

**COMMISSIONE DI STUDIO  
SU  
L'APPLICAZIONE DELL'INTELLIGENZA ARTIFICIALE  
ALLE FUNZIONI DEL MINISTRO PER GLI AFFARI  
REGIONALI E LE AUTONOMIE**

## Sommario

Nota introduttiva del Pres. Torsello

Relazione Conclusiva

Infografiche riassuntive

Allegato:

Decreto istitutivo di una “Commissione di studio con il compito di svolgere attività di supporto e consulenza al Ministro sull’applicazione dell’intelligenza Artificiale alle questioni e ai temi di competenza concernenti gli affari regionali e le autonomie”.

Al Ministro per gli  
affari regionali e le  
autonomie  
On.le Sen. Roberto  
Calderoli

Oggetto: Relazione conclusiva della Commissione di studio sull'applicazione dell'Intelligenza Artificiale alle funzioni del Ministro e del Dipartimento per gli affari regionali e le autonomie.

Ai sensi dell'articolo 1, comma 3, del decreto istitutivo dell'11 settembre 2025, mi onoro di rassegnare alla Sua attenzione, a nome di tutti i Componenti, la relazione conclusiva con la quale la Commissione dà conto dell'attività svolta e formula le proprie proposte in ordine all'introduzione dell'Intelligenza Artificiale nelle funzioni del Dipartimento e degli Uffici di diretta collaborazione del Ministro.

La Relazione muove dalla convinzione che l'Intelligenza Artificiale non debba essere introdotta come mero strumento di produttività, bensì come tecnologia di supporto a processi istituzionali che esigono particolare accuratezza, tracciabilità e responsabilità.

Su questa premessa, il documento ricostruisce il quadro normativo di riferimento e dà conto dei limiti strutturali degli attuali sistemi, dalle allucinazioni all'opacità, dalla non riproducibilità degli esiti alla dipendenza dal fornitore, graduando conseguentemente le possibili applicazioni secondo tre livelli di rischio crescente.

Ne discende un'indicazione di metodo prima ancora che di strumento: una sperimentazione controllata e progressiva, avviata sui compiti a minore sensibilità istituzionale, ancorata a fonti verificate e assistita da una supervisione umana qualificata che, per le funzioni di maggiore delicatezza, non costituisce una facoltà, ma un obbligo.

La Commissione ha altresì dato conto di una prima sperimentazione preliminare, condotta in collaborazione con Microsoft e da intendersi come avvio operativo non esclusivo, e ha delineato un piano d'azione a medio termine in tre fasi, presidiato da un Osservatorio permanente.

Due considerazioni meritano - mi sia consentito - di essere rimesse alla Sua particolare attenzione.

La prima attiene alla rilevanza strategica del tema: la condizione che legittima il ricorso all'Intelligenza Artificiale non è soltanto la conformità alle norme, ma la capacità

dell'Amministrazione di mantenere un controllo effettivo sui dati, sulle fonti, sugli esiti e, in ultimo, sulla decisione, che deve restare sempre e integralmente umana.

La seconda attiene alla natura stessa di queste conclusioni: la tecnologia evolve con una rapidità tale che la soluzione di riferimento di oggi può risultare superata nel volgere di poco tempo.

Le valutazioni qui rassegnate hanno perciò, per loro stessa natura, carattere provvisorio; esse offrono un metodo e una traiettoria di adozione, più che una scelta definitiva, e postulano un aggiornamento continuo, ragione per la quale la Commissione ne ha raccomandato il presidio stabile nel tempo.

Nel ringraziarLa della fiducia accordata e nel rimettere il documento al Suo apprezzamento, la Commissione si rende disponibile per ogni ulteriore approfondimento che la S.V. Ill.ma vorrà ritenere utile.

Voglia gradire, Signor Ministro, i più cordiali saluti, anche a nome di tutta la Commissione.

Mario Luigi Torsello

Mario Luigi  
Torsello  
30.06.2026  
15:53:35  
GMT+02:00



**COMMISSIONE DI STUDIO**

*Decreto del Ministro per gli affari regionali e le autonomie dell'11 settembre 2025*

**L'APPLICAZIONE DELL'INTELLIGENZA ARTIFICIALE  
ALLE FUNZIONI DEL MINISTRO DEGLI AFFARI REGIONALI E LE AUTONOMIE**

## **1. Premessa e obiettivi dello studio**

## **2. Il quadro normativo**

[2.1 Le fonti applicabili](#)

[2.2 Protezione dei dati personali e trasferimenti extra-UE](#)

[2.3 Diritto d'autore](#)

[2.4 Etica e supervisione umana](#)

## **3. Criticità e limiti della tecnologia**

[3.1 Sicurezza informatica e sovranità digitale](#)

[3.2 Limiti tecnici dei sistemi di IA](#)

## **4. Le esigenze del DARA e del sistema delle Conferenze e degli Uffici di diretta collaborazione del Ministro**

[4.1 Esame di legittimità costituzionale](#)

[4.2 Segreteria delle Conferenze](#)

[4.3 Aree montane, minoranze, autonomie speciali](#)

[4.4 Banca dati delle leggi regionali](#)

[4.5 Modernizzazione istituzionale e attività internazionale](#)

[4.6 Progetti PNRR Green Communities](#)

[4.7 Uffici di diretta collaborazione: Ufficio di Gabinetto](#)

[4.8 Uffici di diretta collaborazione: Ufficio Legislativo](#)

[4.9 Sintesi delle esigenze e graduazione del rischio](#)

[4.10 Benchmarking europeo e traiettoria di adozione](#)

## **5. Le soluzioni disponibili sul mercato**

[5.1 Cloud, on-premise, SaaS e architetture ibride](#)

[5.2 Le principali piattaforme di IA generativa](#)

[5.3 Le scelte architetture negli Stati europei](#)

## **6. Valutazioni e raccomandazioni operative**

[6.1 Criteri di scelta](#)

[6.2 Indicazioni per la fase sperimentale](#)

[6.3 Esiti di una sperimentazione preliminare presso gli Uffici del DARA](#)

[6.4 Proposta di un piano d'azione a medio termine in tre fasi](#)

## **7. Conclusioni**

## **8. Riferimenti normativi**

## **Glossario delle espressioni tecniche**

## **Allegato 1 Sperimentazione con Microsoft: due agenti specializzati**

## 1. Premessa e obiettivi dello studio

Il presente studio analizza in modo sistematico le opportunità e le criticità connesse all'adozione di strumenti di intelligenza artificiale (IA) nell'ambito delle funzioni istituzionali del Dipartimento per gli affari regionali e le autonomie (DARA), struttura di supporto alla Presidenza del Consiglio dei ministri che opera nell'area funzionale dei rapporti tra lo Stato e il sistema delle autonomie territoriali, nonché degli Uffici di diretta collaborazione del Ministro per gli affari regionali e le autonomie (MARA)<sup>1</sup>.

Il DARA svolge un ruolo di cerniera istituzionale tra il Governo centrale, le Regioni, le Province autonome e gli enti locali. Assicura il coordinamento dell'azione governativa nei confronti del sistema delle autonomie, svolge le funzioni di segreteria della Conferenza permanente Stato-Regioni e della Conferenza unificata, esamina la legittimità costituzionale della legislazione regionale, supporta le politiche per le aree montane, le minoranze linguistiche e le autonomie speciali e gestisce le banche dati relative all'iter delle leggi regionali e alle impugnative. Gli Uffici di diretta collaborazione del Ministro – con particolare riferimento al Settore legislativo – svolgono attività di consulenza giuridica e legislativa, oltre che di progettazione ed elaborazione normativa nelle materie di competenza del Ministro.

L'adozione dell'IA al DARA non riguarda soltanto l'efficienza delle attività amministrative interne, ma funzioni che incidono direttamente sulla qualità del raccordo tra livelli di governo.

Per questo, l'IA va introdotta non come semplice strumento di produttività, ma come tecnologia di supporto a processi istituzionali che richiedono particolare accuratezza, tracciabilità e responsabilità.

La qualità degli [output](#), la loro verificabilità e la chiarezza della catena di responsabilità umana sono requisiti strutturali, coerenti con il ruolo che il DARA svolge nel sistema delle autonomie.

Il quadro normativo di riferimento è stato profondamente rinnovato con il Regolamento (UE) 2024/1689 ([AI Act](#)), primo corpus normativo organico al mondo in materia di IA, e con la Legge n. 132/2025 del 23 settembre 2025, che ha reso l'Italia il primo Stato membro UE ad affiancare una disciplina nazionale integrativa all'[AI Act](#).

Il metodo di lavoro si articola in quattro fasi: (i) esame dei vincoli normativi e dei limiti tecnici della tecnologia, con particolare riferimento alla protezione dei dati personali, al diritto d'autore, ai profili etici, alla sicurezza informatica, alla [sovranità digitale](#) e ai limiti intrinseci dei sistemi di IA ([allucinazioni](#), [bias](#), opacità); (ii) raccolta e classificazione delle

---

<sup>1</sup> Nel seguito per brevità indicheremo con la sigla DARA sia gli Uffici del dipartimento che gli Uffici di diretta collaborazione del Ministro (MARA).

esigenze del Dipartimento; (iii) confronto delle soluzioni di mercato; (iv) elaborazione di una proposta operativa.

I temi trattati richiedono inevitabilmente il ricorso a termini tecnici di informatica e intelligenza artificiale: per non appesantire la lettura con definizioni nel corpo del testo, ogni termine è spiegato nel Glossario finale, raggiungibile direttamente tramite i collegamenti ipertestuali presenti nel documento.

## 2. Il quadro normativo

Questa sezione illustra le norme che si applicano a qualsiasi scelta del DARA in materia di IA. Le fonti principali - [AI Act](#) europeo, Legge italiana 132/2025, [GDPR](#), Codice dei contratti pubblici e Legge sul diritto d'autore - si sovrappongono e si integrano, definendo un perimetro articolato che richiede un approccio sistematico.

Per ciascun tema l'analisi è strutturata su tre livelli: il contenuto della norma, la sua rilevanza specifica per le funzioni del DARA, le indicazioni operative che ne derivano.

### 2.1 Le fonti applicabili

#### 2.1.1 Il Regolamento europeo sull'intelligenza artificiale ([AI Act](#))

**Quadro normativo.** Il Regolamento (UE) 2024/1689 - pubblicato nella Gazzetta Ufficiale dell'UE il 12 luglio 2024 e in vigore dal 1° agosto 2024 - è il primo corpus normativo organico al mondo in materia di IA.

L'obiettivo è promuovere un'IA antropocentrica e affidabile, garantendo protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta UE.

L'approccio è basato sul rischio: i sistemi di IA sono classificati in quattro categorie - rischio inaccettabile (vietati), alto rischio, rischio limitato, rischio minimo - con obblighi crescenti al crescere del rischio. L'applicazione è progressiva: le pratiche vietate e gli obblighi di alfabetizzazione sono operativi dal 2 febbraio 2025; le norme per i modelli di uso generale ([GPAI](#)) dal 2 agosto 2025; la piena applicazione è prevista dal 2 agosto 2026, con un periodo transitorio fino al 2 agosto 2027 per i sistemi ad alto rischio già regolamentati.

**Rilevanza per il DARA.** Le pubbliche amministrazioni sono «[deployer](#)» quando utilizzano sistemi acquisiti sul mercato e «fornitori» quando li sviluppano internamente.

I sistemi usati per l'accesso a servizi pubblici essenziali ricadono potenzialmente nella categoria ad alto rischio, con conseguenti obblighi di valutazione di conformità, supervisione umana, tracciabilità e qualità dei dati.

**Indicazioni operative.** Verificare la categoria di rischio di ogni sistema prima dell'adozione. Per i sistemi ad alto rischio, avviare la procedura di valutazione di conformità e predisporre la documentazione tecnica richiesta. Mantenere aggiornata la mappatura man mano che il Regolamento entra in piena applicazione.

#### 2.1.2 La Legge italiana sull'IA (L. 132/2025)

**Quadro normativo.** Con la Legge n. 132/2025, entrata in vigore il 10 ottobre 2025, l'Italia ha adottato una disciplina organica che integra l'[AI Act](#) con previsioni specifiche per il contesto istituzionale italiano.

La legge, composta da 28 articoli, ribadisce il principio secondo cui l'IA deve operare come strumento di supporto all'attività umana, mai come sostituto.

L'articolo 14, dedicato alla PA, consente l'uso dell'IA per aumentare l'efficienza, ridurre i tempi dei procedimenti e migliorare i servizi, ma a tre condizioni: (i) conoscibilità del funzionamento del sistema; (ii) tracciabilità del suo utilizzo; (iii) adozione di misure tecniche, organizzative e formative adeguate.

AgID (Agenzia per l'Italia digitale) e ACN (Agenzia per la cybersicurezza nazionale) sono designate autorità nazionali per l'IA: ad AgID spettano le funzioni promozionali e di notifica; all'ACN quelle regolatorie e di vigilanza con poteri ispettivi e sanzionatori. La designazione dell'ACN come autorità di vigilanza rafforza il presidio di sicurezza; quella di AgID come autorità di notifica è coerente con i suoi compiti di promozione e indirizzo dell'Agenda digitale italiana.

**Rilevanza per il DARA.** Le tre condizioni dell'art. 14 non sono opzionali: sono requisiti minimi di legittimità per qualsiasi uso dell'IA in un procedimento amministrativo. Il terzo comma impone un programma di formazione del personale che il DARA dovrà pianificare prima o contestualmente all'adozione di qualsiasi strumento.

**Indicazioni operative.** Predisporre per ogni caso d'uso una scheda di conoscibilità che includa: (i) descrizione del sistema e della sua logica; (ii) limiti noti e tasso di errore atteso; (iii) modalità con cui il sistema motiva le proprie risposte, incluse le fonti richiamate e il percorso argomentativo seguito. Mantenere un registro delle interazioni. Pianificare la formazione del personale come condizione abilitante, non come attività successiva all'adozione.

### **2.1.3 GDPR, Codice della privacy e art. 30 del Codice dei contratti pubblici**

---

**Quadro normativo.** Il Regolamento (UE) 2016/679 (GDPR) resta il riferimento principale in materia di protezione dei dati personali.

Per l'uso dell'IA nella PA, il punto chiave è l'art. 22, che vieta le decisioni basate unicamente su trattamento automatizzato quando producano effetti giuridici o incidano significativamente sull'interessato, salvo eccezioni specifiche.

Il D.Lgs. 196/2003, come novellato dal D.Lgs. 101/2018, rafforza tali garanzie nel contesto nazionale.

L'art. 30 del D.Lgs. 36/2023 (Codice dei contratti pubblici) afferma il principio di non esclusività della decisione algoritmica e di comprensibilità delle logiche dei sistemi di IA usati dalla PA.

**Rilevanza per il DARA.** Anche se il DARA tratta prevalentemente dati pubblici, il GDPR si applica ogni volta che tali dati contengono riferimenti a persone fisiche identificabili, che il trattamento comporti profilazione o decisioni automatizzate, o che i dati vengano trasmessi a fornitori cloud extraeuropei. Ogni atto prodotto con il supporto dell'IA deve

poter essere motivato in modo comprensibile al destinatario, senza ridursi al solo riferimento all'[output algoritmico](#).

**Indicazioni operative.** Prima di alimentare qualsiasi sistema di IA con documentazione istituzionale, verificarne il contenuto rispetto ai criteri [GDPR](#). Dotarsi di una procedura di “data minimization”, principio del [GDPR](#) (art. 5, par. 1, lett. c) secondo cui i dati personali raccolti e trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui vengono trattati. Prevedere nei [workflow](#) una fase esplicita di revisione in cui il funzionario valuta criticamente l'[output](#) e redige la motivazione dell'atto in modo autonomo.

## 2.2 Protezione dei dati personali e trasferimenti extra-UE

### 2.2.1 I dati del DARA e i rischi di re-identificazione

**Il contesto.** Il DARA tratta prevalentemente dati pubblici: testi legislativi, atti delle Conferenze, documenti istituzionali, dati statistici territoriali. Tre situazioni richiedono attenzione: (i) dati pubblici con riferimenti a persone fisiche identificabili; (ii) trattamenti che comportino profilazione o decisioni automatizzate; (iii) dati trasmessi a fornitori [cloud](#) extraeuropei. A ciò si aggiunge il rischio di re-identificazione per [inferenza](#): anche a partire da dati formalmente pubblici, i sistemi di IA possono ricavare informazioni non esplicitamente contenute, come orientamenti politici, relazioni istituzionali o strategie negoziali.

