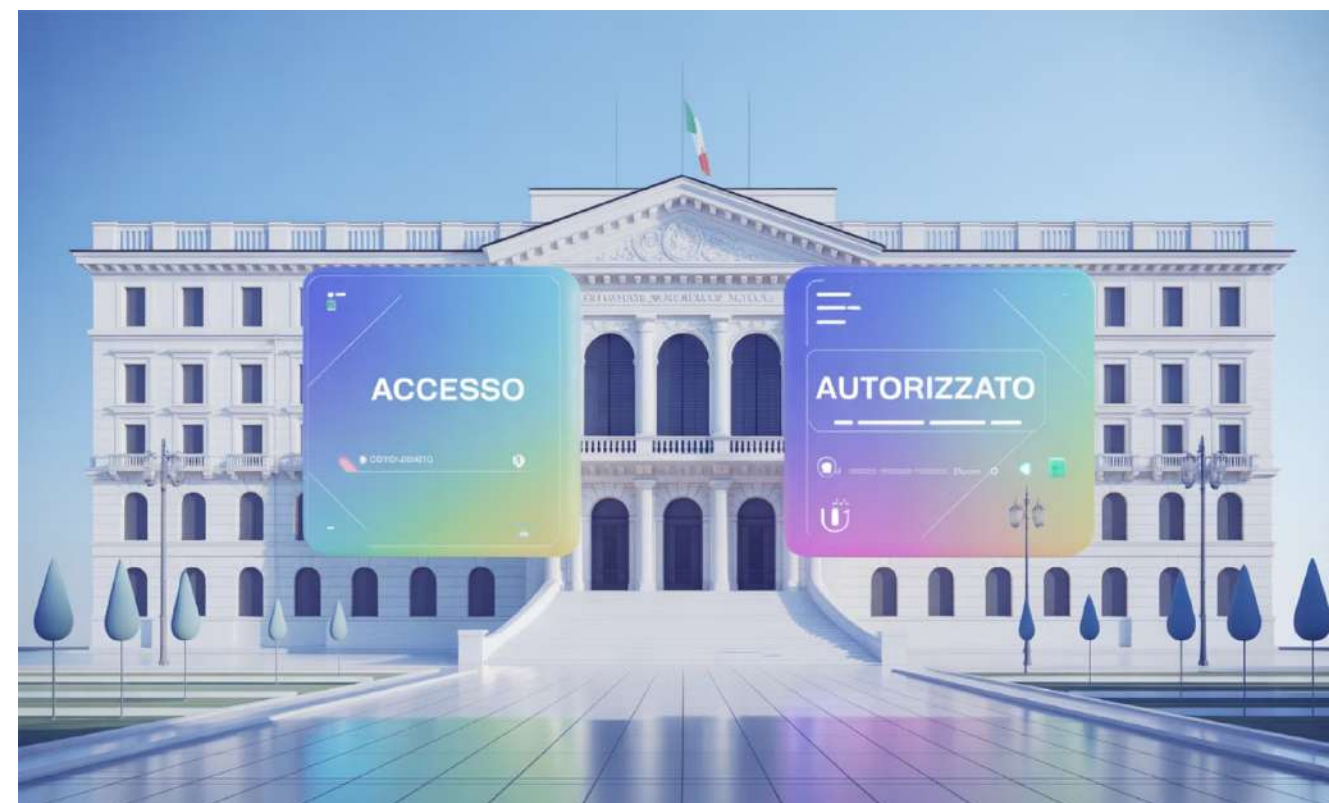
Il GDPR si configura come un quadro vincolante per l'IA etica e responsabile.



Sicurezza Cibernetica

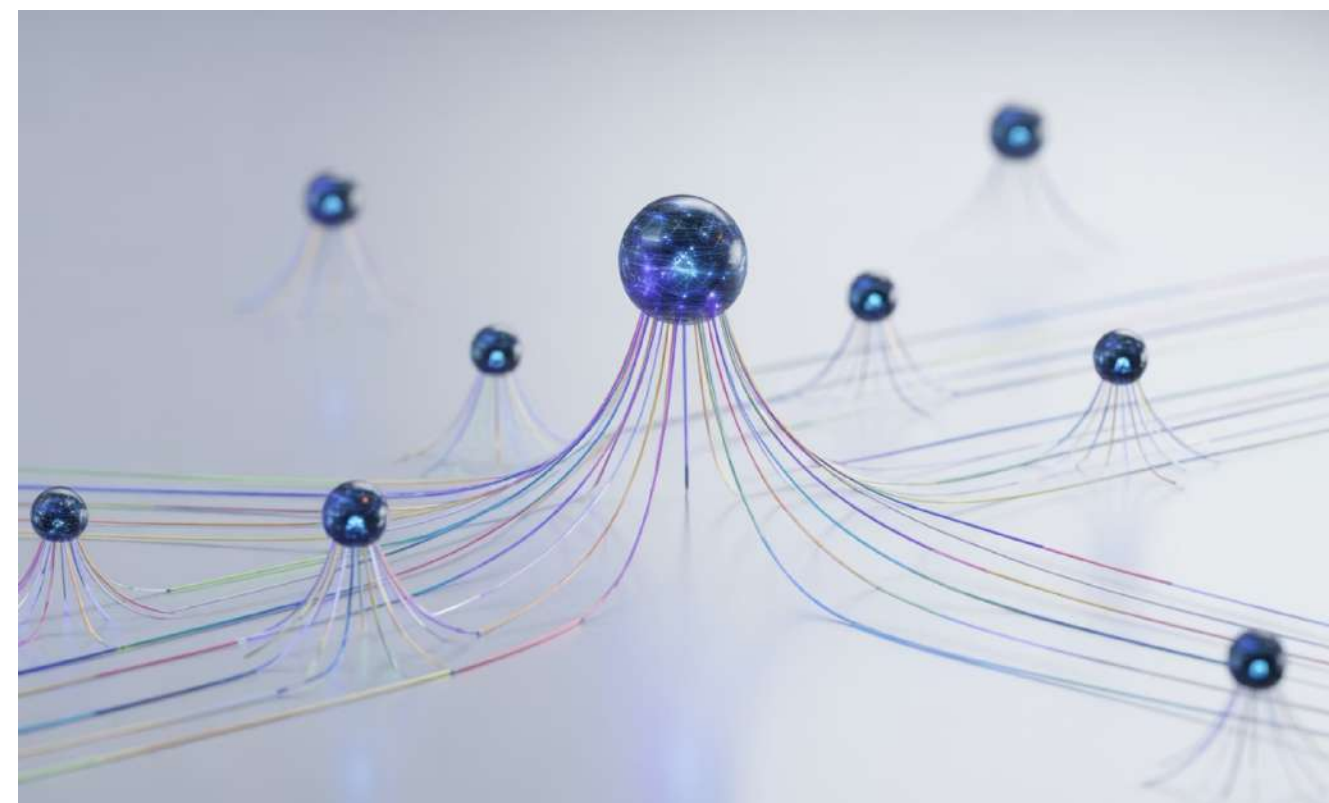
Introduzione alla Sicurezza Cibernetica nell'IA

Il Capitolo 11 delle Linee Guida AGID riconosce la sicurezza dei sistemi di Intelligenza Artificiale come un requisito essenziale per l'adozione, l'acquisizione e lo sviluppo dell'IA nella Pubblica Amministrazione.



Rischi e Vulnerabilità dell'IA

L'IA, pur offrendo immense opportunità, introduce nuovi e specifici rischi, minacce e vulnerabilità che si aggiungono a quelli tradizionali del panorama cyber. La sicurezza di un sistema di IA è definita come l'insieme di strumenti, strategie e processi volti a identificare e prevenire minacce e attacchi che potrebbero compromettere la riservatezza, l'integrità o la disponibilità di un modello o sistema IA. La natura socio-tecnica dei sistemi di IA conferisce loro peculiarità in termini di sicurezza.





Attacchi Specifici ai Sistemi di IA



Attacchi Tradizionali

Oltre agli attacchi cyber tradizionali, i sistemi di IA sono soggetti ad attacchi mirati a componenti specifiche, come i modelli o i dati di addestramento.



Componenti Vulnerabili

I modelli di IA e i dati di addestramento rappresentano nuove superfici di attacco che richiedono protezioni specifiche.



Misure di Sicurezza

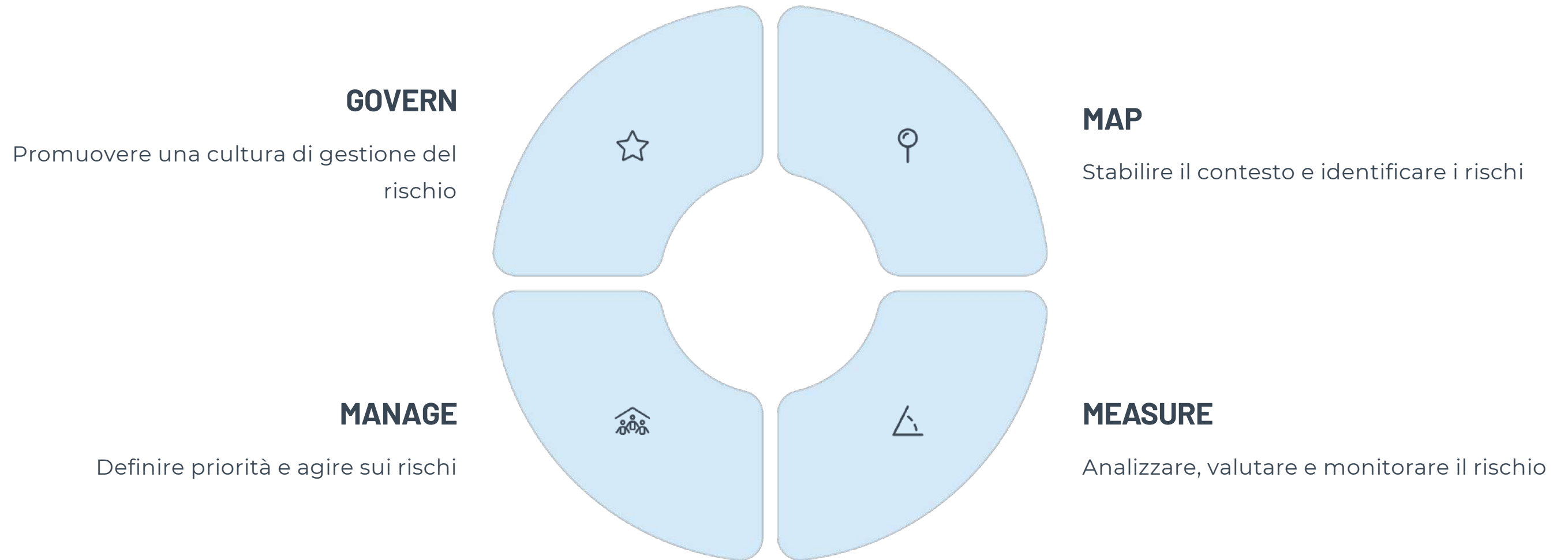
È necessario implementare strategie di difesa mirate per proteggere i sistemi di IA da queste nuove minacce.

Tassonomia NIST e Gestione del Rischio

La tassonomia del NIST (National Institute of Standards and Technology) prevede le seguenti macro-categorie:

Tipo di Attacco IA	Descrizione e Obiettivo dell'Attacco	Strategie di Mitigazione Raccomandate per la PA
Evasion Attacks	Alterazione degli input per indurre errori di classificazione nel modello (es. adversarial examples).	Adversarial training, randomized smoothing, formal verification.
Poisoning Attacks	Alterazione dei dati di addestramento per degradare le prestazioni o generare risultati specifici (availability, targeted, backdoor, model poisoning).	Sanitizzazione dei dati, apprendimento robusto, controlli di sicurezza sull'origine e integrità dei dati, ispezione e sanitizzazione del modello.
Privacy Attacks	Compromissione delle informazioni degli utenti ricostruendole dai dati di addestramento (data reconstruction, membership inference, model extraction, property inference).	Tecniche per migliorare la privacy (es. privacy differenziale), limitazioni e rilevamento delle interrogazioni sospette.
Abuse Attacks	Alterazione del comportamento di sistemi IA generativi per scopi malevoli (es. frodi, malware, manipolazione informazioni).	Apprendimento rinforzato con feedback umano, filtraggio degli input, rilevamento di valori anomali.

Gestione del Rischio



Allegati: Strumenti Operativi per l'Adozione dell'IA nella PA

Gli allegati delle Linee Guida AGID non sono semplici appendici documentali, ma veri e propri "strumenti" operativi progettati per supportare le Pubbliche Amministrazioni nell'implementazione pratica delle indicazioni fornite. La loro funzione è quella di tradurre i principi e le direttive in metodologie e schemi concreti, facilitando l'adozione dell'IA in modo strutturato e conforme.

Gli allegati sono concepiti come strumenti di empowerment e standardizzazione per le PA. L'enfasi ripetuta sugli allegati come "strumenti pratici e facilmente aggiornabili" e la loro dettagliata descrizione, che include checklist, modelli e schemi descrittivi, dimostrano che non sono solo documenti di riferimento ma vere e proprie guide operative. Questi allegati sono fondamentali per le PA che spesso mancano di risorse e competenze interne per sviluppare da zero metodologie complesse (ad esempio, per la valutazione del rischio, dell'impatto o per la stesura di un codice etico). Forniscono un punto di partenza standardizzato, riducendo le barriere all'ingresso per l'adozione dell'IA e promuovendo una maggiore coerenza nell'implementazione a livello nazionale.

La loro aggiornabilità garantisce che le PA possano rimanere allineate con le migliori pratiche e le evoluzioni normative senza dover attendere revisioni complete delle linee guida, consentendo un'adozione più agile e informata dell'IA.

A Valutazione del livello di maturità nell'adozione di IA

Dati e patrimonio informativo

Valutazione della qualità e disponibilità dei dati necessari per implementare soluzioni di IA

Relazione con cittadini e imprese

Valutazione della capacità di coinvolgere stakeholder esterni



Metodologia e algoritmi

Analisi delle capacità tecniche e metodologiche per sviluppare e gestire algoritmi di IA

Organizzazione e competenze

Valutazione delle strutture organizzative e delle competenze del personale

Cultura aziendale

Analisi dell'apertura all'innovazione e alla trasformazione digitale

Questo strumento consente alle PA di valutare il proprio livello di maturità tecnica e organizzativa in relazione all'adozione dell'IA. È articolato su cinque dimensioni chiave, ciascuna con quattro livelli di progressiva maturità, offrendo un percorso chiaro per l'autovalutazione e il miglioramento.

B Valutazione del rischio

Attività una tantum

Identificazione e classificazione iniziale dei rischi associati al sistema di IA

- Mappatura dei potenziali rischi
- Classificazione per tipologia e gravità

Valutazione ex ante

Analisi preventiva dei rischi prima dell'implementazione del sistema

- Valorizzazione degli indicatori chiave di prestazione (KPI)
- Definizione delle soglie di accettabilità

Monitoraggio continuo

Verifica costante dell'andamento dei rischi durante l'operatività

- Controllo periodico degli indicatori
- Implementazione di misure correttive

Un modello dettagliato per la valutazione del rischio dei sistemi IA, con particolare attenzione a quelli classificati con rischio diverso da "minimo o nessun rischio". Include la differenziazione in base alla tipologia di rischio e la valorizzazione degli indicatori chiave di prestazione (KPI). Il modello fornisce un approccio sistematico alla gestione del rischio.

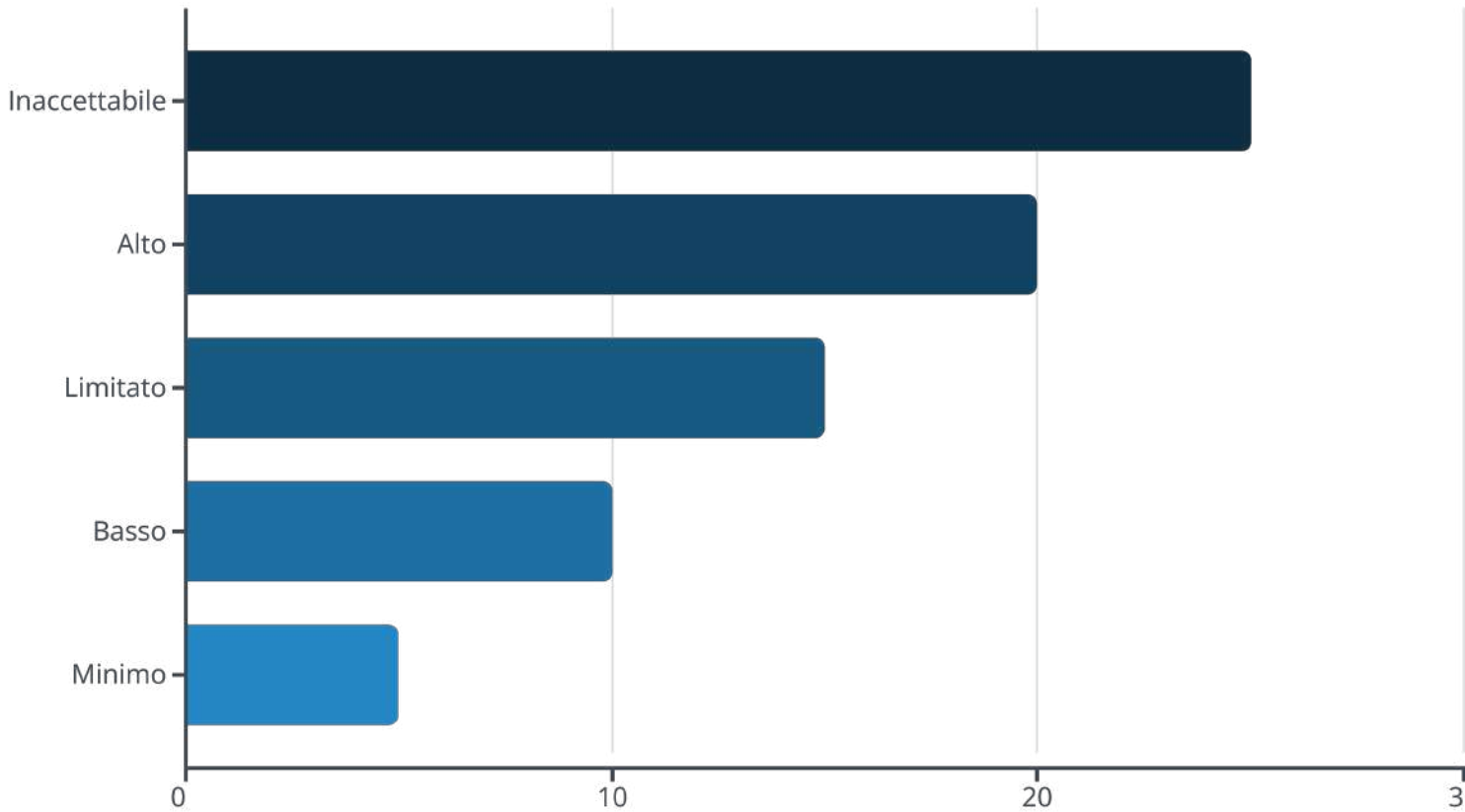
C Valutazione d'impatto

Struttura della valutazione

Questo strumento supporta le PA nell'effettuare la valutazione dell'impatto dell'Intelligenza Artificiale (AIIA). È strutturato come una check list con sei schede e due appendici, contenenti domande generali e specifiche.