**Indicazioni operative.** Prima di inviare documentazione a un sistema di IA, classificarne il contenuto rispetto a tre domande: contiene dati di persone fisiche identificabili? Supporta una decisione automatizzata? Viene trasmessa a un fornitore extraeuropeo? In presenza di risposta affermativa, applicare misure di minimizzazione e [pseudonimizzazione](#) appropriate.

### 2.2.2 Trasferimento di dati verso fornitori extra-UE

**Il contesto.** La grande maggioranza dei modelli di IA è sviluppata da società statunitensi. Usare questi servizi comporta, di regola, il trasferimento di dati verso server fuori dall'Unione europea.

Tre questioni rilevano: la base giuridica del trasferimento (oggi regolata dal [Data Privacy Framework](#) del 2023, che ha sostituito il Privacy Shield invalidato dalla sentenza [Schrems II](#) e resta esposto a un possibile «Schrems III»); l'uso dei dati per l'[addestramento](#) (i piani gratuiti possono consentire al [provider](#) di usare le conversazioni per addestrare i propri modelli, configurando per una PA un trattamento non autorizzato e potenzialmente in contrasto con il principio di limitazione delle finalità di cui all'art. 5 del [GDPR](#)); la localizzazione (la L. 132/2025 sostituisce l'obbligo di localizzazione nazionale con una «preferenza», che resta una valutazione strategica rilevante).

**Indicazioni operative.** Utilizzare piani [enterprise](#) solo se con garanzia esplicita di non uso dei dati per l'[addestramento](#). Verificare la certificazione [DPF](#) del fornitore. Valutare la [data residency](#) (si veda il paragrafo 2.2.3.) in relazione alla sensibilità istituzionale dei contenuti: per documenti sensibili, preferire soluzioni con trattamento documentato entro il perimetro UE.

### **2.2.3 Data residency e localizzazione: un perimetro non statico**

---

**Il contesto.** Quando un funzionario del DARA invia una richiesta a un assistente di IA in [cloud](#), quel testo viene elaborato su un server remoto. La [data residency](#) risponde alla domanda: dove si trova fisicamente quel server?

Vanno distinte due situazioni: i dati a riposo (file archiviati) e i dati in elaborazione (utilizzati mentre il modello lo processa). Questi possono trovarsi in luoghi diversi.

Microsoft, fra i principali partner europei, ha realizzato un perimetro tecnico-contrattuale - l'[EU Data Boundary](#) - che garantisce ai clienti europei sia l'archiviazione sia il trattamento dei dati entro l'UE.

La garanzia ha però tre eccezioni documentate:

- [Flex Routing](#): dal 25 marzo 2026 questa funzione è attiva per impostazione predefinita per i nuovi [tenant](#) UE/EFTA<sup>2</sup>. Nei momenti di picco, Microsoft può instradare l'elaborazione del singolo [prompt](#) fuori dall'UE (USA, Canada o Australia). I dati a riposo restano in UE, ma il trattamento di una specifica richiesta - ad esempio la bozza di analisi di una proposta di legge non ancora pubblica - può avvenire su server extra-UE. Si disattiva manualmente nel pannello di amministrazione.
- [Subprocessor](#) Anthropic: da gennaio 2026 Anthropic è [subprocessor](#) di Microsoft 365 Copilot e i suoi modelli sono esclusi dal perimetro [EU Data Boundary](#). Quando Copilot smista una richiesta verso un modello Anthropic, quella interazione esce dal perimetro UE. Va rilevato che il coinvolgimento di [subprocessor](#) diversi introduce anche un elemento di variabilità nella qualità e nelle garanzie tecniche delle risposte.
- **Trasferimenti residui:** anche con [EU Data Boundary](#) attivo e [Flex Routing](#) disattivato, restano possibili trasferimenti extra-UE di dati [pseudonimizzati](#) per finalità di sicurezza e gestione degli incidenti. La [pseudonimizzazione](#) protegge dall'identificazione diretta, non dal rischio di re-identificazione per [inferenza](#). Il monitoraggio deve essere continuativo, non una tantum.

Il punto critico è che l'equazione «Copilot = [data residency](#) UE = basso rischio organizzativo» è vera sulla carta, ma solo se l'amministrazione mantiene un presidio tecnico continuo.

---

<sup>2</sup> nuovi clienti (aziende o organizzazioni) che si iscrivono alla piattaforma e hanno sede in un paese dell'Unione Europea o dell'Area di libero scambio europea

La [data residency](#) non è una situazione statica: è una configurazione dinamica che il fornitore può modificare anche in modo silenzioso. Con i prodotti [SaaS](#) la decisione su dove avviene il trattamento resta in capo al fornitore.

**Indicazioni operative.** Se si sceglie Copilot di Microsoft, prevedere: disattivazione esplicita e documentata del [Flex Routing](#) con verifica periodica; impostazione della «Default Geography» del [tenant](#) su Italia; gestione contrattuale del [subprocessor](#) Anthropic; [DPIA](#) dedicata al solo strato Copilot; [audit trail](#) che renda noto quale modello ha elaborato ciascuna interazione.

#### **2.2.4 Valutazione d'impatto sulla protezione dei dati (DPIA)**

---

**Il contesto.** L'art. 35 del [GDPR](#) impone una [DPIA](#) quando il trattamento può comportare un rischio elevato per i diritti delle persone fisiche. L'introduzione di sistemi di IA nella PA può presentare un rischio elevato, ma non lo presuppone automaticamente in ogni caso: occorre effettuare uno screening DPIA per ogni caso d'uso e procedere a DPIA completa quando ricorrano rischio elevato, larga scala, dati personali, profilazione, trattamento automatizzato o dati sensibili.

**Indicazioni operative.** Trattare la [DPIA](#) come strumento di governance, non come adempimento formale: è il documento in cui l'amministrazione dimostra di aver compreso cosa sta facendo, perché, e con quali tutele. Prima di avviare la [DPIA](#), effettuare una mappatura funzionale dei casi d'uso per tipologia di dato e sensibilità istituzionale, distinguendo almeno quattro categorie: (a) dati pubblici già disponibili; (b) dati non pubblici interni al DARA; (c) documenti relativi a negoziati in corso o posizioni non ancora definite nelle Conferenze; (d) materiali destinati a valutazioni giuridico-amministrative rilevanti (analisi di legittimità, impugnative). Prevedere una [DPIA](#) separata per ogni caso d'uso significativo.

#### **2.2.5 Obblighi di trasparenza**

---

**Il contesto.** L'[AI Act](#) e la L. 132/2025 impongono di rendere conoscibile il funzionamento e tracciabile l'utilizzo dei sistemi di IA.

Occorre informare i soggetti coinvolti (Regioni, enti locali, cittadini) del fatto che l'IA è stata usata a supporto di un determinato procedimento e indicare le logiche di funzionamento del sistema.

**Indicazioni operative.** Inserire nella documentazione di ogni procedimento supportato dall'IA una nota standardizzata che indichi: quale sistema è stato utilizzato, con quale versione, per quale compito, dove ha elaborato la risposta, e che il risultato è stato sottoposto a revisione umana. Per gli usi più sensibili, l'output deve riportare esplicitamente le fonti richiamate, in modo da consentire la verifica ex post.

## 2.3 Diritto d'autore

### 2.3.1 Le opere prodotte con l'aiuto dell'IA

**Il contesto.** L'art. 25 della L. 132/2025 ha modificato la L. 633/1941 chiarendo che sono tutelate anche le opere create con l'ausilio dell'IA, purché frutto del «lavoro intellettuale dell'autore».

La legge non definisce però quanto contributo umano sia necessario. La responsabilità per i contenuti generati - inclusi estratti di opere protette, dati personali di terzi o affermazioni giuridicamente inesatte - ricade sull'amministrazione che pubblica o utilizza il documento.

**Indicazioni operative.** Documentare sempre il contributo umano nella produzione di ogni atto. Non pubblicare output di IA senza revisione sostanziale. Verificare i contenuti generati per individuare possibili estratti di opere protette o affermazioni inesatte.

### 2.3.2 Text and data mining e addestramento dei modelli

**Il contesto.** Gli artt. 70-ter e 70-quater della L. 633/1941 (attuazione della Direttiva UE 2019/790) consentono riproduzioni ed estrazioni di testo e dati da opere legittimamente accessibili per l'addestramento di modelli di IA, fatti salvi i diritti di opt-out.

Per il DARA rilevano due scenari distinti: l'invio di documenti (anche con testi protetti) a sistemi cloud come Copilot, dove sorge il rischio che il provider utilizzi i contenuti per addestrare i propri modelli; e l'ipotesi di voler addestrare un proprio modello (ad esempio adottando una soluzione RAG) su opere protette, dove occorre verificare l'assenza di opt-out da parte dei titolari. Si rimanda al Capitolo 5 per una analisi comparata di soluzioni architetturelle fornite da provider esterni vrs. soluzioni personalizzate o ibride.

**Indicazioni operative.** Utilizzare esclusivamente piani enterprise che garantiscano la non utilizzazione dei contenuti per l'addestramento. Se il DARA intende costruire un sistema RAG su documenti propri, verificare preventivamente l'assenza di opt-out da parte dei titolari dei diritti.

## 2.4 Etica e supervisione umana

### 2.4.1 Il divieto di decisione interamente automatizzata

**Il contesto.** AI Act, L. 132/2025 e art. 30 del Codice dei contratti pubblici convergono su un principio univoco: nessuna decisione amministrativa può essere assunta esclusivamente sulla base di un output algoritmico.

La supervisione umana deve essere effettiva: è un obbligo giuridico, non una raccomandazione. Il funzionario che «valida» la proposta dell'IA deve disporre di competenze, tempo e strumenti per comprendere l'output e, se necessario, discostarsene.

**Rilevanza per il DARA.** Il rischio principale è che la complessità dei sistemi renda la supervisione umana una mera ratifica formale di decisioni di fatto delegate alla macchina, un'automazione di fatto che elude le garanzie previste dalla legge. I sistemi commerciali disponibili non offrono garanzie di piena trasparenza [algoritmica](#): il DARA deve compensare questi limiti con una supervisione umana rafforzata.

**Indicazioni operative.** Ogni output dell'IA deve essere soggetto a revisione da parte di personale qualificato con competenze di merito. La validazione deve essere sostanziale: il funzionario deve poter motivare la propria valutazione indipendentemente dall'output. Prevedere esplicitamente nei [workflow](#) il tempo necessario per questa revisione.

#### 2.4.2 Bias algoritmico e non discriminazione

---

**Il contesto.** I sistemi di IA apprendono dai dati con cui sono addestrati. Se quei dati riflettono squilibri o distorsioni, il sistema tende a riprodurli e amplificarli. Il [bias](#) può derivare non solo dai dati, ma anche dalla [funzione obiettivo](#) (il criterio matematico che un sistema di IA ottimizza durante l'addestramento: misura quanto bene il modello sta raggiungendo lo scopo prefissato e guida l'aggiustamento dei parametri interni). Ad esempio, un sistema ottimizzato per la velocità può trascurare la completezza; uno ottimizzato per la standardizzazione può perdere le specificità territoriali. Il principio di non discriminazione (art. 3 Cost. e art. 5 [AI Act](#)) impone misure proattive di verifica e correzione.

**Rilevanza per il DARA.** Esempi concreti: trattamenti differenziati tra Regioni a seconda della composizione dei dati di addestramento; criteri di allocazione di fondi influenzati da correlazioni spurie; sottorappresentazione di determinati territori nelle analisi delle aree montane.

**Indicazioni operative.** Includere nella [DPIA](#) una valutazione del rischio di [bias](#) per ogni caso d'uso. Per applicazioni che incidono su allocazione di risorse o valutazioni comparative tra territori, prevedere audit periodici degli output con campionamento sistematico.

#### 2.4.3 Trasparenza e spiegabilità

---

**Il contesto.** «Spiegabilità» è la possibilità di comprendere e ricostruire le ragioni che hanno condotto il sistema a produrre un certo output.

È essenziale nel contesto amministrativo, perché la legittimità dell'azione pubblica richiede decisioni motivate e verificabili.

I modelli di [deep learning](#) sono scatole nere il cui funzionamento non è facilmente interpretabile neppure dagli sviluppatori.

**Rilevanza per il DARA.** L'opacità [algoritmica](#) è in tensione strutturale con l'art. 3 della L. 241/1990 (obbligo di motivazione del provvedimento). L'amministrazione non può

motivare un atto con il semplice riferimento a un output opaco: il funzionario deve poter spiegare la decisione con le proprie parole.

**Indicazioni operative.** Per i sistemi [LLM](#) - la tecnologia prevalente in questo contesto - la forma più accessibile di spiegabilità pratica consiste nel richiedere al modello, tramite opportuni [prompt](#), di esplicitare le fonti e i passaggi logici seguiti ([chain-of-thought](#)). Questo approccio trasforma il problema dall'interpretazione interna del modello alla verifica dell'argomentazione proposta, più accessibile al funzionario. Istituire una verifica umana sistematica degli output come presidio compensativo dell'opacità [algoritmica](#). Si veda a tal proposito anche la sezione 3.2 sulle tecniche di [XAI](#) (explainable artificial intelligence).

## 3. Criticità e limiti della tecnologia

Accanto al quadro normativo, qualsiasi scelta del DARA deve fare i conti con i limiti intrinseci degli attuali sistemi di IA.

Questa sezione descrive i principali rischi di sicurezza informatica, i limiti tecnici strutturali dei modelli linguistici e le implicazioni in termini di [sovranità digitale](#).

La consapevolezza di questi limiti non è un ostacolo all'adozione, ma la premessa per un'adozione responsabile e misurabile.

### 3.1 Sicurezza informatica e sovranità digitale

#### 3.1.1 Nuovi rischi di sicurezza introdotti dall'IA

**Il contesto.** L'adozione dell'IA introduce vettori di attacco specifici: [prompt injection](#) (istruzioni nascoste nei testi per indurre il sistema a comportamenti non previsti), [data poisoning](#) (corruzione dei dati di addestramento), esfiltrazione di dati attraverso le risposte del modello, [social engineering](#) assistito dall'IA (tecnica di manipolazione psicologica con cui indurre una persona a compiere azioni o rivelare informazioni riservate facendo leva su fiducia, urgenza o autorità apparente).

Un funzionario che carica nel [chatbot](#) un PDF ricevuto da un esterno può inconsapevolmente eseguire istruzioni nascoste nel documento. La [clonazione vocale](#) e i [deepfake](#) video iniziano a comparire in casi reali di frode.

Inoltre, per quanto concerne *la sicurezza nazionale ed il “mosaico” informativo*, si rimarca che il ricorso ai grandi servizi commerciali in [cloud](#), allo stato una necessità operativa priva di reali alternative, va accompagnato dalla consapevolezza che – a prescindere dalle assicurazioni anche contrattuali – i flussi di elaborazione e i singoli [prompt](#) possono transitare fuori dall'Unione europea nei momenti di picco o per l'instradamento verso modelli specifici, e che i fornitori statunitensi restano strutturalmente soggetti al [CLOUD Act](#), il quale consente alle autorità di quel Paese l'accesso ai dati di soggetti stranieri indipendentemente dalla localizzazione geografica dichiarata.

**Rilevanza per il DARA.** Il DARA gestisce informazioni sui rapporti tra livelli di governo, negoziati in corso, posizioni delle Regioni su temi sensibili: un patrimonio informativo con valore strategico specifico. I rischi di [prompt injection](#) e [social engineering](#) sono particolarmente critici. Riguardo alla sicurezza nazionale, il rischio per un'amministrazione come il DARA non risiede tanto nella sottrazione di un singolo documento classificato, quanto nella ricomposizione di un quadro strategico sensibile a partire da frammenti singolarmente innocui: i sistemi di IA sono progettati per individuare correlazioni semantiche non percepibili dall'osservatore umano e possono così ricostruire, per aggregazione e [inferenza](#), orientamenti, strategie e obiettivi dell'azione di governo (si veda anche il § 2.2.1 sulla re-identificazione per [inferenza](#)).