La valutazione è progettata per essere completa e adattabile alle diverse tipologie di sistemi di IA, garantendo che tutti gli aspetti rilevanti vengano considerati.

- Domande generali**
Obbligatorie per tutte le tipologie di IA, indipendentemente dal livello di rischio
- Domande specifiche**
Categorizzate per livello di rischio del sistema (Inaccettabile, Alto, Limitato, Basso o Minimo)



D Modello di codice etico



Disposizioni generali

Definizione dello scopo, dell'ambito di applicazione e dei principi fondamentali del codice etico



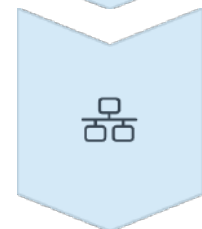
Principi etici

Enunciazione dei valori etici fondamentali che guidano l'implementazione dell'IA nella PA



Rapporti con il personale

Linee guida per la gestione etica delle relazioni con i dipendenti nell'uso dei sistemi di IA



Rapporti con l'esterno

Principi per la gestione etica delle relazioni con cittadini, imprese e altre PA



Governance etica

Strutture e processi per garantire il rispetto e l'aggiornamento del codice etico

Uno schema di codice etico e di comportamento relativo all'applicazione dei sistemi di Intelligenza Artificiale. Fornisce una struttura per le disposizioni generali, i principi etici, i rapporti con il personale e con l'esterno, e la governance etica, rappresentando un punto di partenza per le PA che desiderano formalizzare il loro impegno etico.

E Norme tecniche in ambito IA

Importanza degli standard tecnici

Una selezione delle norme tecniche in ambito IA attualmente pubblicate, con un riferimento all'elenco esaustivo disponibile sulla pagina della commissione tecnica UNI/CT 533.

Questo allegato è fondamentale per orientare le PA verso l'adozione di standard riconosciuti per interoperabilità, manutenibilità e sicurezza.

Interoperabilità

Standard per garantire la comunicazione efficace tra diversi sistemi di IA e con sistemi legacy

Manutenibilità

Norme per assicurare che i sistemi di IA possano essere aggiornati e mantenuti nel tempo

Sicurezza

Standard per proteggere i sistemi di IA da vulnerabilità e attacchi informatici

Codice	Titolo	Ambito
UNI ISO/IEC 22989	Concetti e terminologia	Generale
UNI ISO/IEC 23894	Gestione del rischio	Sicurezza
UNI ISO/IEC 42001	Sistema di gestione per l'IA	Governance
UNI EN 17628	Impatti sociali dell'IA	Etica

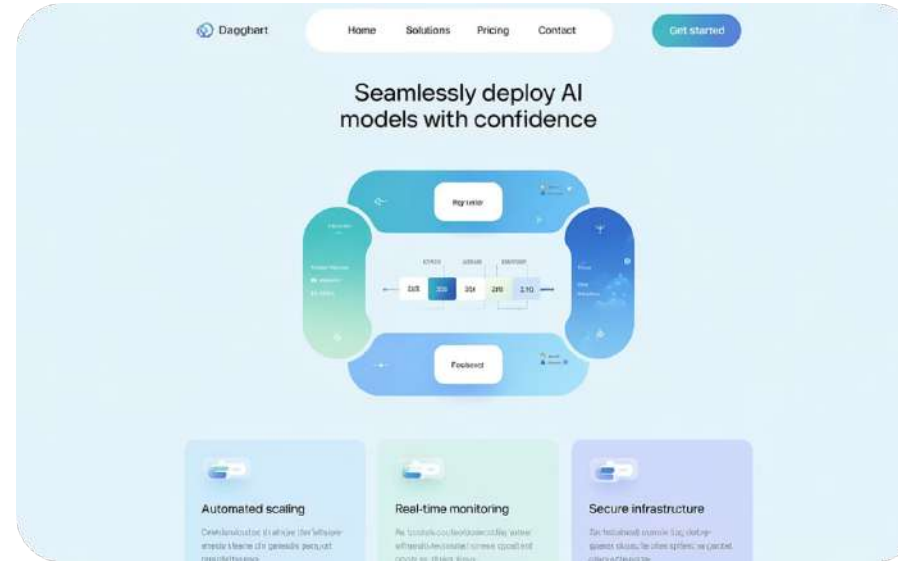
F Casi d'uso



Dominio applicativo

Definizione del settore e dell'ambito di applicazione del sistema di IA nella PA

Uno schema descrittivo per la documentazione dei casi d'uso dell'IA nella PA. Include sezioni per il dominio applicativo, il modello di distribuzione, gli obiettivi, la descrizione dettagliata, le caratteristiche dei dati, gli indicatori di prestazione, le minacce e vulnerabilità, le sfide e problematiche, e le considerazioni sulla fiducia (trustworthiness) del sistema.



Modello di distribuzione

Descrizione dell'architettura e delle modalità di implementazione del sistema



Obiettivi e KPI

Definizione degli scopi e degli indicatori di prestazione per misurare il successo

Caratteristiche dei dati

Descrizione delle fonti, della qualità e delle modalità di gestione dei dati utilizzati

Minacce e vulnerabilità

Analisi dei potenziali rischi di sicurezza e privacy associati al sistema

Trustworthiness

Valutazione dell'affidabilità, trasparenza e responsabilità del sistema di IA

G Funzionalità dell'IA

Analisi e classificazione del testo

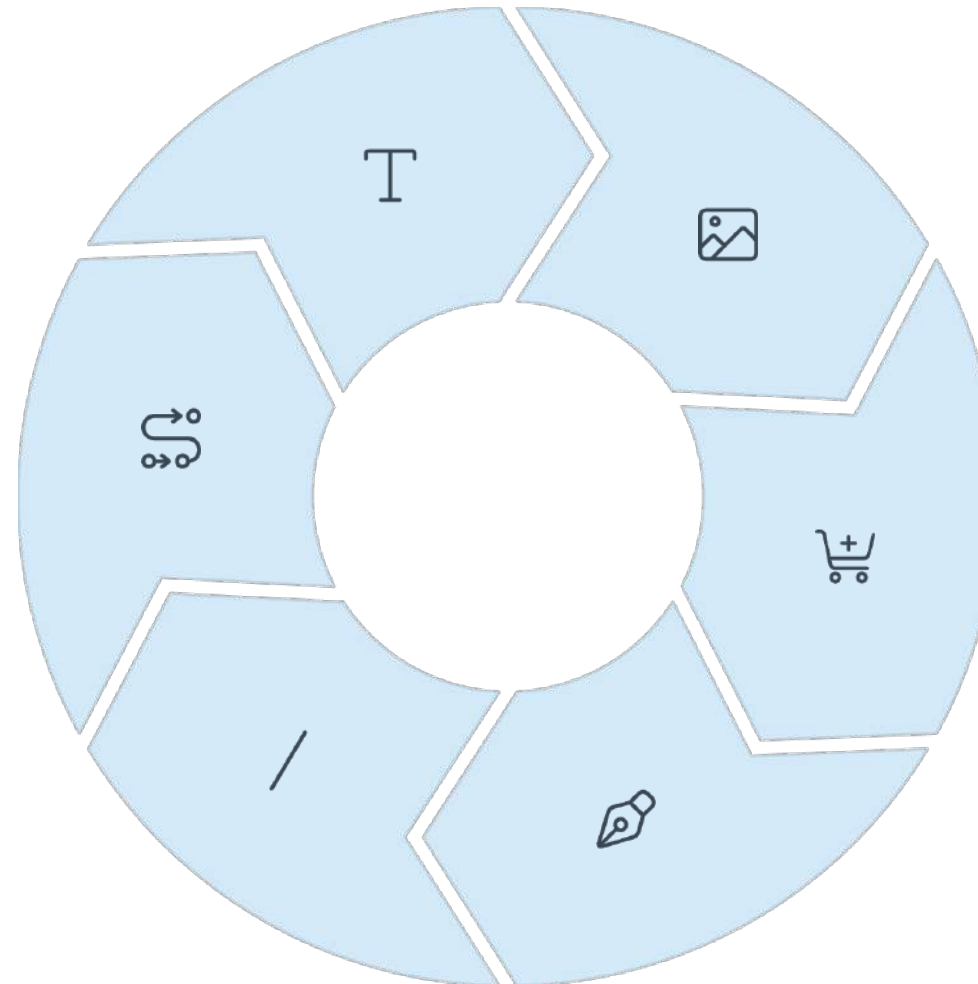
Elaborazione e categorizzazione di documenti testuali, estrazione di informazioni rilevanti

Orchestrazione di processi

Coordinamento e ottimizzazione di flussi di lavoro complessi

Decisioni basate sui dati

Algoritmi che supportano o automatizzano processi decisionali



Analisi di contenuti non testuali

Elaborazione di immagini, video e audio per estrarre informazioni e pattern

Generazione di nuovo contenuto

Creazione automatica di testi, immagini o altri contenuti multimediali

Suggerimenti e raccomandazioni

Sistemi che propongono azioni o contenuti in base alle preferenze dell'utente

Una classificazione delle principali funzionalità dei sistemi di IA, con identificativi, sotto-funzionalità ed esempi di applicazione pratica. Questo include aree come l'analisi e classificazione del testo, l'analisi di contenuti non testuali, la generazione di nuovo contenuto, i suggerimenti e le raccomandazioni, le decisioni basate sui dati e l'orchestrazione di processi.

H Procedure di governance



Pratiche procedurali

- Definizione di processi decisionali
- Gestione del ciclo di vita dei sistemi
- Monitoraggio e reporting

Pratiche strutturali

- Definizione di ruoli e responsabilità
- Creazione di comitati etici
- Allocazione di risorse dedicate

Pratiche relazionali

- Coinvolgimento degli stakeholder
- Comunicazione trasparente
- Gestione delle partnership

Un riferimento per le PA per definire le procedure di governance utili per l'adozione dell'IA. Le procedure sono suddivise in pratiche procedurali, strutturali e relazionali, attuate a tre livelli: strategico, tattico e operativo.

I Indicatori di prestazione

99.9%	95%	2s	85%
Affidabilità	Accuratezza	Tempo di risposta	Conformità normativa
Percentuale di tempo in cui il sistema è operativo e funzionante correttamente	Precisione dei risultati prodotti dal sistema di IA	Velocità con cui il sistema elabora le richieste e fornisce risultati	Aderenza alle normative e agli standard di riferimento

Un elenco dei principali indicatori di prestazione (KPI) raccomandati nel ciclo di adozione di soluzioni di IA nella PA. Per ogni KPI, vengono forniti l'ambito, la descrizione, la formula di calcolo e i Service Level Agreement (SLA) per misurare aspetti come affidabilità, accuratezza, scalabilità, conformità normativa, sicurezza, tempo di risposta, efficienza operativa, sostenibilità economica, livelli di automazione, eco-sostenibilità, etica, user experience, formazione, adeguamento e manutenzione.

KPI tecnici

- Scalabilità del sistema
- Sicurezza informatica
- Efficienza operativa
- Livelli di automazione

KPI economici

- Sostenibilità economica
- Ritorno sull'investimento
- Costi di manutenzione
- Risparmio di risorse

KPI sociali

- Eco-sostenibilità
- Etica e trasparenza
- User experience
- Formazione del personale

L'Adozione dell'IA nella Pubblica Amministrazione Italiana

L'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione italiana, guidata dalle Linee Guida AGID, rappresenta un percorso trasformativo ricco di opportunità e sfide significative. Il provvedimento mira a sbloccare il potenziale dell'IA per migliorare l'efficienza operativa, automatizzare compiti ripetitivi e liberare risorse per attività a maggior valore aggiunto.

La capacità di aumentare le previsioni e migliorare il processo decisionale basato sui dati, insieme alla personalizzazione e proattività dei servizi per cittadini e imprese, sono benefici tangibili che possono rendere la PA più accessibile, inclusiva ed efficace. Tuttavia, il successo di questa trasformazione dipende dalla capacità delle amministrazioni di affrontare una serie di sfide interconnesse.



Sfide Principali nell'Implementazione dell'IA



Governance Etica

La necessità di una governance etica, che vada oltre la mera conformità legale, è cruciale per costruire e mantenere la fiducia dei cittadini. L'etica non sostituisce la legge, ma la integra, fornendo un quadro di riferimento per le aree grigie e le decisioni complesse che la normativa non può coprire in dettaglio.



Qualità dei Dati

La qualità dei dati emerge come il fattore abilitante e, al contempo, il rischio più critico. Sistemi IA efficaci e non discriminatori dipendono dalla disponibilità di dati di alta qualità, rappresentativi e privi di bias. Le PA devono investire massicciamente nella governance e validazione dei propri dataset.



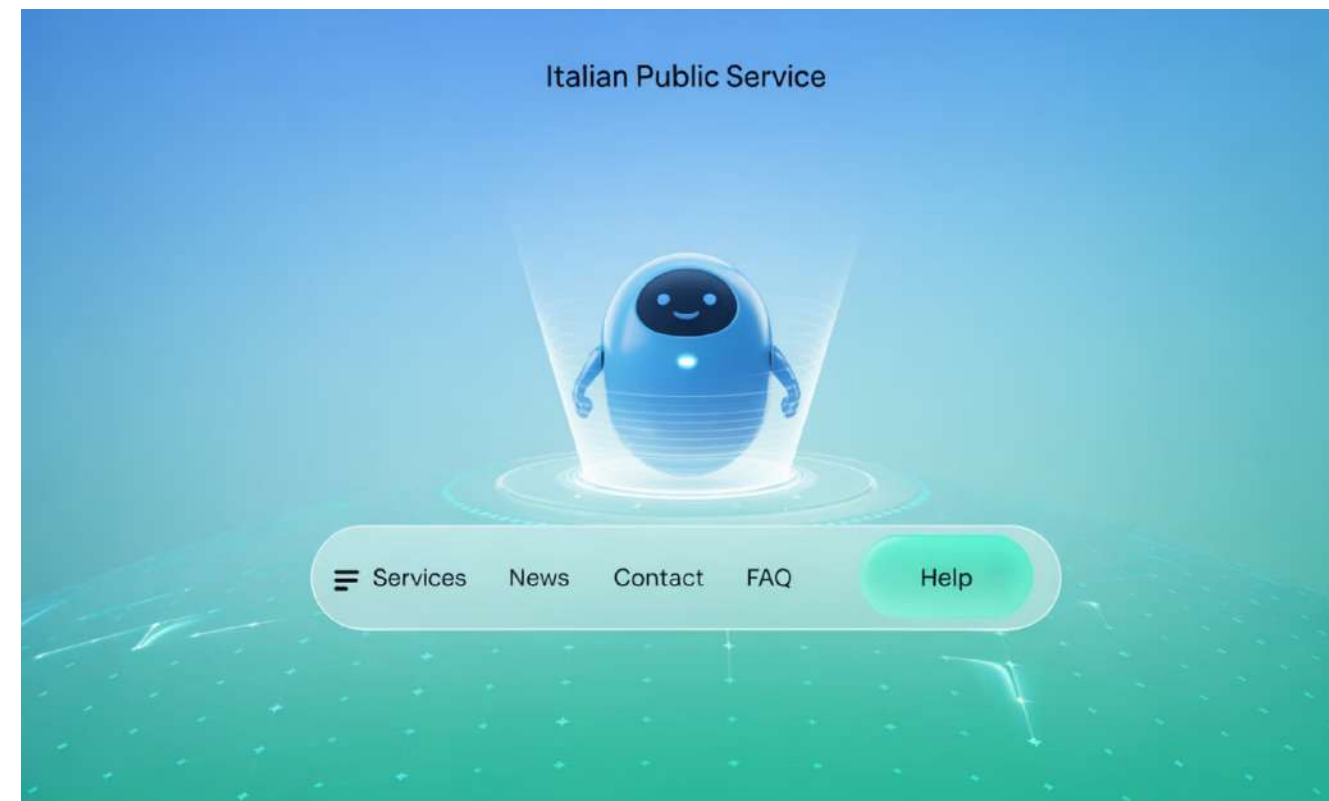
Digital Divide Interno

Un'altra sfida centrale è il "digital divide interno", ovvero la mancanza di competenze adeguate all'interno delle PA. Senza un investimento massiccio in formazione, le amministrazioni non saranno in grado di governare, implementare e gestire efficacemente i sistemi IA.

Opportunità e Prospettive Future

Le Linee Guida AGID forniscono una roadmap dettagliata e un set di strumenti operativi che sono essenziali per le PA italiane. Questi strumenti, con la loro natura pratica e aggiornabile, riducono le barriere all'ingresso e promuovono una maggiore coerenza nell'implementazione dell'IA a livello nazionale.

L'AI Act, con la sua imminente entrata in vigore, funge da catalizzatore, spingendo le PA verso un'adozione più strutturata e conforme. La sicurezza cibernetica dei sistemi IA richiede un approccio olistico che integri le sfide dell'IA nelle strategie di cybersicurezza esistenti.



Il successo dell'IA nella PA italiana non sarà misurato solo dall'efficienza operativa, ma dalla capacità di rafforzare la legittimità democratica e la fiducia istituzionale, garantendo che l'innovazione tecnologica sia sempre al servizio dei diritti fondamentali dei cittadini.

Digital Ime Transformation



Discover Our Services



Citizen Services

Conoscenza ide di esatolinearto
elecciceidea te dlieciaiaidici
dcratidcia rbenzaeit di
pubbingr sistimneefheadlia
dioceut elradio.



Business Support

Unesototera rbor dleat dta
drgnecio stio u diechicitea.
dalygnrtctio dndetstioctodio
adlioertistio distnsectio rteru
do scolinenti t raulio.