**Indicazioni operative.** Non integrare l'IA con sistemi che possano agire autonomamente su input di terzi senza supervisione umana. Formare il personale a riconoscere i casi sospetti di [prompt injection](#), in particolare quando si caricano documenti ricevuti da fonti esterne. Prevedere [penetration testing](#) periodico sui sistemi IA integrati. Applicare il principio del [minimo privilegio](#). Per i sistemi acquisiti come [SaaS](#), la compliance [NIS2](#) è primariamente responsabilità del vendor: richiedere contrattualmente garanzie aggiornate e obbligo di notifica in caso di incidenti.

Nei programmi di formazione previsti dall'art. 14 della L. 132/2025 si deve includere uno specifico focus sulla cultura della sicurezza del dato applicata all'interazione con l'IA: il personale non deve apprendere soltanto l'uso tecnico dello strumento, ma sviluppare la consapevolezza contro-operativa necessaria a formulare i [prompt](#) in modo da minimizzare - non potendo azzerare - il rischio che la combinazione di informazioni, anche ordinarie, alimenti attività di aggregazione informativa e di spionaggio estero.

### 3.1.2 Sovranità digitale

**Il contesto.** La L. 132/2025 ha ridefinito la [sovranità digitale](#) come capacità dello Stato di esercitare un controllo giuridico, tecnico e operativo sui propri processi digitali, indipendentemente dalla localizzazione fisica dei server. Il concetto si articola su tre piani: sovranità giuridica (processi regolati dal diritto europeo e nazionale); sovranità tecnica (competenze per governare i propri sistemi); sovranità operativa (capacità di operare anche in caso di interruzione di servizi di terzi). L'ACN è il referente istituzionale per la valutazione di conformità dei sistemi IA adottati dalla PA.

**Rilevanza per il DARA.** La scelta tra architetture cloud-based e [on-premise](#), tra [SaaS](#) e soluzioni custom (si veda il Capitolo 5), ha effetti diretti su sicurezza, sovranità dei dati e conformità. La [sovranità digitale](#) non è autarchia: è la capacità di scegliere - anche fornitori esteri - senza esserne costretti.

**Indicazioni operative.** Adottare un'[architettura ibrida](#): componenti generalisti in [cloud](#), basi documentali e dati strategici sotto controllo diretto. Preferire fornitori che offrano portabilità dei dati e standard aperti. Prevedere clausole contrattuali di exit. Monitorare le linee guida di AgID e ACN e i provvedimenti del Garante.

## 3.2 Limiti tecnici dei sistemi di IA

### 3.2.1 Allucinazioni

**Il contesto.** I grandi modelli linguistici ([LLM](#)) possono generare contenuti plausibili ma falsi: citazioni giurisprudenziali inesistenti, norme inventate, dati statistici fasulli. È una conseguenza della natura probabilistica di questi modelli: in mancanza di informazioni verificabili, tendono a colmare le lacune con inferenze statistiche sul linguaggio. Le [allucinazioni](#) sono strutturali alla tecnologia attuale, non malfunzionamenti occasionali.

**Rilevanza per il DARA.** In un contesto dove l'accuratezza giuridico-amministrativa è imprescindibile, le [allucinazioni](#) sono un rischio critico. Un'analisi giuridica con riferimenti normativi inesistenti può condurre a decisioni gravemente viziate o a impugnative infondate davanti alla Corte costituzionale. Il tasso di [allucinazioni](#) deve essere un criterio esplicito di scelta e valutazione.

**Indicazioni operative.** Adottare la tecnica [RAG \(Retrieval-Augmented Generation\)](#) per ancorare le risposte a basi documentali verificate. Esigere sempre la citazione delle fonti. Richiedere ai fornitori dati sul tasso di [allucinazioni](#) nei task giuridici. Definire criteri di accettazione misurabili (ad esempio, tasso inferiore al 5% su campione statistico) come soglia per il passaggio dalla sperimentazione alla produzione. Torniamo a sottolineare che la supervisione umana effettiva non è una strategia di mitigazione facoltativa, ma un obbligo giuridico trasversale: vale per le bozze come per le analisi più complesse.

### 3.2.2 Opacità algoritmica

---

**Il contesto.** I modelli di [deep learning](#) sono scatole nere: i loro sviluppatori non sono in grado di spiegare in modo completo perché producano un determinato output. Questa opacità - caratteristica intrinseca della tecnologia, non mancanza del fornitore - confligge con i principi di trasparenza e motivazione che reggono l'azione amministrativa (art. 3 L. 241/1990).

Esistono tecniche di [Explainable AI \(XAI\)](#) che migliorano parzialmente la trasparenza, ma non eliminano il problema di fondo. Per un'amministrazione che utilizza sistemi [LLM in cloud](#), la maggior parte delle tecniche [XAI](#) - dalle più classiche alle più recenti- richiede modifiche al modello, che i fornitori [SaaS](#) non consentono. In questo contesto operativo il presidio più accessibile rimane il [chain-of-thought prompting](#), che consente al funzionario di verificare il ragionamento esplicitato dal modello senza infrastruttura aggiuntiva; non è un sostituto della [XAI](#), ma il suo surrogato pratico nelle condizioni d'uso tipiche della PA.

**Indicazioni operative.** Adottare registri delle decisioni e [audit trail](#) per tracciare input, output, fonti e versione del modello. Richiedere funzionalità [XAI](#) ove disponibili. Usare sistematicamente [prompt](#) strutturati che richiedano al modello di esplicitare le proprie fonti e il ragionamento, consentendo al funzionario di verificare la coerenza della risposta.

### 3.2.3 Non riproducibilità degli output

---

**Il contesto.** I [chatbot](#) moderni non sono deterministici: a parità di input, possono produrre output diversi in momenti diversi. In un contesto amministrativo questo può tradursi in trattamenti differenziati di situazioni analoghe. I modelli vengono periodicamente aggiornati dai fornitori con possibili variazioni di prestazioni che sfuggono al controllo dell'amministrazione. Il fenomeno è amplificato nelle piattaforme [SaaS](#) multi-modello, dove lo stesso [prompt](#) può essere instradato verso modelli diversi in momenti diversi.

**Rilevanza per il DARA.** La non riproducibilità è un problema specifico per funzioni che richiedono uniformità di trattamento, come l'esame di legittimità costituzionale delle leggi regionali.

**Indicazioni operative.** Standardizzare i [prompt](#) per i compiti ricorrenti: formulazioni precise e costanti, che chiedano al modello risposte ancorate ai documenti forniti e non interpretazioni creative, aiutano utenti non specializzati a ridurre il problema. Nei sistemi accessibili tramite [API](#) o piattaforme [enterprise](#) configurabili è possibile anche agire direttamente sul parametro tecnico che governa la casualità delle risposte del modello («[temperatura](#)»): un valore basso lo spinge verso le risposte statisticamente più probabili e stabili, un valore alto introduce più variazione; nei prodotti [SaaS](#) come Copilot questo parametro non è invece accessibile all'utente finale e rimane fissato dal fornitore. E' inoltre utile: conservare i log delle interazioni e le versioni del modello usate, prevedere ambienti di test periodici e definire procedure di governance per gestire gli aggiornamenti del fornitore.

#### **3.2.4 Dipendenza dal fornitore ([vendor lock-in](#))**

---

**Il contesto.** L'adozione di un sistema di IA può creare dipendenza strutturale dal fornitore: costi alti di switching (abbandonare un fornitore e passare a un altro), perdita di competenze interne, vulnerabilità a modifiche unilaterali del contratto. Per una PA, dipendere da un fornitore privato extraeuropeo per funzioni sensibili pone questioni di autonomia strategica che vanno oltre la convenienza economica.

**Indicazioni operative.** Adottare architetture interoperabili basate su standard aperti. Prevedere clausole contrattuali su reversibilità, continuità del servizio, accesso ai dati e trasferimento delle conoscenze. Diversificare i fornitori (approccio multi-[provider](#)). Rafforzare le competenze interne. Preferire soluzioni conformi a standard europei di [sovranità digitale](#).

## 4. Le esigenze del DARA e del sistema delle Conferenze e degli Uffici di diretta collaborazione del Ministro (MARA)

Questa sezione identifica le aree di attività del DARA che potrebbero trarre maggior beneficio dall'introduzione dell'IA. Per ciascuna area, l'analisi è strutturata su tre livelli: la descrizione dell'esigenza operativa, le ragioni per cui tale esigenza è rilevante per le specifiche funzioni istituzionali, e le raccomandazioni operative per un utilizzo responsabile e conforme.

L'analisi integra le esigenze di digitalizzazione espresse dalle Regioni, dall'ANCI e dall'UPI in relazione ai [flussi di lavoro](#) istituzionali (disciplinati dal D.Lgs. 281/1997) e alle criticità riscontrate dagli utenti abilitati.

### 4.1 Esame di legittimità costituzionale delle leggi regionali

**Le funzioni.** L'esame di legittimità costituzionale delle leggi regionali e provinciali è svolto dall'Ufficio per le autonomie speciali e per l'esame di legittimità costituzionale della legislazione delle Regioni e delle Province autonome (Ufficio II), che cura l'istruttoria sulle leggi regionali e provinciali in vista dell'eventuale impugnativa.

**Il problema.** Il DARA esamina sistematicamente le leggi regionali per valutare l'eventuale impugnativa davanti alla Corte costituzionale. L'attività richiede il confronto tra testi normativi voluminosi, la verifica del riparto di competenze ex art. 117 Cost., l'analisi della giurisprudenza costituzionale rilevante e la redazione di relazioni istruttorie circostanziate. Il carico documentale è ingente e i tempi istituzionali impongono un'analisi rapida senza margini per omissioni.

**Perché interessa il DARA.** È la funzione a maggiore specificità istituzionale del Dipartimento e quella in cui un supporto efficace dell'IA avrebbe il più elevato impatto in termini di efficienza. L'analisi automatizzata dei testi regionali, il confronto con la giurisprudenza costituzionale e la classificazione delle materie potrebbero ridurre significativamente il tempo dedicato alla fase istruttoria, liberando risorse per la valutazione giuridica qualificata.

**Raccomandazioni.** L'IA può essere utilizzata esclusivamente come strumento di supporto istruttorio: individuazione di possibili profili di incostituzionalità, generazione di bozze di relazioni da sottoporre a revisione, classificazione automatica delle materie. La supervisione umana qualificata è imprescindibile: il funzionario deve valutare nel merito giuridico l'analisi proposta, verificare il corretto inquadramento del riparto di competenze ex art. 117 Cost. e accertare la pertinenza dei precedenti della Corte costituzionale richiamati. Si sconsiglia qualsiasi automazione delle valutazioni finali.

In linea con le proposte del sistema delle autonomie, l'IA dovrà facilitare un approccio collaborativo e preventivo: mappando la ripartizione delle funzioni amministrative locali

in ogni regione, effettuando analisi comparative interregionali per evidenziare buone pratiche e segnalando tempestivamente lacune tecniche o terminologie critiche già emerse in passati conflitti di competenza. Ciò permetterà di attivare un confronto preventivo con il Governo, riducendo l'errore amministrativo e prevenendo il contenzioso costituzionale.

## 4.2 Segreteria della Conferenza Stato-Regioni e della Conferenza unificata

**Le funzioni.** La gestione delle Conferenze genera un flusso documentale continuo e voluminoso: organizzazione delle sedute, preparazione dei dossier, redazione dei verbali, monitoraggio delle intese e dei pareri, aggiornamento degli archivi.

**Il problema.** La sperimentazione tecnologica in questo ambito deve affrontare tre criticità operative segnalate dagli enti territoriali: la scarsa leggibilità e l'eccessiva dimensione dei provvedimenti trasmessi tramite scansioni ad alta risoluzione (che appesantiscono i canali PEC); la complessità di navigazione delle aree riservate basate su complessi «codici sito» con barriere d'accesso come la 2FA; la difficoltà nel tracciare in modo certo l'iter di un provvedimento e dei relativi emendamenti (l'effetto «navetta»).

**Perché interessa il DARA.** È l'area a maggiore potenziale di efficientamento nel breve periodo. Le attività coinvolte sono ripetitive, strutturate e ad alta intensità testuale: esattamente il tipo di compiti in cui i modelli linguistici attuali ottengono i risultati più affidabili. La sintesi di documenti, la comparazione delle posizioni delle diverse Regioni su un tema, il tracciamento dello stato di attuazione delle intese e la generazione di report periodici sono applicazioni sperimentabili nel breve termine.

**Raccomandazioni.** Avviare la sperimentazione su queste attività, privilegiando compiti a bassa sensibilità. Definire una classificazione della sensibilità dei materiali e limitare l'uso dell'IA ai documenti già approvati o formalmente pubblici.

Le soluzioni di IA dovranno essere applicate lungo le fasi procedurali dell'iter delle Conferenze: nella diramazione (assegnazione e tagging automatico dei provvedimenti per materia e priorità, generazione di schede sintetiche); nella convocazione tecnica (pianificazione automatizzata delle agende, recupero rapido di precedenti storici); nella riunione tecnica (verbalizzazione assistita [speech-to-text](#), comparazione in tempo reale delle versioni del testo); nel post-Conferenza (classificazione automatica delle proposte emendative, tracciamento del percorso istituzionale e verifica del recepimento nel testo finale pubblicato).

## 4.3 Aree montane, minoranze linguistiche, autonomie speciali

**Le funzioni.** Il DARA gestisce programmi per le aree montane (Fondo per lo sviluppo delle montagne italiane), la tutela delle minoranze linguistiche storiche e il coordinamento con le Regioni a statuto speciale.

**Il problema.** Queste funzioni richiedono la gestione di dataset territoriali eterogenei, il monitoraggio di programmi di finanziamento pluriennali e la valutazione comparativa dell'impatto delle politiche.

**Perché interessa il DARA.** La dimensione quantitativa e la dispersione territoriale dei dati rendono questi ambiti adatti a strumenti di analisi automatizzata. Di particolare interesse è l'estensione delle capacità analitiche del progetto ReOPEN SPL, finalizzato a supportare gli enti territoriali nei settori dell'acqua, dei rifiuti e dei trasporti.

**Raccomandazioni.** Privilegiare applicazioni su dati aggregati e pubblicamente disponibili, evitando trattamenti che incidano su persone fisiche identificabili. Verificare che i modelli non introducano [bias](#) sistematici nelle analisi territoriali. Condurre una [DPIA](#) preventiva per ogni applicazione che comporti trattamento automatizzato su scala significativa.

#### 4.4 Banca dati delle leggi regionali

**Il problema.** Il DARA gestisce una banca dati sull'iter di esame delle leggi regionali, incluse le motivazioni delle impugnative. Si tratta di un patrimonio documentale di grande valore, attualmente sfruttato in modo prevalentemente statico: la ricerca avviene per parole chiave o navigazione manuale, senza possibilità di interrogazioni semantiche o analisi delle tendenze nel tempo.

**Perché interessa il DARA.** La trasformazione della banca dati da archivio a strumento di supporto decisionale è il caso d'uso con il miglior rapporto tra fattibilità tecnica e impatto operativo. La tecnica [RAG](#) (Retrieval Augmented Generation) consentirebbe di costruire un sistema di interrogazione semantica fondato sui documenti dell'archivio, riducendo drasticamente le [allucinazioni](#) e garantendo la citabilità delle fonti.

**Raccomandazioni.** Avviare un [PoC](#) su questa area con priorità. La base documentale per il sistema [RAG](#) dovrebbe essere costruita a partire dalle fonti già gestite dal DARA: leggi regionali con le motivazioni delle impugnative, giurisprudenza della Corte costituzionale rilevante, atti delle Conferenze già approvati. In questo modo l'IA opererebbe come strumento di accesso e ordinamento di materiali già appartenenti al patrimonio conoscitivo dell'amministrazione, con ogni risposta ancorata a testi citabili. Prevedere un [audit trail](#) degli accessi e delle interrogazioni.

#### 4.5 Modernizzazione istituzionale e attività internazionale

**Il problema.** Il Servizio per la modernizzazione istituzionale svolge attività di analisi comparata, [benchmarking](#) e cooperazione transfrontaliera che richiedono la consultazione di fonti eterogenee in più lingue, la sintesi di modelli istituzionali di altri Paesi e la produzione di documenti di analisi per interlocutori istituzionali.

**Perché interessa il DARA.** L'IA generativa ha prestazioni particolarmente elevate in compiti di sintesi, comparazione e redazione documentale multilingue: esattamente le attività di questo servizio, senza richiedere accesso a dati sensibili.

**Raccomandazioni.** Applicazione a basso rischio, adatta a una sperimentazione precoce. Utilizzare l'IA per la sintesi di fonti pubbliche e la redazione di bozze documentali, mantenendo la validazione umana prima della condivisione istituzionale. Prestare attenzione alla qualità delle traduzioni in contesti giuridico-amministrativi.