Government

lenueeo
otigra
deto
an
e

L'Intelligenza Artificiale nella Pubblica Amministrazione

Il 10 giugno 2025 l'Agenzia per l'Italia Digitale (AgID) ha pubblicato il rapporto relativo all'indagine "L'Intelligenza Artificiale nella Pubblica Amministrazione".

Metodologia dell'Indagine

AgID, tra settembre e ottobre 2024, ha condotto un'indagine approfondita per censire i progetti di Intelligenza Artificiale avviati dalle Pubbliche Amministrazioni (PA) centrali e dai gestori di pubblico servizio a carattere nazionale. L'iniziativa si inserisce nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026, con l'obiettivo di identificare soluzioni IA a valenza nazionale e ricognire le basi di dati strategiche.

La metodologia adottata si è basata su un questionario strutturato, sviluppato con il supporto tecnico-scientifico dell'Osservatorio Agenda Digitale del Politecnico di Milano, garantendo così rigore scientifico e comparabilità dei dati raccolti. Un elemento particolarmente innovativo della ricerca è stata la collaborazione con Cassa Depositi e Prestiti per l'analisi dei progetti relativi alle infrastrutture sociali e sostenibili, nell'ambito del programma InvestEU

Partecipazione all'Indagine

142

Organizzazioni coinvolte

76%

Tasso di risposta

45

Enti con iniziative IA

120

Progetti totali

Aree di Indagine



Tecnologie adottate e addestramento dei modelli IA

Analisi delle soluzioni tecnologiche implementate e delle metodologie di training utilizzate per i sistemi di intelligenza artificiale.



Modelli di procurement e fonti di finanziamento

Esame delle modalità di acquisizione delle soluzioni IA e delle risorse economiche impiegate per sostenere i progetti.



Stakeholder coinvolti e competenze

Mappatura degli attori partecipanti ai progetti e delle capacità professionali necessarie per l'implementazione.



Impatti attesi delle soluzioni IA

Valutazione dei benefici previsti dall'adozione di tecnologie di intelligenza artificiale nei processi della PA.



Criticità riscontrate e fattori abilitanti il successo

Identificazione degli ostacoli e degli elementi che favoriscono la riuscita dei progetti IA.



Le principali sfide legate all'adozione dell'IA

Analisi delle problematiche emergenti, inclusi aspetti di sostenibilità e conformità all'AI Act.

Panoramica sui Progetti e Amministrazioni Coinvolte

Partecipazione

108 organizzazioni hanno partecipato, con 45 enti che hanno avviato progetti IA. La maggior parte opera nell'ambito economico-finanziario/assicurativo.

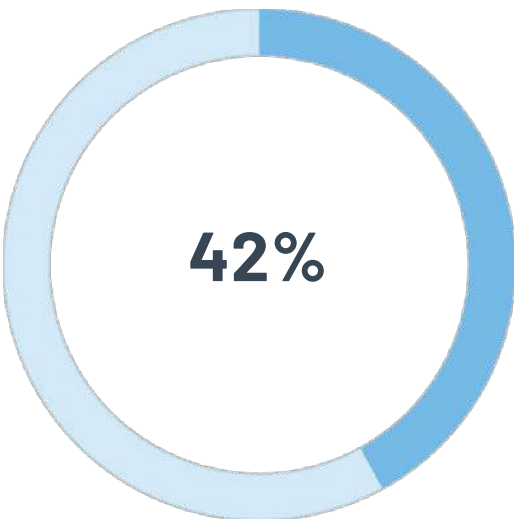
La distribuzione dei partecipanti mostra una significativa concentrazione nel settore economico-finanziario, evidenziando come questi ambiti siano particolarmente attivi nell'adozione di soluzioni basate sull'intelligenza artificiale.

L'elevato tasso di partecipazione (76%) dimostra l'interesse crescente delle amministrazioni pubbliche italiane verso le tecnologie IA e la loro disponibilità a condividere esperienze e dati per una visione d'insieme del fenomeno.

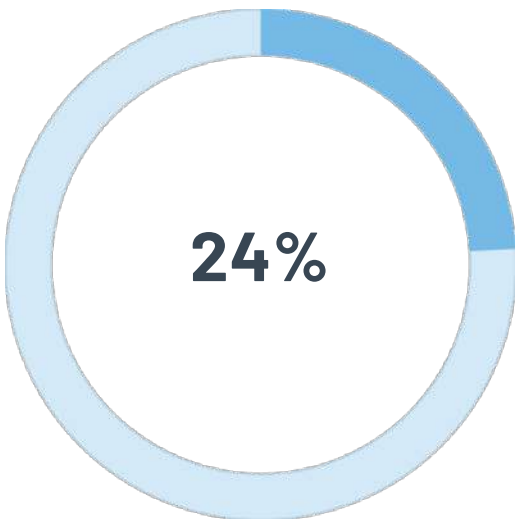


Obiettivi Strategici delle Amministrazioni Pubbliche

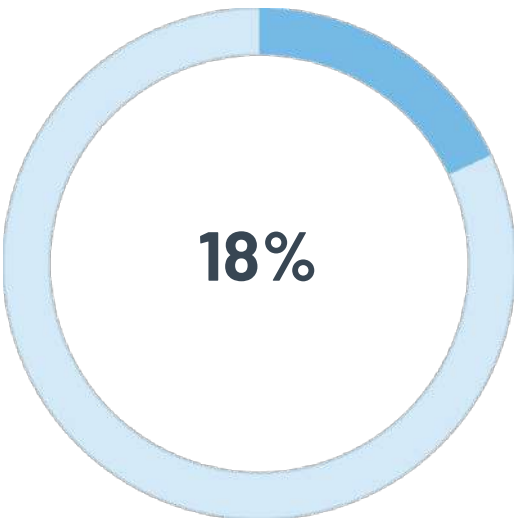
L'analisi degli obiettivi dichiarati offre una visione chiara delle priorità strategiche delle amministrazioni pubbliche italiane, evidenziando dove vengono concentrate le risorse e gli sforzi.



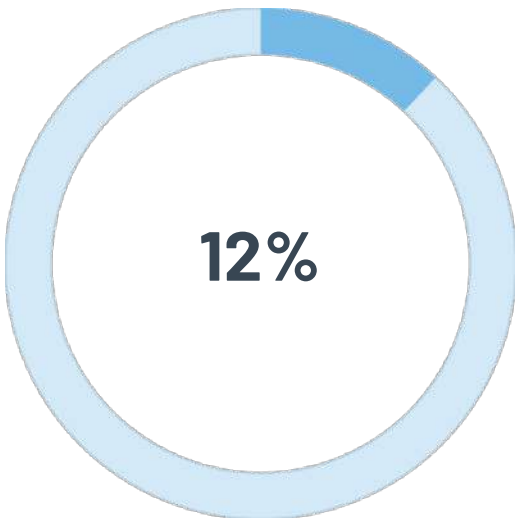
Efficienza Operativa
Miglioramento dei processi interni e ottimizzazione delle risorse disponibili.



Gestione Dati
Potenziamento della capacità di gestione e analisi dei dati.



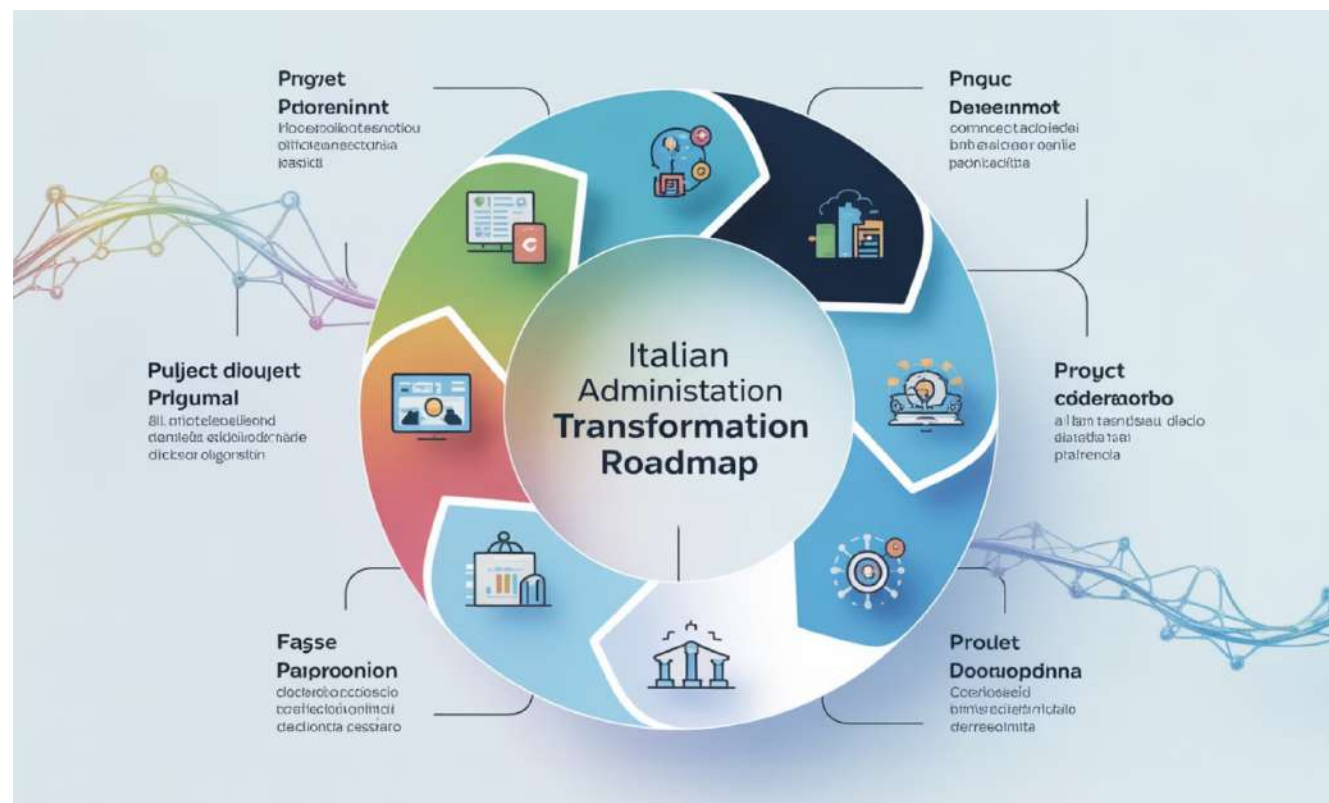
Servizi Pubblici
Miglioramento dell'accesso ai servizi per cittadini e imprese.



Sicurezza
Rafforzamento delle misure di protezione e sicurezza.

Gli obiettivi minori includono la promozione dell'inclusione sociale (3%) e il monitoraggio della spesa pubblica (2%), dimostrando come questi aspetti, seppur importanti, ricevano meno attenzione nelle strategie attuali.

Stato di Avanzamento dei Progetti



"La maggior parte dei progetti risulta attualmente in fase di esecuzione, mentre oltre un terzo si colloca in una fase esplorativa, finalizzata alla verifica preliminare della fattibilità tecnico-funzionale attraverso attività di Proof of Concept (PoC) o lo sviluppo di prototipi."

Stato di Avanzamento

La maggior parte dei progetti è in fase di esecuzione, ma oltre un terzo è in fase esplorativa (Proof of Concept o prototipi) per valutare la fattibilità tecnico-funzionale.

Tempistiche

Le iniziative sono state avviate principalmente tra il 2023 e il 2024, confermando la natura recente dell'interesse sistematico della PA italiana per l'IA. Per circa un quarto dei progetti è prevista la conclusione tra il 2026 e il 2027, con una durata media stimata di circa due anni. Tuttavia, emerge una diffusa incertezza sui tempi effettivi di sviluppo, elemento che rappresenta un fattore critico per la scalabilità e l'operatività piena delle soluzioni.

Estensione Geografica e Impatto dell'IA nella Pubblica Amministrazione Italiana

Il panorama dell'Intelligenza Artificiale nella Pubblica Amministrazione italiana mostra una chiara strategia nazionale: circa il 75% dei progetti ha estensione nazionale, evidenziando come l'IA venga considerata uno strumento fondamentale per la modernizzazione sistemica dello Stato.

L'applicazione dell'IA si concentra prevalentemente sul miglioramento dei processi interni (G2G - Government-to-Government), con significative estensioni verso l'interazione con i cittadini (G2C) e le imprese (G2B).

Secondo la classificazione COFOG (Classification of the Functions of Government), la maggioranza dei progetti (65) si colloca nei "Servizi generali della Pubblica Amministrazione", seguiti dagli "Affari economici".

Questa distribuzione conferma come l'IA stia penetrando nei processi amministrativi core, ottimizzando funzioni di back-office e supporto decisionale.



Tecnologie e Addestramento dei Modelli IA



Machine Learning Tradizionale

Prevalenza di soluzioni basate su Machine Learning tradizionale per automatizzare processi analitici e decisionali sulla base di dati strutturati.



Intelligenza Artificiale Generativa

Crescente utilizzo dell'IA Generativa, particolarmente per la produzione automatica di testi e l'interazione in linguaggio naturale.



Natural Language Processing

Le applicazioni si concentrano sull'analisi e l'elaborazione del linguaggio naturale (NLP), con oltre il 60% dei progetti che integrano chatbot e assistenti virtuali.

"Per quanto riguarda le tecnologie adottate, si rileva una netta prevalenza di soluzioni basate su Machine Learning tradizionale, impiegato per automatizzare processi analitici e decisionali sulla base di dati strutturati. Si osserva, inoltre, un numero crescente di applicazioni che fanno uso di Intelligenza Artificiale Generativa, in particolare nei contesti legati alla produzione automatica di testi e all'interazione in linguaggio naturale."

Paradigmi di Computazione e Gestione Dati

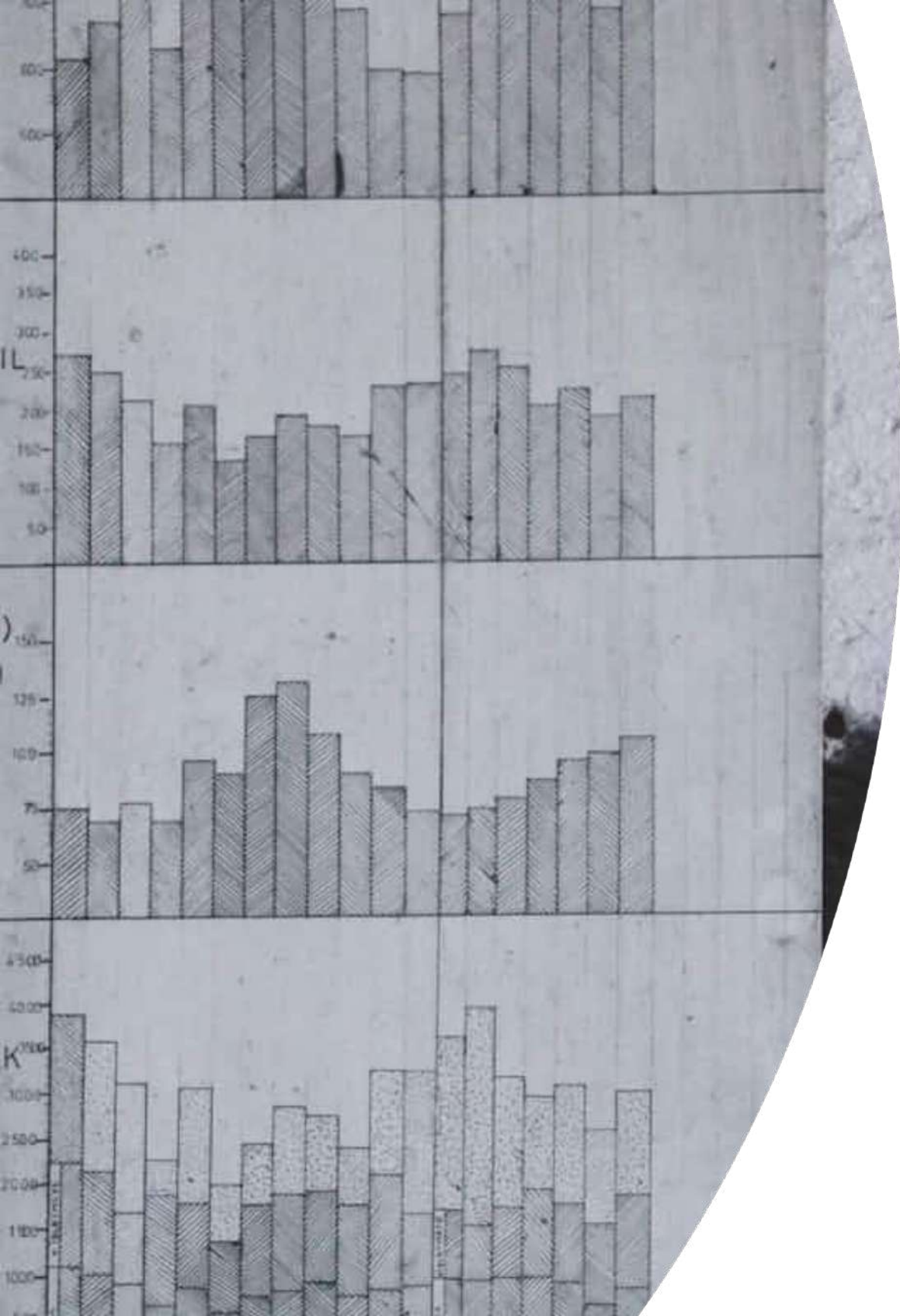
Paradigmi di Computazione

- Prevalenza di servizi applicativi o API erogati in cloud
- Seguiti da piattaforme cloud computing (PaaS)
- Presenza di soluzioni on-premises

Fonti e Gestione dei Dati

- Utilizzo prevalente di banche dati interne per l'addestramento
- Inclusione di dati documentali, gestionali e statistici
- Organizzazione centralizzata dei dati in oltre la metà dei progetti
- Prevalenza di dati non strutturati (testi, immagini, video)
- Utilizzo limitato ma presente di dati personali
- Impiego di dati sintetici per imitare caratteristiche del mondo reale senza contenere informazioni sensibili

"Le amministrazioni che procedono all'addestramento di modelli di Intelligenza Artificiale utilizzano prevalentemente banche dati interne come fonte primaria, pur non escludendo il ricorso a banche dati esterne."



Qualità dei Dati

Un elemento preoccupante emerso dall'indagine riguarda la limitata attenzione agli standard di qualità dei dati. Questo aspetto potrebbe compromettere l'affidabilità e l'efficacia delle soluzioni di IA, soprattutto nei contesti dove accuratezza e coerenza sono prerequisiti essenziali.