#### 4.6 Progetti PNRR Green Communities

**Le funzioni.** Il Servizio PNRR, incardinato all'interno del DARA, è responsabile dell'attuazione della misura Green Communities (M2C1 - Investimento 3.2) del Piano nazionale di ripresa e resilienza. L'attività consiste nell'erogare assistenza tecnica ai Comuni montani nella realizzazione di progetti di sviluppo in ambito energetico e ambientale, nel rispetto degli obiettivi e delle regole europee in termini di target e [milestone](#), nonché dei vincoli [DNSH](#) e dei [Criteri ambientali minimi \(CAM\)](#).

**Il problema.** Il Servizio gestisce un elevato numero di procedimenti paralleli, ciascuno con una propria documentazione progettuale, cronoprogramma e rendicontazione finanziaria. Il monitoraggio dell'avanzamento avviene in rapporto con il sistema [ReGiS](#) e deve tenere conto dei vincoli tecnici connessi alla progettazione [BIM](#), dei requisiti [DNSH](#) e [CAM](#), e delle scadenze europee di [milestone](#). Il volume e la disomogeneità dei dati da elaborare, uniti alla necessità di rilevare tempestivamente anomalie finanziarie e difformità esecutive, rendono il presidio manuale poco scalabile e ad alto rischio di omissioni.

**Perché interessa il DARA.** La natura ripetitiva e strutturata delle attività di monitoraggio — verifica della documentazione progettuale, incrocio dei dati [ReGiS](#), controllo della conformità ai criteri [DNSH](#) e [CAM](#), rilevazione di scostamenti rispetto ai cronoprogrammi — è particolarmente adatta all'impiego di strumenti di IA. L'automazione delle fasi di estrazione, classificazione e verifica incrociata dei dati potrebbe ridurre significativamente il carico operativo del Servizio, liberando risorse per le funzioni di valutazione e indirizzo. L'IA potrebbe inoltre supportare la comunicazione standardizzata con i Comuni beneficiari, attraverso sistemi agentici di assistenza strutturata su procedure e adempimenti predefiniti.

**Raccomandazioni.** In linea con la graduazione del rischio di cui al §4.9, le applicazioni su questa area si collocano prevalentemente nel primo e nel secondo livello. Le attività di monitoraggio documentale e di verifica di conformità su dati strutturati rientrano nel primo livello, con supervisione umana agevole; le analisi comparative tra procedimenti o la rilevazione precoce di anomalie finanziarie si collocano nel secondo livello e richiedono

fonti dati verificate e supervisione qualificata prima di qualsiasi utilizzo operativo. In nessun caso l'IA può sostituire la valutazione del funzionario responsabile del procedimento, né produrre comunicazioni verso i Comuni beneficiari senza revisione umana. Si raccomanda di avviare una sperimentazione su dati aggregati e già rendicontati, con definizione ex ante dei criteri di qualità degli output e adozione delle cautele previste ai capitoli 2 e 3.

#### 4.7 Uffici di diretta collaborazione del Ministro: Ufficio di Gabinetto

Gli Uffici del MARA di diretta collaborazione del Ministro – in particolare l'Ufficio di Gabinetto e l'Ufficio legislativo – sono deputati a svolgere attività ad alto potenziale di efficientamento, sia sotto il profilo della tempistica sia sotto quello dei contenuti.

**Le funzioni.** L'Ufficio di Gabinetto, per il tramite del Capo di Gabinetto, coadiuva il Ministro supportandone l'azione complessiva; verifica gli atti da sottoporre all'esame e alla firma del Ministro; sovrintende e coordina le attività affidate agli Uffici di diretta collaborazione, assicurando il raccordo tra questi e gli uffici di amministrazione attiva di cui si avvale il Ministro per l'espletamento delle funzioni delegate, anche con riferimento agli interventi e alle attività previste nel Piano nazionale di ripresa e resilienza (PNRR), nel rispetto del principio di separazione tra tali funzioni; collabora con il Ministro nella predisposizione e nell'aggiornamento del programma e delle direttive; assiste il Ministro nelle iniziative in campo internazionale ed europeo; collabora alla definizione degli obiettivi dell'Amministrazione, all'elaborazione delle politiche pubbliche, alla valutazione della loro attuazione e alle connesse attività di comunicazione; cura i rapporti del Ministro con i soggetti pubblici e privati e con gli altri organi istituzionali.

**Perché interessa gli uffici del MARA.** L'intelligenza artificiale può supportare le predette attività, anche attraverso la creazione di «agenti ad hoc», con particolare riferimento ad alcune aree tematiche: l'attuazione dell'autonomia differenziata; la cura dei provvedimenti di sostegno per le zone montane e le isole minori, nonché per la tutela delle minoranze linguistiche; la revisione degli Statuti delle autonomie speciali e i procedimenti relativi alle Commissioni paritetiche per le norme di attuazione; l'attuazione della delega in materia fiscale con riferimento alle autonomie territoriali; gli approfondimenti per la revisione del TUEL e dell'ordinamento delle province; i procedimenti amministrativi relativi alle istanze rivolte a vario titolo al Ministro o connesse alle sue competenze (ad esempio istanze di accesso agli atti e attività di rilievo internazionale).

**Raccomandazioni.** Diverse di queste materie – come l'autonomia differenziata o la delega fiscale – attengono a negoziati e posizioni istituzionali in corso ad elevata sensibilità: l'impiego dell'IA deve quindi restare di affiancamento, modulato sulla

classificazione dei materiali e assoggettato alle cautele dei capitoli 2 e 3 (protezione dei dati, tracciabilità, supervisione umana qualificata), coerentemente con la graduazione del rischio di cui al § 4.9.

#### **4.8 Uffici di diretta collaborazione del Ministro (MARA): Ufficio Legislativo**

**Le funzioni.** L'Ufficio legislativo provvede alla consulenza giuridica e legislativa, cura la predisposizione dei disegni di legge e degli altri atti normativi di competenza del Ministro e segue l'andamento dei lavori parlamentari. Le competenze principali si articolano nella predisposizione di disegni di legge e altri atti normativi (progettazione ed elaborazione di testi normativi nelle materie di competenza del Ministro); nell'analisi normativa (monitoraggio ed esame degli atti normativi predisposti da altre amministrazioni e degli emendamenti parlamentari, ai fini della formulazione di pareri); nel contenzioso costituzionale (predisposizione di contributi su questioni di legittimità costituzionale nelle materie di competenza del Ministro e sui conflitti di attribuzione tra Stato e Regioni); nel sindacato ispettivo (in collaborazione con l'Ufficio IV del DARA, gestione del relativo [flusso di lavoro](#), raccordo con le altre amministrazioni e predisposizione delle risposte).

**Perché interessa gli uffici del MARA.** L'intelligenza artificiale può offrire un supporto concreto e strategico intervenendo su più livelli – ausilio alla redazione di atti normativi e monitoraggio dell'impatto delle politiche, analisi degli atti normativi predisposti da altre amministrazioni e degli emendamenti parlamentari ai fini della formulazione di pareri e di ipotesi di modifiche normative, con effetti positivi in termini di capacità analitiche, velocità operativa e qualità del lavoro. I principali ambiti di efficientamento riguardano la ricerca intelligente di norme e precedenti (giurisprudenziali, dottrinali, statistici e «storici»), il supporto al *drafting* legislativo, le analisi di impatto della regolamentazione ([AIR/VIR](#)), la redazione di testi normativi, la predisposizione di note, appunti e testi di carattere giuridico, nonché di pareri attinenti al merito e alla legittimità costituzionale (in particolare sotto il profilo del riparto di competenze tra Stato e Regioni) di ipotesi normative in discussione. Anche per l'Ufficio legislativo i lavori della Commissione hanno evidenziato l'opportunità di creare «[agenti ad hoc](#)»: in una prima fase, l'esigenza è emersa con riferimento all'analisi e alla gestione degli emendamenti parlamentari trasmessi all'Ufficio (ai fini della formulazione del parere di competenza) e alle attività di sindacato ispettivo (ai fini della predisposizione delle risposte, attraverso la gestione del relativo [flusso di lavoro](#) e il raccordo con il DARA e le altre amministrazioni).

**Raccomandazioni.** Trattandosi di attività a forte componente giuridico-amministrativa, valgono integralmente i limiti e le cautele dei capitoli 2 e 3: impiego, in via esclusiva, di affiancamento nelle valutazioni di competenza, supervisione umana qualificata, ancoraggio a fonti verificate tramite [RAG](#) e tracciabilità rafforzata. In termini di graduazione del rischio (§ 4.9), la redazione degli atti normativi, l'analisi e la gestione degli emendamenti e la predisposizione di note e appunti la redazione di contributi in

relazione al contenzioso costituzionale, si collocano nel terzo livello, ad alto rischio, trattandosi di valutazioni che comportano un forte impatto sull'ordinamento giuridico. In tutti questi casi, infatti la decisione non può essere delegata all'output del sistema. Diversamente, le attività di ricerca e di sintesi a carattere istruttorio, di analisi di impatto, di mero supporto al *drafting* normativo si collocano nel secondo livello in quanto l'output, pur comportando una supervisione umana qualificata, orienta ma non costituisce la decisione finale.

#### 4.9 Sintesi delle esigenze e graduazione del rischio

Dall'analisi per aree funzionali emerge un quadro differenziato.

Le applicazioni a maggiore fattibilità immediata riguardano la ricerca semantica nella banca dati delle leggi regionali, la sintesi documentale per la segreteria delle Conferenze e il supporto alle attività di analisi comparata. Rientrano in questa categoria anche gli strumenti per la normalizzazione dei testi scansionati ad alta risoluzione e per il superamento delle ricerche basate su codici portale, da sostituire con interrogazioni semantiche intuitive.

Presentano invece maggiore complessità le applicazioni che incidono su valutazioni giuridiche, come l'analisi di legittimità costituzionale: qui i limiti attuali dei modelli - rischio di [allucinazioni](#), opacità degli output, non piena affidabilità giuridica - impongono un utilizzo esclusivamente assistivo.

In questo perimetro più complesso si colloca anche il tracciamento ex post del recepimento degli emendamenti proposti da Regioni, ANCI e UPI.

Le raccomandazioni formulate per i diversi casi d'uso fanno riferimento a un livello di rischio indicativo, attribuito a ciascuna applicazione dell'IA. I livelli di rischio orientano le cautele organizzative, tecnologiche e giuridiche da adottare.

L'[AI Act](#) (si veda il Capitolo 2) introduce una classificazione delle applicazioni di IA in base al livello di rischio.

Tuttavia, in assenza degli standard tecnici e delle linee guida applicative previsti dal Regolamento, l'attribuzione dei livelli di rischio ai casi d'uso del DARA ha carattere indicativo.

La valutazione proposta dalla Commissione segue un criterio funzionale: il rischio aumenta in funzione dell'incidenza dell'IA sul processo decisionale.

Le applicazioni di ricerca e consultazione documentale sono generalmente a rischio contenuto; quelle che supportano l'istruttoria e la predisposizione di atti sono a rischio medio; quelle che possono incidere direttamente su decisioni istituzionali o valutazioni giuridiche, come il contenzioso costituzionale, sono considerate ad alto rischio e richiedono sempre la piena supervisione umana.

Per rendere più operativa l'analisi, si è qui proposta una graduazione esplicita in tre livelli di intensità di rischio:

- **Primo livello - supporto documentale a basso rischio:** sintesi di atti già pubblici, ricerca semantica su archivi aperti, classificazione automatica di materie legislative, generazione di bozze di verbali da revisionare, [chatbot](#) informativi su base [RAG](#). Tecnologie mature, perimetro documentale circoscritto, supervisione umana agevole.
- **Secondo livello - attività istruttorie a rischio medio:** analisi comparativa di testi normativi, verifica del riparto di competenze, preparazione di dossier per le Conferenze, confronto di orientamenti giurisprudenziali. Richiedono fonti verificate (architetture [RAG](#) su archivi istituzionali validati), supervisione umana qualificata da parte di giuristi e tracciabilità rafforzata.
- **Terzo livello - attività valutative ad alto rischio:** analisi di legittimità costituzionale, valutazione dell'opportunità di un'impugnativa, posizionamento nelle Conferenze. L'IA deve restare rigorosamente assistiva: il funzionario non può delegare la decisione all'output del sistema, nemmeno parzialmente.

In tutti i casi, le esigenze non funzionali trasversali - trasparenza, protezione dei dati, interoperabilità, auditabilità, supervisione umana - non sono opzionali ma costituiscono requisiti minimi.

#### 4.10 Benchmarking europeo e traiettoria di adozione

Le esperienze europee mostrano una convergenza verso modelli di assistenza documentale, ricerca semantica e automazione controllata, con forte attenzione alla protezione dei dati, alla tracciabilità e alla riduzione della dipendenza dai singoli fornitori.

Francia, Estonia, Spagna, Portogallo e Germania stanno sperimentando soluzioni diverse, ma accomunate da un'impostazione prudente: uso dell'IA come supporto all'operatore, ancoraggio a basi documentali verificate, attenzione alla [sovranità digitale](#) e progressiva costruzione di [architetture ibride](#).

La lezione principale non è l'identificazione della «migliore piattaforma», ma la costruzione di una traiettoria di adozione coerente con le funzioni istituzionali, i vincoli di sicurezza e gli obiettivi di autonomia tecnologica.

Il settore evolve a una velocità tale per cui la soluzione leader di oggi può essere superata nel giro di pochi mesi: scegliere un'architettura flessibile e non vincolata a un unico fornitore vale più di qualsiasi classifica puntuale delle piattaforme disponibili.

Per il DARA, questa traiettoria si articola in tre fasi: (a) sperimentazione controllata su casi d'uso a basso rischio, con criteri di successo definiti ex ante; (b) costruzione di un'[architettura ibrida](#) in cui i modelli commerciali in [cloud](#) siano affiancati da basi documentali governate direttamente dall'amministrazione; (c) progressivo

rafforzamento delle competenze interne, diversificazione dei fornitori e adozione di requisiti di interoperabilità che riducano la dipendenza da un singolo ecosistema.

## 5. Le soluzioni disponibili sul mercato

### 5.1 Cloud, on-premise, SaaS e architetture ibride

L'adozione dell'IA implica due scelte architettrali principali.

La prima è tra cloud-based (infrastrutture e modelli erogati da un fornitore esterno, accessibili via internet) e [on-premise](#) (sistemi installati su infrastrutture controllate dall'amministrazione). Il [cloud](#) è oggi la modalità prevalente di erogazione dell'IA generativa: offre rapidità di adozione e scalabilità, riducendo gli investimenti iniziali. L'[on-premise](#) garantisce maggiore controllo ma richiede investimenti significativi e competenze tecniche. In pratica i due modelli tendono a convergere verso [architetture ibride](#), con alcuni componenti in [cloud](#) e altri sotto controllo diretto dell'amministrazione.

La seconda scelta è tra [SaaS](#) (piattaforme standardizzate accessibili via web o [API](#)) e soluzioni custom (progettate su misura per i processi dell'amministrazione).

Le [SaaS](#) consentono rapida sperimentazione a fronte di minore personalizzazione e maggiore dipendenza dal [provider](#).

Le custom richiedono tempi e investimenti maggiori, ma permettono un'aderenza più stretta ai processi istituzionali e un controllo più incisivo su sicurezza, interoperabilità e gestione dei dati.

Per amministrazioni complesse come il DARA, la scelta richiede una valutazione articolata che tenga conto della natura dei dati trattati, criticità delle funzioni coinvolte, requisiti di sicurezza, interoperabilità, sostenibilità economica e disponibilità di competenze interne.

### 5.2 Le principali piattaforme di IA generativa

Il mercato dell'IA generativa nel 2026 è dominato da quattro grandi ecosistemi: OpenAI, Anthropic, Google, Microsoft.

Accanto a questi esistono modelli [open source](#) o semi-open, più flessibili ma con minori garanzie in tema di responsabilità, sicurezza certificata e supporto [enterprise](#).

Il settore evolve molto velocemente: la tabella seguente è una fotografia al giugno 2026 e va riverificata al momento di qualsiasi scelta operativa.