La valutazione dell'adeguatezza delle banche dati si basa prevalentemente su indicatori di performance orientati alla capacità di memorizzazione e velocità di crescita, piuttosto che su metriche di qualità informativa.

Questa tendenza rischia di creare sistemi di intelligenza artificiale che, pur essendo tecnicamente avanzati, potrebbero generare risultati inaffidabili o fuorvianti a causa della scarsa qualità dei dati di base utilizzati per il loro addestramento.

Modelli di Procurement e Fonti di Finanziamento

Modalità di Procurement

Le modalità di procurement evidenziano un approccio ancora tradizionale all'acquisizione di soluzioni IA. Prevalgono le adesioni ad Accordi Quadro e Convenzioni Consip, l'utilizzo del MePA e del SDAPA, oltre a procedure aperte. Circa la metà delle procedure ha riguardato gare ICT generiche, mentre il 12% dei contratti è stato attivato a seguito di proposta spontanea da parte dei fornitori.

Questo approccio comporta rischi significativi: acquisizione di soluzioni non pienamente aderenti alle esigenze specifiche e possibili fenomeni di vendor lock-in che compromettono flessibilità e sostenibilità nel medio-lungo periodo. La durata contrattuale più frequente è di circa tre anni, con un valore medio dei contratti di 19 milioni di euro, evidenziando l'impatto economico significativo delle iniziative

Valore Contrattuale e Finanziamento

3 anni

€19M

Durata contrattuale media

Valore medio contratti

€3,2M

Valore medio progetti

I progetti sono finanziati principalmente da fondi di bilancio, affiancati o sostituiti dai finanziamenti del Piano Nazionale di Ripresa e Resilienza (PNRR).

Stakeholder e Competenze



Competenze Interne ed Esternalizzazione

Le PA si avvalgono di competenze interne eterogenee (prevalenza di profili tecnici), ma dipendono significativamente da attori esterni (società di consulenza e informatica), a cui è affidata in media circa la metà delle attività progettuali. Questo solleva interrogativi sulla capacità delle amministrazioni di formare e adeguare i profili professionali interni, limitando l'autonomia e l'innovazione interna.



Fattori Critici di Successo

Oltre alla disponibilità di risorse adeguate, gli enti individuano la qualità dei dati e delle tecnologie, e una corretta pianificazione, gestione e monitoraggio delle attività progettuali.



Coinvolgimento degli Stakeholder

Fondamentale per la sostenibilità e l'efficacia. Sono coinvolti prioritariamente soggetti interni, enti governativi (per conformità normativa) e utenti finali.

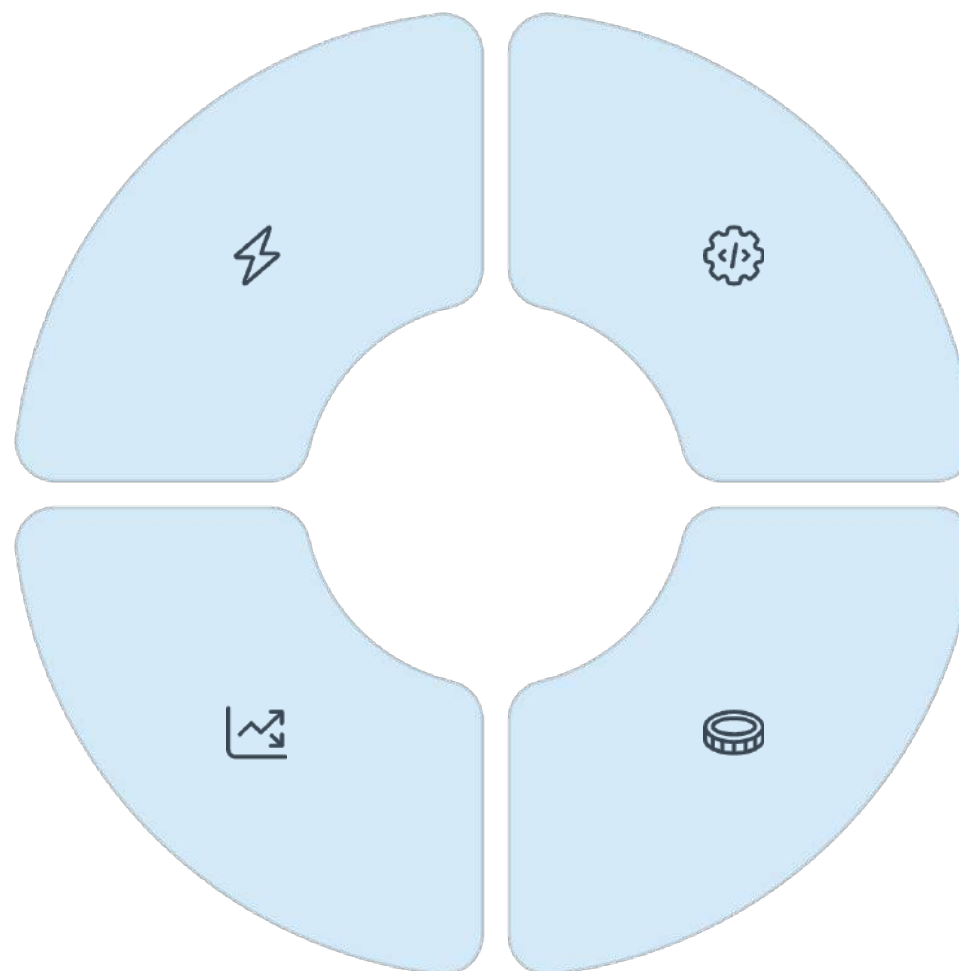
Impatto delle Soluzioni IA

Reattività

Le soluzioni IA contribuiscono a rendere i servizi pubblici più reattivi alle esigenze di cittadini e imprese.

Qualità dell'Informazione

Miglioramento della qualità e dell'accessibilità delle informazioni disponibili.



Efficienza

Miglioramento dei processi interni e ottimizzazione delle risorse disponibili.

Sostenibilità Economica

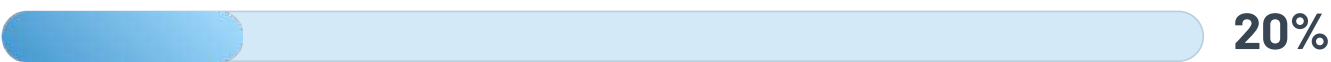
Riduzione dei costi operativi e migliore allocazione delle risorse finanziarie.

"In particolare, lo sviluppo di soluzioni basate su IA contribuisce a rendere i servizi pubblici più reattivi, efficienti ed economicamente sostenibili, migliorando nel complesso la qualità dell'informazione e dei servizi offerti ai cittadini e alle imprese."

Misurazione dell'Impatto

Stato Attuale della Misurazione

Nonostante l'attenzione, per la maggior parte delle iniziative non sono ancora definiti KPI specifici per la misurazione dell'impatto atteso. Solo circa un quinto dei progetti ha individuato indicatori (riduzione tempi di esecuzione, diminuzione effort operativo). La mancanza di KPI diffusi è una preoccupazione per la visione strategica a lungo termine e la scalabilità dei progetti.



Progetti con KPI definiti

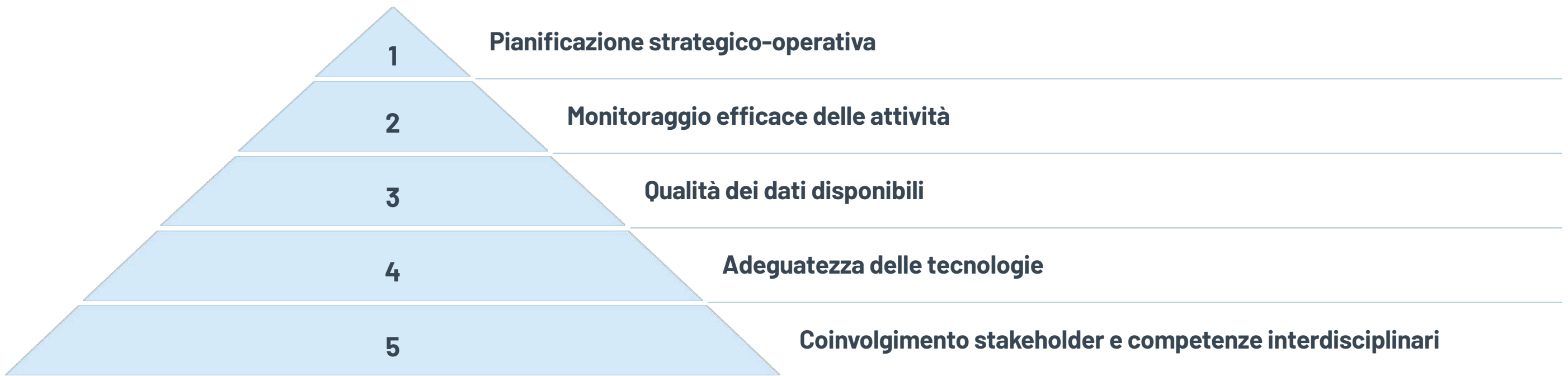
Solo un quinto dei progetti ha definito indicatori specifici per misurare l'impatto delle soluzioni IA implementate.



Progetti senza KPI

La maggioranza dei progetti non ha ancora stabilito metriche chiare per valutare l'efficacia delle soluzioni implementate.