Critero	ChatGPT (OpenAI)	Claude (Anthropic)	Gemini (Google)	Copilot (Microsoft)
<b>Modello di punta (giu. 2026)</b>	GPT-5.5	Opus 4.8 (mag. 2026)	Gemini 3.1 Pro	GPT-5.5 via Azure
<b>Finestra di contesto</b>	128K <a href="#">token</a>	1M <a href="#">token</a> (nativo); 200K via Microsoft Foundry	1M <a href="#">token</a>	128K <a href="#">token</a>

<a href="#">Data residency UE</a>	In sviluppo	Disponibile ( <a href="#">enterprise</a> )	Disponibile (GCP)	Disponibile (Azure)
<b>Punti di forza PA</b>	Ecosistema ampio, <a href="#">API</a> mature	Accuratezza nelle istruzioni, documenti lunghi	Capacità <a href="#">multimodali</a> , contesto ampio	Integrazione M365, compliance EU

*Nota. I valori di finestra di contesto e di data residency dipendono dal piano (enterprise/consumer), dal modello e dal canale di erogazione (API nativa, Microsoft Foundry/Azure, Google Vertex AI, Amazon Bedrock) e vanno verificati sul canale effettivamente adottato. Per Claude, ad esempio, la finestra di contesto è di 1M token sull'API nativa, su Amazon Bedrock e su Google Vertex AI, ma di 200K token su Microsoft Foundry: per il DARA, che accederebbe tramite l'ecosistema Microsoft, il valore operativo è quest'ultimo.*

**Soluzioni europee e italiane.** Accanto ai quattro grandi ecosistemi internazionali, il panorama include soluzioni europee e italiane rilevanti in una prospettiva di [sovranità digitale](#).

Mistral AI (Francia) propone modelli open-weight con alta qualità per l'italiano e infrastruttura europea. In Italia, Almawave (Almaviva) e Fastweb hanno sviluppato soluzioni [LLM](#) orientate alla PA; il progetto Minerva (Sapienza in collaborazione con il CINECA) sta costruendo un [LLM](#) su base accademica italiana. I modelli cinesi (DeepSeek, Qwen) hanno prestazioni tecniche elevate, ma la loro adozione da parte di una PA italiana presenta rischi di [sovranità digitale](#) analoghi a quelli del [CLOUD Act](#) statunitense: l'esclusione da questa analisi è una scelta consapevole.

La tendenza di fondo è verso modelli multi-modello e interoperabili: *le piattaforme principali tendono a integrare differenti modelli dentro la medesima interfaccia*. Per le PA è una buona notizia: riduce il rischio di lock-in e favorisce approcci modulari.

### 5.3 Le scelte architetture negli Stati europei

L'evoluzione delle strategie europee mostra una tendenza comune: nessuno dei principali Stati membri ha adottato un modello integralmente centralizzato o integralmente esternalizzato. Le soluzioni effettivamente implementate convergono verso [architetture ibride](#), multilivello e progressive.

La Francia, attraverso la strategia [Cloud au centre](#) e il [Cloud interministériel](#), ha promosso un modello in cui i servizi [cloud](#) per la PA devono essere gestiti da operatori con requisiti di fiducia elevati. La Germania promuove soluzioni «[cloud](#) sovrane» che utilizzano tecnologie globali mantenendo il controllo dei dati strategici sotto controllo nazionale. La Spagna privilegia l'utilizzo di piattaforme condivise e servizi comuni, favorendo interoperabilità e riuso. I Paesi nordici adottano modelli pragmatici in cui il ricorso a [cloud](#) commerciali è considerato compatibile con la tutela dei dati pubblici, purché accompagnato da adeguate garanzie organizzative. L'Estonia integra l'IA dentro

un'infrastruttura digitale nazionale già consolidata, fondata sul sistema X-Road e su un forte paradigma di interoperabilità.

Paese	Assetto	Architettura	Implicazione per la PA
<b>Francia</b>	<a href="#">Sovranità digitale</a>	<a href="#">Cloud</a> au centre + <a href="#">Cloud</a> interministériel	Controllo pubblico e localizzazione forte dei dati
<b>Germania</b>	Prudenziale e federale	<a href="#">Architetture ibride</a> e government <a href="#">cloud</a>	Standardizzazione con forte tutela della riservatezza
<b>Spagna</b>	Servizi condivisi	Interoperabilità e riuso di piattaforme comuni	Riduzione dei silos e rafforzamento dell'ecosistema
<b>Finlandia</b>	Sperimentazione controllata	<a href="#">Cloud</a> commerciale con auditing rigoroso	Innovazione rapida ma governata
<b>Estonia</b>	Digital-first	X-Road e architetture <a href="#">API</a> -centriche	Integrazione nativa tra basi dati pubbliche
<b>Regno Unito</b>	Governance centralizzata	Linee guida comuni e procurement controllato	Accountability e riduzione del lock-in

A livello comparato emerge una linea evolutiva comune: adozione progressiva e sperimentale; preferenza per [architetture ibride](#); crescente attenzione alla [sovranità digitale](#); forte enfasi su auditabilità, supervisione umana e governance; tendenza a modelli multi-provider per ridurre la dipendenza da singoli fornitori.

Per il DARA, la soluzione più coerente con il quadro europeo è un'[architettura ibrida](#) e modulare, in cui i servizi generalisti e di produttività vengano erogati tramite [SaaS](#) commercial e i componenti più sensibili rimangono sotto controllo diretto dell'amministrazione.

## 6. Valutazioni e raccomandazioni operative

### 6.1 Criteri di scelta

Le funzioni del DARA e degli Uffici di diretta collaborazione del Ministro per gli affari regionali e le autonomie si collocano in un ambito caratterizzato da elevata rilevanza istituzionale, forte componente giuridico-amministrativa, necessità di tracciabilità delle decisioni e gestione di documentazione complessa.

La scelta di una piattaforma di IA deve considerare cinque criteri prioritari:

- **Accuratezza e fedeltà alle istruzioni.** Il DARA tratta materie dove errori interpretativi o riferimenti normativi inesatti producono conseguenze istituzionali rilevanti. Servono piattaforme con basso tasso di [allucinazione](#).
- **Capacità di gestire documenti lunghi e complessi.** L'analisi di leggi regionali, dossier, verbali e atti normativi richiede di processare testi estesi mantenendo coerenza argomentativa.
- **Conformità normativa e protezione dei dati.** Piani [enterprise](#) con garanzie di non utilizzo dei dati per addestramento, [data residency](#) UE, certificazioni di sicurezza ([SOC 2](#), [ISO 27001](#)) e auditabilità degli accessi.
- **Qualità della produzione testuale in italiano.** Capacità di generare testi giuridico-amministrativi con terminologia appropriata e registro formale adeguato al contesto istituzionale.
- **Integrabilità con l'infrastruttura esistente.** Compatibilità con i sistemi già in uso presso la Presidenza del Consiglio e disponibilità di [API](#) per i [workflow](#) documentali.

A questi cinque criteri tecnici si aggiungono due profili organizzativi: la disponibilità di supporto specialistico da parte del fornitore e la sostenibilità della curva di apprendimento all'interno dell'amministrazione.

### 6.2 Indicazioni per la fase sperimentale

Come già osservato, non esiste oggi una piattaforma «migliore in assoluto».

La rapida evoluzione del mercato suggerisce un approccio aperto e progressivamente evolutivo, che mantenga flessibilità tecnologica e capacità di adattamento.

Il panorama si è peraltro arricchito negli ultimi tempi di nuovi modelli, tra cui soluzioni italiane di un certo rilievo come il già citato sistema Minerva, segno che la capacità di sviluppare modelli competitivi non è più prerogativa esclusiva dei grandi player internazionali.

Per l'avvio della sperimentazione, la Commissione ritiene tuttavia opportuno valorizzare le opportunità già disponibili nell'ambito dell'ecosistema Microsoft.

La ragione determinante è l'esistenza di un accordo già operativo tra la Presidenza del Consiglio dei ministri e Microsoft, che consente di attivare sperimentazioni, ottenere supporto specialistico nei [PoC](#) e ricevere iniziative di formazione del personale - condizione che abbatta tempi e costi di avvio in modo decisivo.

Due ulteriori ragioni di coerenza organizzativa: la suite Microsoft 365 è già ampiamente diffusa nelle PA italiane e l'ecosistema offre garanzie [enterprise](#) consolidate su compliance, auditabilità, gestione delle identità digitali e [data residency](#) europea tramite Azure.

Queste ragioni sono coerenti con i requisiti di protezione dei dati, tracciabilità e supervisione umana delineati nei capitoli 2 e 3, a condizione che vengano adottate le cautele operative descritte al §2.2.3.

La sperimentazione con Copilot dovrebbe tuttavia restare confinata a compiti a bassa sensibilità istituzionale - sintesi di atti già pubblici, supporto alla redazione di bozze di verbali, ricerca in archivi aperti - previa adozione di tutte le cautele del §2.2.3: disattivazione documentata del [Flex Routing](#), verifica della Default Geography, gestione contrattuale del [subprocessor](#) Anthropic, [DPIA](#) dedicata al solo strato Copilot, [audit trail](#) del modello effettivamente utilizzato. Queste cautele non sono opzionali ma condizioni necessarie.

Questa indicazione non è esclusiva né definitiva.

Per attività con forte componente giuridico-testuale, la Commissione segnala che esistono soluzioni concorrenti che in test indipendenti hanno mostrato risultati di interesse per la gestione di documenti estesi e l'accuratezza nelle istruzioni complesse.

La valutazione comparativa è raccomandata nella fase di sperimentazione.

Da escludere per le attività istituzionali: soluzioni [open-source](#) non certificate, in particolare quelle provenienti da ambiti che non offrono garanzie equivalenti in materia di protezione dei dati.

Va tuttavia distinto il caso dei modelli [open source](#) installati in locale ([on-premise](#)) con basi documentali [RAG](#) private: in questa configurazione i dati non lasciano l'infrastruttura dell'amministrazione e i requisiti di protezione dati sono più facilmente soddisfabili.

Sistemi leggeri di questo tipo - come GPT4All e soluzioni analoghe - rappresentano un'alternativa concreta per casi d'uso con dati particolarmente riservati, ma richiedono competenze tecniche interne adeguate.

### **6.3 Esiti di una sperimentazione preliminare presso gli Uffici del DARA**

Per focalizzare la sperimentazione sui temi di interesse del Dipartimento e degli Uffici di diretta collaborazione del Ministro ed effettuare specifici test operativi, è stata condotta un'attività di confronto tecnico con personale specializzato di Microsoft.

La sperimentazione si è articolata in due tavoli di lavoro, corrispondenti agli ambiti descritti nell'Allegato 1: il Tavolo A, dedicato alle attività del Dipartimento (Ufficio II), e il Tavolo B, dedicato agli Uffici di diretta collaborazione del Ministro (Gabinetto e Ufficio Legislativo). Il presente paragrafo dà conto degli esiti relativi al Tavolo A; per il Tavolo B si rinvia all'Allegato 1.

Con specifico riferimento agli Uffici del DARA, l'analisi ha riguardato le competenze dell'Ufficio per le autonomie speciali e per l'esame di legittimità costituzionale della legislazione delle Regioni e delle Province autonome (Ufficio II) e, in particolare, l'istruttoria sulle leggi regionali e provinciali.

Le tematiche individuate hanno riguardato:

- reperimento quotidiano delle leggi regionali e provinciali, nonché delle delibere statutarie;
- reperimento dei precedenti giurisprudenziali costituzionali.

Su tali ambiti è stato svolto un test operativo, articolato in una prima fase di definizione di [prompt](#) sottoposti a Copilot e in una seconda fase di sviluppo di [agenti](#) basati su Copilot.

Sul versante dei precedenti giurisprudenziali costituzionali il perimetro è stato esteso, valutando la possibilità di generare un [agente](#) dedicato in grado di esaminare la singola legge regionale e di supportarne l'istruttoria mediante l'estrazione dei contenuti normativi e dei precedenti pertinenti. I risultati dei test sono raccolti nell'Allegato 1.

Il reperimento quotidiano delle leggi regionali e provinciali e delle delibere statutarie non ha invece consentito, allo stato, ulteriori sviluppi, per la marcata disomogeneità implementativa dei siti istituzionali dei BUR, che rende difficile l'alimentazione automatica della base di conoscenza.

Con riferimento ai precedenti giurisprudenziali costituzionali, l'approccio prospettato è risultato di interesse per l'Ufficio II, potendo agevolare le attività istruttorie sui temi indicati.

Fermo restando l'intervento umano di validazione dei risultati, la tecnologia può contribuire al reperimento della documentazione istruttoria e alla sua analisi preliminare.

Quanto descritto è coerente con la cornice giuridica vigente in materia di uso dell'IA nella pubblica amministrazione: in particolare l'art. 14 l. 132/2025, il cui comma 2 dispone che tale uso avvenga "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", mentre il comma 3 pone a carico dell'amministrazione l'adozione di "misure tecniche, organizzative e formative finalizzate a garantire un utilizzo responsabile dell'intelligenza artificiale e a sviluppare le capacità trasversali degli utilizzatori", da

realizzare “con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente”.

L'intero percorso e i relativi risultati sono documentati nell'Allegato 1.

Si tratta di una sperimentazione su casi d'uso a bassa sensibilità, soggetta alle cautele indicate al §2.2.3 e al principio di non esclusività rispetto ad altre soluzioni di mercato richiamato nei paragrafi che precedono.

## 6.4 Proposta di un piano d'azione a medio termine in tre fasi

### Fase 1 - Preparazione (0–6 mesi)

---

Costruire le condizioni organizzative, giuridiche e tecniche per un uso controllato dell'IA:

- costituire un gruppo di lavoro interno con competenze giuridiche, informatiche e organizzative;
- effettuare una [DPIA](#) per ciascun caso d'uso identificato, preceduta dalla mappatura funzionale descritta al §2.2.4;
- mappare flussi di dati e procedimenti amministrativi suscettibili di supporto dell'IA;
- definire una policy interna che indichi casi d'uso consentiti, limitazioni e procedure di verifica degli output;
- avviare un programma di formazione del personale (obbligo ex art. 14 L. 132/2025) su potenzialità e limiti dell'IA, protezione dei dati e verifica critica degli output, includendo uno specifico modulo sulla cultura della sicurezza del dato applicata all'interazione con l'IA, volto a sviluppare nel personale la consapevolezza necessaria a formulare i [prompt](#) in modo da ridurre il rischio di aggregazione informativa indebita (si veda il § 3.1.1).

### Fase 2 - Sperimentazione (6–12 mesi)

---

Avviare progetti pilota in aree a rischio contenuto:

- sintesi documentali per le Conferenze, ricerche giuridiche preliminari, reportistica sui fondi per la montagna;
- negoziare contratti [enterprise](#) con clausole che costituiscono condizioni essenziali per preservare controllo, continuità e verificabilità delle funzioni amministrative: [data residency](#) UE e processing (localizzazione dell'elaborazione, non solo dell'archiviazione), non utilizzo dei dati per addestramento, audit di sicurezza, [SLA](#), portabilità dei dati, reversibilità del servizio, comunicazione preventiva di modifiche rilevanti al modello o ai [subprocessor](#), conservazione dei log delle interazioni, indicazione del modello effettivamente utilizzato;
- valutare implementazioni [RAG](#) basate sulla banca dati delle leggi regionali e sulla giurisprudenza costituzionale;
- monitoraggio sistematico della qualità degli output e dei tempi di lavorazione, con confronto pre/post IA.

### Fase 3 - Consolidamento (12–24 mesi)

---

Sulla base dei risultati della sperimentazione:

- estendere l'uso ad altre aree funzionali;
- sviluppare modelli personalizzati ([fine-tuning](#)) sulla terminologia giuridico-istituzionale del DARA;
- integrare l'IA nei [workflow](#) documentali esistenti tramite [API](#);
- istituire un meccanismo di audit periodico degli output, con verifica di accuratezza, non discriminazione e trasparenza;
- condividere le buone pratiche con altre strutture della Presidenza del Consiglio e altre PA, in coerenza con la Strategia italiana per l'IA 2024-2026.
- istituire un Osservatorio permanente sull'IA presso il Dipartimento: un organismo leggero, che si avvalga anche di esperti accademici esterni, con il compito di monitorare in modo dinamico l'evoluzione tecnologica e normativa e di aggiornare costantemente le indicazioni su quali strumenti adottare e su come utilizzarli. La scelta risponde alla natura non lineare del progresso dell'IA – in cui la potenza di calcolo impiegata per i modelli di frontiera raddoppia nell'ordine di pochi mesi e l'efficienza [algoritmica](#) cresce a ritmi analoghi – che rende rapidamente obsoleta qualsiasi «fotografia» dello stato dell'arte e impone all'amministrazione una capacità di adattamento continuo, speculare alla fluidità della tecnologia.