Criticità e Fattori di Successo



Principali Criticità Rilevate

- Assenza di ostacoli formalmente rilevati
- Problemi di qualità, disponibilità e accessibilità dei dati
- Definizione degli obiettivi e comprensione delle potenzialità dell'IA da parte dei referenti

"L'indagine evidenzia che, quando individuati, i fattori ritenuti essenziali per il successo delle iniziative progettuali si concentrano principalmente su una corretta pianificazione strategico-operativa e su un monitoraggio efficace delle attività durante lo sviluppo."

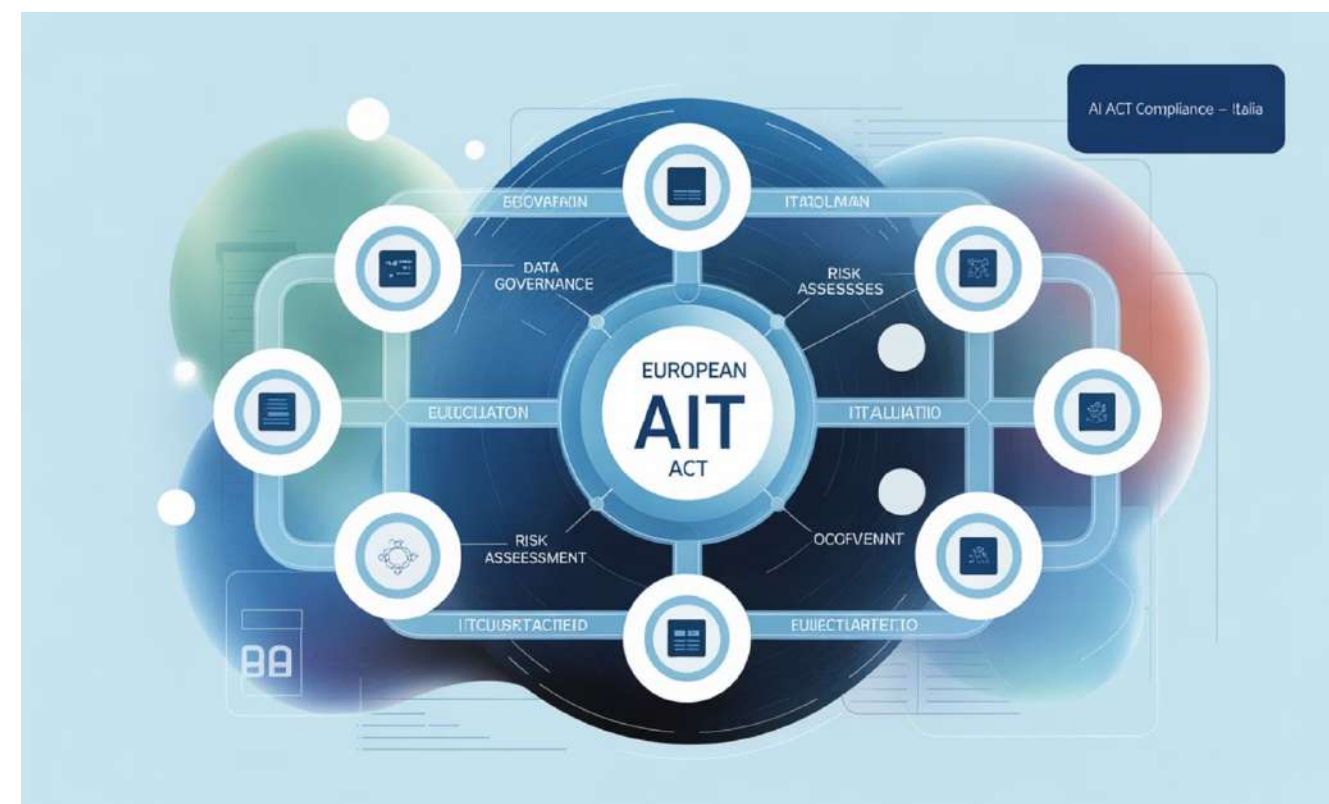
Le Sfide dell'Intelligenza Artificiale

Sostenibilità Ambientale

Il funzionamento e l'addestramento dei modelli IA richiedono elevate capacità computazionali, con significativo consumo energetico e impatto ambientale. C'è attenzione da parte delle amministrazioni, ma il livello di consapevolezza e intervento non è ancora soddisfacente, evidenziando un margine di miglioramento nell'adozione di pratiche di IA sostenibile e nella valutazione dell'impatto ecologico fin dalla progettazione.

Conformità Normativa (AI Act)

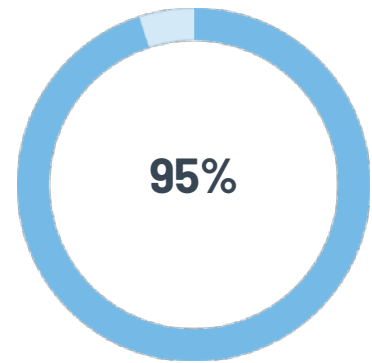
L'AI Act europeo mira a garantire che i sistemi IA siano sviluppati e utilizzati in modo sicuro, etico e trasparente, con un approccio proporzionato al rischio.



Analisi del Rischio

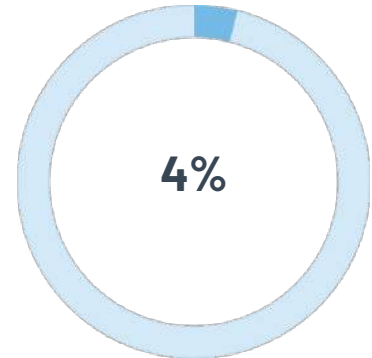
Quasi la totalità dei progetti analizzati risulta conforme al quadro normativo vigente.

Questo conferma una limitata esposizione dei progetti pubblici a scenari regolatori complessi



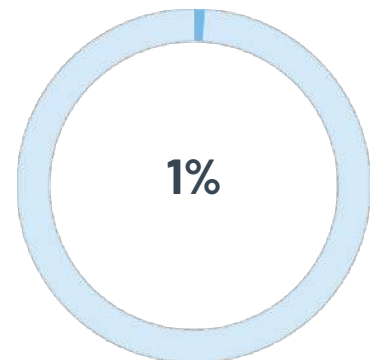
Progetti a basso rischio

Non rientrano nelle categorie ad alto rischio dell'AI Act



Profilazione automatica

Progetti che includono elementi di profilazione



Impatti significativi

Su diritti in ambiti sensibili come lavoro o istruzione



Raccomandazioni Operative (Conclusioni AgID)

AgID formula una serie di raccomandazioni operative per un'adozione più efficace, sostenibile e strategica dell'IA nel settore pubblico:

Raccomandazioni Tecnologiche e di Gestione Dati



Superare i Limiti Tecnologici

Privilegiare tecnologie di Machine Learning "tradizionali", affidabili e a basso impatto ambientale, integrando l'IA nei sistemi informativi esistenti della PA per coerenza architettonica e massimizzazione dell'efficacia.



Rafforzare Qualità e Gestione dei Dati

Integrare e valorizzare fonti informative eterogenee, assicurando standard elevati di accuratezza, completezza, affidabilità e interoperabilità. Cruciale la conformità alle normative sulla protezione dei dati personali e la riduzione dei gap di qualità tramite formazione e sviluppo organizzativo.



Innovare il Procurement Pubblico

Semplificare l'accesso alle soluzioni IA tramite strumenti esistenti (Accordi Quadro, Convenzioni Consip) e promuovere forme di procurement innovativo. Utilizzare gare dedicate, precedute da progetti pilota per testare fattibilità ed efficacia.



Pianificazione Progettuale a Medio-Lungo Termine

Definire chiaramente obiettivi, KPI tecnici e indicatori di impatto fin dalle fasi iniziali. Valutare scalabilità e replicabilità delle soluzioni, coinvolgere le strutture interne trasversalmente e adottare metodologie di open innovation per la condivisione di esperienze e buone pratiche.

"Le amministrazioni dovrebbero privilegiare tecnologie di Machine Learning "tradizionali", affidabili e a basso impatto ambientale, evitando approcci basati esclusivamente su tendenze di mercato legate all'IA generativa, spesso più energivore e meno consolidate."

"La pianificazione progettuale deve evolvere verso un'ottica di medio-lungo termine, con una definizione chiara di obiettivi, KPI tecnici e indicatori di impatto sin dalle fasi iniziali."

Sviluppo delle Competenze

Sviluppare Competenze Mirate e Trasversali

- Mappare le risorse interne
- Rafforzare competenze tecniche e gestionali
- Promuovere percorsi formativi differenziati
- Incentivare la creazione di profili professionali dedicati all'IA (es. AI Officer, Data Steward)

Questi interventi sono essenziali per presidiare l'uso dell'IA nella PA con continuità e visione strategica.

"Ogni amministrazione dovrebbe mappare le proprie risorse interne, rafforzare le competenze tecniche e gestionali e promuovere percorsi formativi differenziati per ruolo, livello e contesto. In parallelo, è auspicabile incentivare la creazione di profili professionali dedicati all'IA, come l'AI Officer o il Data Steward..."



AI Officer

Figura professionale dedicata alla supervisione strategica dei progetti di intelligenza artificiale.



Data Steward

Responsabile della qualità, integrità e gestione dei dati utilizzati nei sistemi di IA.