## 7. Conclusioni

L'intelligenza artificiale rappresenta un'opportunità concreta per il DARA e per gli Uffici di diretta collaborazione del Ministro di incrementare l'efficienza dei propri processi, migliorare la qualità delle analisi e potenziare la capacità di supporto alle politiche per le autonomie territoriali.

La sua adozione richiede però un approccio prudente, graduale e consapevole delle criticità giuridiche, etiche e tecnologiche che la caratterizzano.

Il quadro normativo - [AI Act](#) europeo, Legge 132/2025, [GDPR](#), Codice dei contratti pubblici - offre coordinate non prive di zone grigie, in particolare in materia di diritto d'autore delle opere generate con l'aiuto dell'IA, responsabilità per gli output algoritmici ed effettività della supervisione umana.

Sul piano tecnologico, i limiti intrinseci dei modelli linguistici - [allucinazioni](#), opacità, non riproducibilità, [vendor lock-in](#) - impongono cautela e strategie di mitigazione strutturate.

Il punto di partenza è la formazione del personale e la definizione di protocolli rigorosi di verifica degli output.

La scelta dello strumento di IA più idoneo non può prescindere da una valutazione multicriteriale che tenga conto di accuratezza, conformità normativa, integrabilità con l'infrastruttura esistente e qualità della produzione testuale in italiano.

Un approccio multi-piattaforma, che combini le eccellenze di ciascuna soluzione, appare preferibile a una scelta monolitica.

Per il DARA, l'introduzione dell'intelligenza artificiale dovrebbe procedere secondo una logica di sperimentazione controllata, proporzionata alla sensibilità delle funzioni coinvolte.

Gli strumenti di IA possono offrire un contributo significativo alla sintesi documentale, alla ricerca semantica, alla gestione delle basi dati e alla preparazione di bozze istruttorie; devono invece restare sottoposti a cautele rafforzate quando incidono sull'analisi di legittimità costituzionale, sulla gestione di documenti relativi a negoziati in corso o su attività suscettibili di orientare valutazioni istituzionali.

La condizione di legittimazione dell'uso dell'IA non è dunque soltanto la conformità normativa, ma la capacità dell'amministrazione di mantenere controllo effettivo sui dati, sulle fonti, sugli output, sulle configurazioni tecniche e sulla decisione finale.

L'adozione dell'IA nel DARA e negli Uffici di diretta collaborazione del Ministro per gli affari regionali e le autonomie non è un traguardo, ma un percorso che deve essere accompagnato da un investimento continuo in competenze, governance e cultura dell'innovazione responsabile.

## 8. Riferimenti normativi

### 8.1 Fonti normative

---

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 ([AI Act](#)).
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ([GDPR](#)).
- Legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale».
- Decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali.
- Decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici), art. 30.
- Legge 22 aprile 1941, n. 633, e successive modificazioni (Legge sul diritto d'autore).
- DPCM 1° ottobre 2012 e DM 28 marzo 2023 sull'organizzazione del DARA.
- Decreto legislativo 28 agosto 1997, n. 281 (Sistema delle Conferenze).

### 8.2 Documenti istituzionali

---

- Strategia italiana per l'intelligenza artificiale 2024-2026, Dipartimento per la Trasformazione Digitale e AgID, 2024.
- Piano triennale per l'informatica nella PA 2024-2026, Strumento 5 – Intelligenza Artificiale nella PA, AgID.
- AgID, «L'intelligenza artificiale nella Pubblica Amministrazione», 2025.
- AgID, Linee guida per l'adozione dell'IA nella PA (Determinazione n. 17/2025).
- OCSE, «Governing with Artificial Intelligence», 2025.
- Repubblica francese - DINUM, documentazione sul [Cloud](#) au centre e [Cloud](#) de confiance.
- Estonia - State Information System Authority (RIA), documentazione su Bürokratt / #KrattAI.
- Government Digital Service UK, AI Playbook for the UK Government.
- Germania - Bundesministerium des Innern und für Heimat (BMI), documentazione sul government [cloud](#) tedesco e sull'«AI Opportunity Market and transparency database».
- Spagna - Gobierno de España, «Hybrid [cloud](#) services strategy for Public Administrations» e «2024 Artificial Intelligence Strategy».
- Estonia - X-Road, documentazione su «implementation models» e «case studies library» (infrastruttura nazionale di interoperabilità).
- Regno Unito - Cabinet Office, «Guidance to civil servants on use of generative AI».

## Glossario delle espressioni tecniche

Questo glossario raccoglie i termini di informatica e intelligenza artificiale ricorrenti nello studio. Ogni voce apre con una definizione essenziale in corsivo, seguita da una spiegazione in linguaggio comune e, quando utile, da un esempio pratico o un'annotazione per la pubblica amministrazione.

### **Agente (agente IA) / «agenti ad hoc»**

*Sistema di IA configurato non per rispondere a una singola richiesta, ma per svolgere in autonomia una sequenza di passaggi orientati a un obiettivo, eventualmente interagendo con altri strumenti o dati.*

A differenza del chatbot, che produce una risposta per ogni prompt, un «agente» pianifica ed esegue più operazioni concatenate (ad esempio: recuperare un documento, confrontarlo con una norma, redigere una bozza). Gli «agenti ad hoc» richiamati nello studio sono agenti specializzati su un singolo flusso di lavoro (gestione degli emendamenti, atti di sindacato ispettivo). Per la PA il maggior grado di autonomia accresce i benefici ma anche i rischi: vanno rafforzati supervisione umana, tracciabilità e principio del minimo privilegio, evitando che l'agente compia azioni rilevanti su input di terzi senza controllo.

### **AI Act**

*Regolamento (UE) 2024/1689. Primo quadro giuridico completo al mondo in materia di IA.*

L'impianto del Regolamento è basato sul rischio: classifica gli usi concreti dei sistemi di IA in quattro categorie (rischio

inaccettabile, alto, limitato, minimo) con obblighi crescenti. Per la PA italiana l'aspetto pratico più importante è che la maggior parte degli usi rilevanti ricade nelle fasce ad alto rischio o limitato, determinando l'intero perimetro di ciò che è consentito fare, come, e con quali tutele.

### **AIR e VIR**

*Analisi di impatto della regolamentazione (AIR) e verifica di impatto della regolamentazione (VIR): strumenti di valutazione della qualità della normazione.*

L'AIR è condotta prima dell'adozione di un atto normativo per stimarne effetti, costi e benefici e confrontare le opzioni alternative; la VIR ne verifica ex post gli effetti realmente prodotti. Per lo Stato sono disciplinate dal d.P.C.M. 15 settembre 2017, n. 169. Per l'Ufficio legislativo l'IA può supportare la raccolta e la sintesi delle evidenze e la stesura delle relazioni, ferma restando la responsabilità umana sulla valutazione.

### **Algoritmo / decisione algoritmica**

*Sequenza finita e non ambigua di istruzioni che, applicata a un input, produce un output. La «decisione algoritmica» è una decisione presa o suggerita applicando un algoritmo o un modello di IA.*

Non tutto ciò che è algoritmo è intelligenza artificiale: il calcolo di un'imposta è un algoritmo elementare, un LLM è una composizione di algoritmi di enorme complessità. Per il diritto amministrativo la nozione è rilevante: la giurisprudenza del Consiglio di Stato riconosce all'interessato il diritto di

conoscere la «regola algoritmica» applicata al suo caso, in coerenza con l'obbligo di motivazione (art. 3 L. 241/1990) e con il principio di non esclusività della decisione algoritmica (art. 30 d.lgs. 36/2023).

### **Allucinazione**

*Errore tipico dei chatbot moderni: il sistema genera un'informazione plausibile ma falsa.*

Le allucinazioni sono una conseguenza strutturale del funzionamento dei modelli linguistici: in mancanza di informazioni verificabili, generano testo statisticamente plausibile, non necessariamente veritiero. Per la PA il rischio è ricevere testi formalmente impeccabili ma sostanzialmente errati. La mitigazione passa per tre leve: usare la tecnica RAG, pretendere sempre la citazione delle fonti, e mantenere la verifica umana come passaggio non eliminabile.

### **API (Application Programming Interface)**

*Insieme di regole tecniche che permette a due programmi di comunicare tra loro.*

Le API determinano cosa è tecnicamente possibile fare, a che velocità, con quali costi e con quale livello di personalizzazione: leggere la documentazione delle API di un fornitore è uno dei modi più affidabili per capire se quel fornitore risponde alle esigenze dell'organizzazione.

### **Architettura ibrida**

*Modello che combina componenti in cloud e componenti sotto controllo diretto dell'organizzazione.*

Invece di scegliere in blocco tra cloud e on-premise, l'architettura ibrida

distribuisce i componenti secondo la loro sensibilità. È la configurazione verso cui convergono quasi tutte le strategie pubbliche europee e la soluzione più realistica per la PA italiana.

### **Audit trail**

*Registrazione continua e ordinata che permette di ricostruire, a posteriori, tutto ciò che il sistema ha fatto.*

Per un sistema di IA usato dalla PA, l'audit trail dovrebbe contenere almeno: chi ha interrogato il sistema, con quale domanda, in quale data e ora, quale risposta ha ricevuto, quali documenti sono stati consultati, quali decisioni successive ne sono derivate. L'AI Act impone obblighi specifici di tracciabilità per i sistemi ad alto rischio.

### **Benchmark / benchmarking**

*Punto di riferimento per misurare prestazioni o confrontare pratiche. In ambito IA, test standardizzato che misura le capacità di un modello su compiti definiti.*

I benchmark dei modelli (ad esempio MMLU, GPQA) consentono confronti oggettivi ma parziali: nessuno esaurisce le capacità di un modello e le classifiche cambiano rapidamente. In senso organizzativo, «fare benchmarking» significa confrontare i propri processi con quelli di amministrazioni simili o di altri Paesi (come nel § 4.9), per individuare buone pratiche e margini di miglioramento.

### **Bias algoritmico**

*Distorsione sistematica nelle risposte di un sistema di IA, dovuta ai dati di addestramento o al modo in cui il sistema è stato progettato.*

Un sistema che applichi in modo uniforme una distorsione discriminatoria può violare il principio di uguaglianza davanti alla legge in modo molto più sistematico - e meno visibile - del pregiudizio del singolo funzionario. L'AI Act impone valutazioni specifiche sui dati di addestramento e sui possibili impatti discriminatori per i sistemi ad alto rischio. Due casi concreti illustrano il rischio: il sistema di selezione del personale sperimentato da Amazon e abbandonato nel 2018, che — addestrato su curricula in prevalenza maschili — aveva imparato a penalizzare i profili femminili; e il sistema statunitense COMPAS di valutazione del rischio di recidiva, accusato di tassi di errore più elevati per gli imputati afroamericani.

## **BIM**

*Building Information Modeling: metodologia di progettazione e gestione delle opere edili e infrastrutturali fondata su un modello digitale che integra i dati geometrici, tecnici e gestionali dell'intero ciclo di vita dell'opera.*

Il BIM non è un semplice disegno tridimensionale, ma una base informativa strutturata che accompagna l'opera dalla progettazione alla manutenzione. Nei progetti PNRR Green Communities la documentazione progettuale in formato BIM è uno dei vincoli tecnici di cui il Servizio PNRR del DARA deve tenere conto in fase di monitoraggio e verifica. Per la PA il dato rilevante è che si tratta di documentazione complessa e standardizzata, che si presta all'estrazione e al controllo automatizzato delle informazioni in essa contenute.

## **Black box (scatola nera)**

*Sistema il cui funzionamento interno non è ricostruibile osservandolo dall'esterno.*

Per la PA italiana crea una tensione concreta con l'art. 3 della L. 241/1990 sull'obbligo di motivazione del provvedimento. La giurisprudenza richiede che il funzionario non si limiti a recepire l'output, ma lo valuti criticamente e ne dia conto in motivazione. Due precisazioni evitano equivoci: non si tratta di segretezza intenzionale (gli sviluppatori non «nascondono» il funzionamento, lo ignorano davvero in dettaglio), né di imprevedibilità (su input simili il modello produce in genere output simili; semplicemente non se ne può ricostruire passo per passo la catena causale).

## **CAM (Criteri Ambientali Minimi)**

*Requisiti ambientali minimi che le stazioni appaltanti pubbliche sono tenute a inserire nei bandi di gara e nei contratti di appalto, in attuazione del Piano d'azione nazionale per gli acquisti verdi (PAN GPP).*

I CAM sono definiti dal Ministero dell'Ambiente e della sicurezza energetica con decreti ministeriali specifici per categoria merceologica (edilizia, energia, trasporti, ecc.). Nel contesto PNRR, il rispetto dei CAM è condizione necessaria per la rendicontabilità della spesa: i progetti che non rispettano i criteri ambientali applicabili non possono essere portati a rendiconto verso la Commissione europea. Per il Servizio PNRR del DARA, la verifica del rispetto dei CAM nei progetti Green Communities è un adempimento ricorrente e documentalmente impegnativo, che si

presta a forme di supporto automatizzato nella fase di controllo della documentazione progettuale.

### **Chain-of-thought**

*Tecnica di prompting che chiede al modello di esplicitare i passaggi del proprio ragionamento prima di fornire la risposta.*

Invece di restituire la sola conclusione, il modello espone in sequenza le tappe argomentative e le fonti richiamate. Per la PA è il presidio di «spiegabilità pratica» più accessibile quando si usano LLM in cloud (§ 2.4.3 e § 3.2.2): non apre la «scatola nera» del modello, ma sposta la verifica dall'interno dell'algoritmo all'argomentazione esposta, che il funzionario può controllare e contestare. Non sostituisce le tecniche di XAI, ma ne è il surrogato operativo nelle condizioni d'uso tipiche dell'amministrazione.

### **Chatbot**

*Programma con cui si può conversare in linguaggio naturale.*

I chatbot di nuova generazione - ChatGPT, Claude, Gemini, Copilot - sono interfacce conversazionali costruite sopra grandi modelli linguistici. Per la PA, il chatbot è uno strumento di produttività individuale e, in configurazioni avanzate con RAG, un assistente per la consultazione di archivi normativi.

### **CLOUD Act**

*Legge statunitense del 2018 che consente alle autorità USA di richiedere dati ai fornitori soggetti alla giurisdizione americana, anche quando i dati sono conservati fuori dagli USA.*

È il motivo per cui la sola data residency non basta a garantire la sovranità sui dati. Un fornitore statunitense che conservi

dati su server europei resta soggetto al CLOUD Act. Per la PA italiana è un parametro di valutazione del rischio che incide sulla scelta tra fornitori soggetti alla giurisdizione USA e fornitori europei. Il conflitto con il GDPR, che vieta i trasferimenti non autorizzati, è strutturale e non ancora pienamente risolto: è anche la ragione per cui alcuni Paesi, come la Francia, hanno costruito modelli di cloud di fiducia pensati per essere immuni dall'extraterritorialità normativa.

### **Cloud computing**

*Modello in cui i programmi e i dati risiedono su server remoti gestiti da un fornitore, accessibili via internet.*

Per la pubblica amministrazione italiana il quadro è regolato dalle Strategie Cloud Italia e dalla qualificazione dei servizi cloud da parte di ACN: non tutti i servizi cloud sono ammessi per tutti i tipi di dati.

### **Cloud sovrano / cloud di fiducia**

*Servizi cloud progettati per restare sotto controllo giuridico e operativo nazionale o europeo.*

L'idea concilia due esigenze in tensione: usare le tecnologie dei grandi provider e sottrarre i dati pubblici più sensibili alla giurisdizione estera. In Italia la cornice è data dalla qualificazione dei servizi cloud da parte di ACN e dal Polo Strategico Nazionale.

### **Constitutional AI**

*Metodo di addestramento sviluppato da Anthropic per orientare i propri modelli (famiglia Claude) verso comportamenti sicuri ed etici.*

Il nome richiama l'idea di una «costituzione»: un insieme di principi che

il modello viene addestrato a rispettare durante la generazione delle risposte. È una scelta di metodo specifica di Anthropic: altri fornitori usano combinazioni diverse — feedback umano su larga scala (RLHF), filtri post-generazione, regole codificate. Nessuno di questi approcci elimina del tutto le allucinazioni: quando un fornitore enfatizza il proprio metodo descrive il proprio approccio, non offre una certificazione di affidabilità.

### **Data poisoning**

*Attacco in cui i dati usati per addestrare un sistema di IA vengono deliberatamente «avvelenati», così da indurne risposte errate o manipolate.*

Agisce in fase di addestramento e contamina il modello stesso, a differenza del prompt injection, che agisce in fase d'uso sulle singole interazioni. Esempio: diffondere in massa contenuti falsi o orientati affinché vengano assorbiti dai modelli che si addestrano sul web. Per la PA il rischio è soprattutto indiretto (qualità dei modelli adottati) e rientra nella due diligence sui fornitori.

### **Data Privacy Framework (DPF)**

*Accordo tra UE e USA del 2023 che regola i trasferimenti di dati personali dall'Unione Europea verso gli Stati Uniti, in sostituzione del Privacy Shield invalidato dalla sentenza Schrems II.*

Il DPF consente di trasferire dati verso operatori statunitensi certificati, ma resta esposto a incertezze giuridiche: un eventuale «Schrems III» è già considerato possibile. Per la PA è la base giuridica attuale del trasferimento ma non una

garanzia permanente: la valutazione del rischio caso per caso rimane necessaria.

### **Data Processing Agreement (DPA)**

*Accordo sul trattamento dei dati, previsto dall'art. 28 del GDPR, che regola il rapporto tra titolare e responsabile del trattamento.*

Definisce finalità, durata e natura del trattamento, obblighi di sicurezza e riservatezza, ricorso a subprocessor e sorte dei dati alla cessazione del rapporto. Per la PA che adotti un servizio di IA è il documento contrattuale in cui si fissano garanzie come il non utilizzo dei dati per l'addestramento, la localizzazione e le condizioni di reversibilità: va sempre richiesto e letto insieme a SLA e certificazioni.

### **Data residency**

*Indica dove fisicamente risiedono i dati.*

Va distinta dai dati in elaborazione: un servizio può garantire l'archiviazione in UE e al tempo stesso elaborare fuori dall'UE singole richieste nei momenti di picco (è il caso del Flex Routing di Copilot). La data residency non è uno stato statico ma una configurazione che il fornitore può modificare.

### **Deep learning (apprendimento profondo)**

*Sottocategoria del machine learning che utilizza reti neurali con molti livelli per apprendere rappresentazioni complesse dei dati.*

Il deep learning è alla base degli attuali LLM e dei modelli di visione artificiale. Le sue capacità emergenti sono straordinarie, ma la complessità di queste reti le rende intrinsecamente opache: neppure gli sviluppatori riescono a spiegare esattamente perché il modello produca un determinato output - da qui il

problema della «scatola nera». Il termine «profondo» si riferisce al numero di strati di neuroni artificiali attraversati: dai due-tre strati dei sistemi degli anni Novanta alle decine o centinaia dei modelli odierni, resi possibili dalla disponibilità di GPU potenti e di grandi quantità di dati.

### **Deepfake e clonazione vocale**

*Contenuti audio o video sintetici, generati o alterati dall'IA, che riproducono in modo realistico la voce o l'immagine di una persona.*

La clonazione vocale è oggi ottenibile da pochi secondi di registrato; le videochiamate falsificate compaiono in casi reali di frode. Per la PA il rischio principale è il social engineering: una richiesta apparentemente autentica del vertice può indurre azioni indebite. La difesa è soprattutto organizzativa: procedure di doppia conferma sulle operazioni sensibili e canali di verifica indipendenti.

### **DNSH (Do No Significant Harm)**

*Principio europeo, sancito dal Regolamento (UE) 2021/241 che istituisce il dispositivo per la ripresa e la resilienza, secondo cui nessun intervento finanziato dal PNRR deve arrecare un danno significativo a nessuno dei sei obiettivi ambientali dell'UE.*

I sei obiettivi ambientali di riferimento sono: mitigazione dei cambiamenti climatici, adattamento ai cambiamenti climatici, uso sostenibile delle risorse idriche, transizione verso l'economia circolare, prevenzione e riduzione dell'inquinamento, protezione e ripristino della biodiversità. Per ogni progetto PNRR occorre dimostrare, con apposita documentazione tecnica, che l'intervento

non contrasta in modo significativo con nessuno di questi obiettivi. Per il Servizio PNRR del DARA, la verifica del rispetto del principio DNSH nei progetti Green Communities è un adempimento obbligatorio che richiede l'esame di documentazione tecnica complessa e può beneficiare di strumenti di supporto automatizzato nella fase istruttoria.

### **Deployer**

*Termine dell'AI Act per indicare chi utilizza un sistema di IA acquisito sul mercato.*

La distinzione tra fornitore (provider) e utilizzatore (deployer) è centrale nell'AI Act, perché gli obblighi sono diversi. Una PA che adotti un chatbot di un fornitore esterno è di norma un deployer. Se però personalizza il sistema in modo sostanziale, può ricadere in obblighi da fornitore. Attenzione alla linea di confine: se l'amministrazione personalizza il sistema in modo sostanziale — ad esempio con il fine-tuning su propri dati — può ricadere essa stessa negli obblighi, più gravosi, del fornitore.

### **DPIA (Data Protection Impact Assessment)**

*Valutazione d'impatto sulla protezione dei dati, prevista dall'art. 35 del GDPR.*

Per i sistemi di IA usati dalla PA è quasi sempre necessaria. Il Garante italiano ha richiesto DPIA approfondite per usi di IA in ambito pubblico. Una DPIA fatta bene non è un adempimento formale: è il documento in cui l'amministrazione dimostra di aver capito cosa sta facendo, perché, e con quali tutele.

### **Enterprise (piano enterprise)**

*Versione di un servizio destinata alle organizzazioni anziché ai singoli utenti, con garanzie contrattuali aggiuntive.*

Rispetto ai piani consumer, i piani enterprise dei chatbot offrono di norma garanzie dirimenti per la PA: non utilizzo dei dati per l'addestramento, separazione logica degli ambienti, SLA, supporto dedicato, certificazioni (ISO 27001, SOC 2) e possibilità di sottoscrivere un Data Processing Agreement. L'uso di piani consumer per attività lavorative è in genere sconsigliato: il passaggio all'enterprise non è solo una scelta di prezzo, ma di conformità.

### **EU Data Boundary**

*Perimetro tecnico-contrattuale con cui Microsoft si impegna a conservare ed elaborare entro l'UE/EFTA i dati dei clienti europei.*

La garanzia non è assoluta: esistono eccezioni documentate (Flex Routing, subprocessor Anthropic, trasferimenti pseudonimizzati residui). Per la PA il punto pratico è che il perimetro è una configurazione dinamica che il fornitore può modificare con impostazioni predefinite a sé favorevoli.

### **Explainable AI (XAI)**

*Insieme di tecniche che mirano a rendere comprensibili le decisioni dei sistemi di IA.*

Le tecniche XAI non eliminano il problema della scatola nera, ma offrono strumenti per illuminarla. Per la PA italiana, il diritto del cittadino a conoscere la regola applicata al proprio caso si traduce nella necessità di affiancare al sistema di IA strumenti XAI adeguati. Una distinzione utile è tra spiegazione (dare conto a posteriori di un singolo output, ad

esempio con esempi controfattuali) e interpretazione (disporre di un modello la cui logica è leggibile in sé): i modelli più potenti sono in genere meno interpretabili, e viceversa.

### **Fine-tuning**

*Tecnica con cui un modello già addestrato viene personalizzato su dati specifici di un determinato dominio.*

Per molte esigenze della PA, una strada più leggera e altrettanto efficace è la combinazione tra un buon prompt e una tecnica RAG. La scelta tra fine-tuning, RAG e prompt engineering dipende dal tipo di compito, dal volume di dati specialistici e dalla criticità delle risposte.

### **Flex Routing**

*Funzione di Microsoft 365 Copilot che, nei momenti di picco, può spostare l'elaborazione di una richiesta fuori dall'UE.*

Dal 25 marzo 2026 la funzione è attiva di serie per i nuovi tenant UE/EFTA e va disattivata manualmente nel pannello di amministrazione. Illustra un punto generale: con i prodotti SaaS la decisione su dove avviene il trattamento resta in capo al fornitore.

### **Funzione obiettivo**

*Il criterio matematico che un sistema di IA è progettato per ottimizzare durante l'addestramento e il funzionamento.*

Definisce che cosa significhi «meglio» per quel sistema: precisione, velocità, uniformità, riduzione dei costi. La scelta non è mai neutrale: un sistema ottimizzato per la velocità può trascurare la completezza; uno ottimizzato per la standardizzazione può perdere le specificità territoriali (§ 2.4.2). Per la PA

selezionare la funzione obiettivo è una decisione di indirizzo, non meramente tecnica, e va assunta consapevolmente. Vale qui la cosiddetta legge di Goodhart: «quando una misura diventa un obiettivo, smette di essere una buona misura».

### **GDPR**

*Regolamento generale dell'UE sulla protezione dei dati personali (Reg. UE 2016/679), in vigore dal 2018.*

Per l'IA, gli articoli più rilevanti sono l'art. 22 (decisioni automatizzate), l'art. 25 (privacy by design), l'art. 32 (sicurezza) e l'art. 35 (DPIA). In Italia l'autorità di riferimento è il Garante per la protezione dei dati personali. Tra i principi cardine rientra la responsabilizzazione (accountability) del titolare del trattamento.

### **GPAI (General Purpose AI)**

*Intelligenza artificiale di uso generale: modelli capaci di svolgere un'ampia varietà di compiti, non specializzati su un singolo dominio.*

L'AI Act dedica un capitolo specifico ai modelli GPAI, imponendo ai loro fornitori obblighi di trasparenza sulle capacità del modello, sulla qualità dei dati di addestramento e sui rischi sistemici. Questi obblighi sono entrati in vigore nell'agosto 2025. ChatGPT, Claude e Gemini sono GPAI.

### **Inferenza**

*In ambito IA, l'operazione con cui il modello produce una risposta a partire da un input.*

Va distinta dal training: si addestra una volta (fase costosa), si interroga molte volte (inferenza). Per la PA che integri l'IA in modo strutturale, il costo per inferenza

- moltiplicato per il numero di utenti e interazioni - definisce il costo operativo annuo del servizio. I fornitori applicano in genere una tariffazione «per token» consumato in ingresso e in uscita.

### **ISO 27001**

*Standard internazionale che certifica la gestione della sicurezza delle informazioni di un'organizzazione.*

Per la PA che valuti un fornitore IA, ISO 27001 è una garanzia di base ma non sufficiente. Va letta insieme ad altri elementi contrattuali (Data Processing Agreement, SLA, eventuali certificazioni nazionali) e mai presa da sola come prova di adeguatezza.

### **LLM (Large Language Model)**

*Tipo di modello di IA addestrato su enormi quantità di testo, in grado di comprendere e generare linguaggio naturale.*

Gli LLM non «sanno» le cose nel senso in cui le sa una persona: producono testo predicendo, parola dopo parola, la sequenza più probabile. Questa caratteristica spiega sia le loro capacità sorprendenti sia i loro limiti - in particolare la propensione alle allucinazioni.

### **Machine learning (apprendimento automatico)**

*Branca dell'IA in cui il sistema «impara» dai dati, anziché essere programmato con regole esplicite.*

Anziché ricevere istruzioni del tipo «se... allora...», il sistema osserva molti esempi e deduce da solo le regolarità. Il deep learning ne è un sottoinsieme, basato su reti neurali profonde; esistono molte altre tecniche (alberi decisionali, regressioni) ancora largamente usate quando i dati

sono strutturati e serve maggiore interpretabilità. È il campo a cui appartengono gli LLM.

### **Milestone**

*Nel quadro del PNRR, traguardo di natura qualitativa che segna il completamento di una fase rilevante di un investimento o di una riforma, da conseguire entro una scadenza europea predefinita.*

Le milestone si distinguono dai target, che misurano risultati quantitativi (numero di interventi, opere o beneficiari). Entrambi condizionano l'erogazione delle tranche di finanziamento europeo e sono monitorati attraverso il sistema ReGiS. Per il Servizio PNRR del DARA il rispetto delle milestone dei progetti Green Communities è un vincolo stringente: il controllo dell'avanzamento rispetto alle scadenze e la rilevazione tempestiva degli scostamenti sono attività ricorrenti e ad alta intensità documentale, che si prestano al supporto di strumenti di IA.

### **Minimo privilegio (least privilege)**

*Principio di sicurezza per cui ogni utente o programma deve disporre soltanto dei permessi strettamente necessari al proprio compito.*

Tradotto per l'IA: definire con precisione quali dati il sistema può leggere, dove può scrivere, con chi può comunicare, e chiedere conto al fornitore di questi parametri. È uno dei principi più disattesi, perché i privilegi tendono ad accumularsi nel tempo. Per il DARA è essenziale soprattutto quando si integrano agenti o si collega l'IA a basi documentali sensibili.

### **Multimodale**

*Si dice di un sistema di IA capace di lavorare con più tipi di input e output: testo, immagini, audio, video.*

Permette, ad esempio, di caricare un PDF complesso e chiederne la sintesi, far trascrivere un audio o interpretare un grafico. Per la PA apre possibilità concrete (estrazione di testo da documenti scansionati), ma anche rischi specifici: l'analisi automatica di immagini di persone richiede particolare cautela, e alcuni usi (riconoscimento facciale in spazi pubblici) sono vietati dall'AI Act.

### **NIS2**

*Direttiva UE 2022/2555 sulla sicurezza delle reti e dei sistemi informativi, recepita in Italia con D.Lgs. 138/2024.*

NIS2 amplia significativamente la platea dei soggetti obbligati rispetto alla precedente NIS1, includendo le pubbliche amministrazioni delle dimensioni medio-grandi. Impone misure di gestione del rischio, segnalazione degli incidenti di sicurezza e responsabilità del management. Per il DARA, la compliance NIS2 dei fornitori di servizi cloud e IA è un requisito contrattuale essenziale.

### **On-premise**

*Modello in cui i programmi e i dati restano su infrastrutture controllate dall'organizzazione.*

Vantaggi: massimo controllo, indipendenza da fornitori esterni, nessun problema di trasferimento internazionale. Svantaggi: investimento iniziale alto, necessità di competenze interne, ritardo nell'adozione di nuove funzionalità.

### **Open source (nel campo IA)**

*Software il cui codice sorgente è disponibile pubblicamente, modificabile e ridistribuibile.*

Un modello è davvero aperto solo se sono pubblici sia il codice sia i «pesi». Vantaggi per la PA: maggiore controllo, possibilità di esecuzione on-premise, indipendenza dal fornitore. Svantaggi: minori garanzie di supporto e sicurezza certificata; attenzione alla provenienza geopolitica del modello.

### **Opt-out**

*Possibilità di «uscire» da un trattamento dei propri dati, esercitata dall'interessato attraverso una scelta esplicita.*

In ambito IA ha due significati distinti: sul fronte degli utenti, la possibilità di impedire che le conversazioni vengano usate per addestrare il modello (di norma garantita di default nei piani enterprise); sul fronte degli editori/autori, la facoltà di segnalare che i propri contenuti non vengano usati per l'addestramento, anche tramite protocolli tecnici come robots.txt e ai.txt. La questione è regolata dagli artt. 70-ter e 70-quater della L. 633/1941.

### **Output / Input**

*L'input è ciò che il sistema riceve; l'output è ciò che il sistema produce in risposta.*

La distinzione è importante perché molti fornitori tariffano separatamente i token in ingresso (input) e quelli in uscita (output), e perché le politiche di trattamento (uso per addestramento, conservazione) possono differire tra input e output.

### **Penetration testing**

*Test di sicurezza che simula un attacco informatico per verificare quanto un sistema sia effettivamente vulnerabile.*

Per i sistemi IA usati dalla PA, il penetration test dovrebbe essere periodico (almeno annuale) e coprire vettori specifici dell'IA: prompt injection, tentativi di estrazione di dati di addestramento, attacchi alle API.

### **PoC (Proof of Concept)**

*Prova di concetto: progetto pilota di dimensioni limitate per verificare se una tecnologia è adatta alle esigenze concrete di un'organizzazione, prima di investirvi su larga scala.*

Un PoC ben fatto ha tre caratteristiche: scopo definito, durata limitata (tre-sei mesi tipicamente), criteri di successo decisi all'inizio. Per la PA, il PoC è lo strumento standard di adozione progressiva dell'IA.

### **Prompt**

*L'istruzione o domanda che l'utente scrive al chatbot.*

La qualità del prompt influenza la qualità della risposta in modo molto marcato. Un prompt vago produce risposte vaghe; un prompt preciso e ben contestualizzato produce risposte molto più utili. Per la PA, l'adozione di prompt standard condivisi per i compiti ricorrenti è uno dei modi più efficaci ed economici per migliorare la qualità dei risultati. Esistono varianti tecniche: zero-shot (la domanda è posta senza esempi), few-shot (si forniscono uno o più esempi del tipo di risposta desiderata) e chain-of-thought (si chiede al modello di ragionare passo per passo prima di rispondere).

### **Prompt engineering**

*L'insieme delle tecniche per formulare i prompt in modo da ottenere risposte più affidabili dal modello.*

Non è questione di stile: vincolare il modello (definire un ruolo, fornire esempi, separare istruzioni e contenuti, chiedere ragionamento esplicito, vietare l'invenzione di informazioni) migliora sensibilmente i risultati. Per la PA, costruire una libreria condivisa di prompt validati per i compiti ricorrenti (sintesi di norme, prime analisi di documenti) è un investimento ad alto rendimento e basso costo.

### **Prompt injection**

*Attacco informatico in cui istruzioni nascoste in un testo inducono il chatbot a comportarsi in modo non voluto.*

Un funzionario che carica nel chatbot un PDF ricevuto da un esterno può inconsapevolmente eseguire istruzioni nascoste nel documento. Per la PA, la mitigazione è anche organizzativa: non integrare l'IA con sistemi che possano agire autonomamente su input di terzi senza supervisione umana.

### **Provider / fornitore**

*L'azienda che sviluppa o eroga il sistema di IA.*

Nell'AI Act il termine «provider» ha un significato giuridico preciso: è chi sviluppa il sistema e lo immette sul mercato a proprio nome. La qualifica di provider comporta obblighi molto più pesanti di quella di deployer: valutazione di conformità, registrazione, documentazione tecnica, gestione del rischio e sorveglianza post-commercializzazione.

### **Pseudonimizzazione**

*Tecnica che sostituisce i dati identificativi diretti con codici o pseudonimi, così che i dati non siano più riferibili a una persona*

*senza informazioni aggiuntive custodite separatamente.*

Va distinta dall'anonimizzazione: un dato pseudonimizzato resta un dato personale perché la re-identificazione è possibile ricombinando le informazioni. La pseudonimizzazione riduce il rischio, non lo azzerava.

### **RAG (Retrieval-Augmented Generation)**

*Tecnica che combina un chatbot con una base documentale verificata: prima si cerca nei documenti, poi si genera la risposta basandosi solo su quanto trovato.*

Il vantaggio è doppio: si riducono drasticamente le allucinazioni e si ottiene trasparenza, perché la risposta è ancorata a documenti citabili. Per usi istituzionali è la tecnica più raccomandata ed è spesso preferibile al fine-tuning.

### **ReGiS (Registro e Gestione degli Interventi e della Spesa)**

*Sistema informativo nazionale attraverso cui le amministrazioni titolari di misure PNRR monitorano l'avanzamento fisico e finanziario dei progetti, rendicontano le spese e trasmettono i dati alla Commissione europea.*

ReGiS è gestito dalla Ragioneria Generale dello Stato ed è lo strumento unico di monitoraggio, rendicontazione e controllo del PNRR previsto dal Piano operativo di monitoraggio. Ogni amministrazione titolare di una misura è tenuta ad alimentare il sistema con i dati relativi all'avanzamento degli interventi, alle spese sostenute e al raggiungimento di milestone e target europei. Per il Servizio PNRR del DARA, l'incrocio e la verifica dei dati inseriti in ReGiS con la documentazione progettuale dei Comuni beneficiari Green Communities

costituisce un'attività ricorrente e ad alta intensità documentale, che si presta all'automazione parziale delle fasi di estrazione e controllo.

### **Rete neurale**

*Modello di calcolo ispirato – molto alla lontana – al funzionamento dei neuroni del cervello, organizzato in strati di unità matematiche.*

Una rete neurale artificiale è fatta di «neuroni» – in realtà piccole funzioni matematiche – disposti in strati: ogni unità riceve numeri in ingresso, li combina secondo certi «pesi» e passa il risultato allo strato successivo; i pesi vengono regolati durante l'addestramento finché la rete produce gli output desiderati. L'analogia con il cervello biologico è suggestiva ma fuorviante: i neuroni artificiali sono enormemente più semplici di quelli reali e non vi è alcuna evidenza che la rete «pensi» o «comprenda». La struttura a molti strati («profonda») è la base del deep learning e dei modelli linguistici che stanno dietro ai chatbot moderni.

### **SaaS (Software as a Service)**

*Modello in cui il software viene usato come servizio via internet, senza installare nulla in locale.*

Vantaggi: nessuna gestione tecnica, sempre l'ultima versione disponibile, costi prevedibili nel breve termine. Svantaggi per la PA: dati sui sistemi del fornitore, dipendenza continua, rischio di vendor lock-in, costi crescenti all'aumentare dell'uso.

### **Schrems II**

*Sentenza della Corte di giustizia UE del 2020 (Causa C-311/18) che ha invalidato il*

*Privacy Shield, l'accordo che regolava il trasferimento di dati personali dall'UE agli USA.*

La sentenza ricorda che la conformità al DPF (il successore del Privacy Shield) non è una garanzia eterna, e che valutazioni di rischio caso per caso restano necessarie. La sentenza prende il nome dall'attivista austriaco Max Schrems e fa seguito a Schrems I (2015), che aveva invalidato il precedente accordo «Safe Harbor»; un eventuale «Schrems III» sul Data Privacy Framework è considerato possibile.

### **SLA (Service Level Agreement)**

*Accordo sui livelli di servizio: parte del contratto che definisce le prestazioni minime garantite dal fornitore.*

Uno SLA tipico definisce parametri misurabili e penali in caso di mancato rispetto: disponibilità del servizio, tempi di risposta del supporto, tempo massimo di risoluzione di incidenti gravi. Senza uno SLA, le promesse commerciali del fornitore restano promesse. Esempio di parametro tipico: una disponibilità garantita del 99,9% corrisponde a circa otto ore di indisponibilità all'anno.

### **SOC 2**

*Certificazione di sicurezza, ampiamente usata negli Stati Uniti, che attesta che un fornitore ha implementato controlli adeguati su sicurezza, disponibilità, integrità dei dati e riservatezza.*

SOC 2 non sostituisce le certificazioni europee (in primis ISO 27001) ma le integra. La versione più rilevante è SOC 2 Type II, che valuta l'effettiva applicazione dei controlli su un periodo di 6-12 mesi.

### **Social engineering**

*Tecniche di attacco che puntano sull'inganno della persona anziché sulla violazione tecnica del sistema.*

L'esempio classico è la falsa e-mail del superiore che chiede un trasferimento urgente. L'IA generativa elimina i segnali tradizionali (errori di lingua, formulazioni innaturali) e consente messaggi perfetti e personalizzati, oltre a deepfake audio e video. Per la PA la difesa è soprattutto organizzativa: doppia conferma per le operazioni sensibili, formazione continua e canali di verifica indipendenti.

### **Sovranità digitale**

*Capacità di uno Stato di esercitare un controllo effettivo - giuridico, tecnico e operativo - sui propri dati, processi e infrastrutture digitali.*

La sovranità digitale non è autarchia: è la capacità di scegliere - anche fornitori esteri - senza esserne costretti. A livello italiano, il Polo Strategico Nazionale è la principale infrastruttura sovrana per i dati strategici della PA. Sul piano europeo la priorità si traduce in iniziative concrete come Gaia-X (federazione di cloud europei) e gli investimenti EuroHPC su supercomputer e modelli IA europei.

### **Speech-to-text**

*Tecnologia che converte automaticamente il parlato in testo scritto.*

Consente, ad esempio, la verbalizzazione assistita delle sedute (§ 4.2): l'audio di una riunione viene trascritto e può poi essere sintetizzato o indicizzato. La qualità varia con l'audio, gli accenti e la terminologia specialistica; per usi istituzionali la trascrizione va sempre rivista, e vanno valutati i profili di riservatezza dei contenuti registrati.

### **Subprocessor**

*Soggetto terzo a cui un fornitore affida a sua volta una parte del trattamento dei dati, per conto del cliente.*

Da gennaio 2026, Anthropic è subprocessor di Microsoft 365 Copilot e i suoi modelli sono esclusi dall'EU Data Boundary. Per la PA, mappare i subprocessor di un servizio e governarne contrattualmente le variazioni è parte integrante della due diligence.

### **Temperatura**

*Parametro tecnico che governa il grado di casualità delle risposte di un modello linguistico.*

Un valore basso spinge il modello verso le risposte statisticamente più probabili e stabili (utile per compiti che richiedono uniformità); un valore alto introduce maggiore variazione. È accessibile tramite API o piattaforme enterprise configurabili, mentre nei prodotti SaaS come Copilot resta fissato dal fornitore. Per la PA una temperatura bassa riduce la non riproducibilità degli output (§ 3.2.3).

### **Tenant**

*Nei servizi cloud, l'istanza logica isolata assegnata a una singola organizzazione, con utenti, dati e impostazioni separati da quelli degli altri clienti che condividono la stessa infrastruttura.*

Un fornitore SaaS serve molti clienti sulla medesima infrastruttura fisica, ma ciascuno opera all'interno del proprio tenant, separato logicamente dagli altri. Per la PA il tenant è l'unità su cui si configurano le garanzie rilevanti: la localizzazione dei dati (ad esempio impostando la «Default Geography» su Italia), le politiche di accesso, l'attivazione o disattivazione di funzioni come il Flex

Routing. Distinguere ciò che è governabile a livello di tenant da ciò che resta deciso dal fornitore a monte è essenziale per valutare il reale grado di controllo sull'ambiente.

### **Text and data mining (TDM)**

*Estrazione automatica di informazioni da grandi quantità di testo e dati mediante strumenti informatici; è alla base dell'addestramento dei modelli di IA.*

Sul piano del diritto d'autore, gran parte del materiale aspirato è protetto. Il diritto europeo (Direttiva UE 2019/790) e quello italiano (artt. 70-ter e 70-quater L. 633/1941) prevedono eccezioni: il TDM è lecito per la ricerca scientifica di organismi di ricerca e istituti del patrimonio culturale (art. 70-ter) e, per altre finalità, salvo riserva (opt-out) del titolare dei diritti (art. 70-quater). Per il DARA rileva nella due diligence sui modelli e qualora intendesse addestrare un proprio sistema su opere protette.

### **Token**

*Unità minima di testo con cui i modelli linguistici lavorano.*

Un token corrisponde in media a circa 0,75 parole in italiano. Il concetto è importante per due motivi pratici: la «finestra di contesto» è misurata in token, e la tariffazione dei fornitori si basa sui token consumati in ingresso e in uscita.

### **Training / addestramento**

*La fase in cui un modello di IA viene istruito usando grandi quantità di dati.*

Va distinto nettamente dall'inferenza: si addestra una volta (fase costosa), si interroga molte volte. Per la PA, l'addestramento da zero di un modello generale è oggi fuori portata e

generalmente non necessario: le scelte rilevanti sono adottare un modello esistente, eventualmente fare fine-tuning su dati propri, oppure costruire sopra il modello una soluzione RAG. Per i modelli di frontiera l'addestramento richiede mesi di calcolo su cluster di decine di migliaia di GPU e costi nell'ordine di decine o centinaia di milioni di euro; per modelli più piccoli i numeri scendono di alcuni ordini di grandezza.

### **Vendor lock-in**

*Dipendenza strutturale da un fornitore, tale che cambiarlo diventi molto costoso o praticamente impossibile.*

Per la PA è un rischio strategico che limita la libertà di scelta nel tempo e indebolisce la sovranità digitale. Le mitigazioni: preferire standard aperti, evitare integrazioni profonde con un singolo fornitore, prevedere clausole contrattuali di exit, mantenere competenze interne sufficienti.

### **Workflow (flusso di lavoro)**

*La sequenza ordinata di passaggi che compongono un processo lavorativo.*

«Integrare l'IA nei workflow» significa inserirla nelle fasi già esistenti del lavoro, anziché creare un sistema separato che vive parallelamente al processo. La differenza tra un'adozione che funziona e una che non funziona, spesso, è proprio questo passaggio.

### **XAI (Explainable AI)**

*Vedi la voce [Explainable AI](#).*

## Allegato 1 - Sperimentazione con Microsoft: due agenti specializzati

Percorso di collaborazione tra la Commissione PCM e Microsoft per la sperimentazione di agenti di Intelligenza Artificiale. Documento predisposto congiuntamente dalla Commissione e da Microsoft, allegato alla presente relazione per dare evidenza della prima attuazione operativa degli indirizzi del § 6.2.

### Scheda sintetica dell'iniziativa

<b>Ambito</b>	Applicazione dell'Intelligenza Artificiale Generativa e di <u>agenti specializzati</u> a supporto delle attività istituzionali
<b>Contesto</b>	Lavori della Commissione sull'applicazione dell'Intelligenza Artificiale presso la Presidenza del Consiglio dei Ministri
<b>Partner tecnologico</b>	Microsoft
<b>Approccio</b>	Analisi dei processi reali, identificazione dei casi d'uso, sviluppo e prova preliminare di prototipi di <u>agenti specializzati</u>
<b>Tavolo A</b>	Dipartimento per gli Affari regionali e le autonomie - Ufficio II
<b>Tavolo B</b>	Uffici di diretta collaborazione del Ministro - Gabinetto e Ufficio Legislativo
<b>Risultati conseguiti</b>	Realizzazione di due primi prototipi di <u>agenti specializzati</u> , in fase di prova e non ancora validati operativamente, e definizione di una metodologia replicabile per l'adozione dell'AI
<b>Obiettivo</b>	Supportare attività documentali, normative e istruttorie valorizzando il patrimonio informativo esistente

### Introduzione

Nell'ambito delle attività promosse dalla Commissione per l'applicazione dell'Intelligenza Artificiale presso la Presidenza del Consiglio dei Ministri, è stato avviato un percorso di confronto e collaborazione con Microsoft finalizzato a esplorare le potenzialità dell'Intelligenza Artificiale Generativa e degli agenti specializzati a supporto dell'attività amministrativa e istituzionale del Dipartimento per gli Affari Regionali a fronte delle sue richieste.

Sin dalle prime interlocuzioni, il lavoro si è caratterizzato per un approccio fortemente orientato ai casi d'uso concreti. L'obiettivo condiviso non era limitarsi a una valutazione teorica delle tecnologie disponibili, ma comprendere in che modo queste potessero essere applicate a

processi reali, supportando l'attività degli uffici attraverso strumenti capaci di valorizzare il patrimonio informativo già esistente e di facilitare l'accesso alla conoscenza.

A partire da questa impostazione, è stato avviato un percorso di analisi delle modalità operative adottate dagli uffici coinvolti, volto a individuare attività caratterizzate da elevata intensità documentale e dalla necessità di consultare un ampio numero di fonti informative. Questo lavoro congiunto ha consentito di identificare due distinti ambiti di sperimentazione, corrispondenti alle esigenze degli Uffici di diretta collaborazione del Ministro e del Dipartimento per gli Affari regionali e le autonomie, portando a una prima sperimentazione di due prototipi di [agenti specializzati](#), costruiti a partire da esigenze operative reali e da intendersi come punto di partenza per un percorso ancora da completare.

## **Tavolo A – Dipartimento per gli Affari regionali e le autonomie**

Con riferimento alle attività del Dipartimento per gli Affari regionali e le autonomie, il percorso di lavoro si è concentrato sull'analisi dei processi caratterizzati da una significativa componente documentale e normativa. Attraverso una serie di incontri di approfondimento con gli uffici competenti, sono state esaminate le principali modalità operative adottate nell'analisi di leggi regionali, provvedimenti amministrativi e documentazione di supporto alle attività istituzionali.

L'attività congiunta ha consentito di ricostruire il [flusso di lavoro](#) normalmente seguito dagli uffici, individuando le fonti informative utilizzate, le attività di ricerca e consultazione più ricorrenti e le tipologie di output maggiormente richieste nel corso delle istruttorie. Tale analisi ha permesso di identificare una serie di attività nelle quali l'Intelligenza Artificiale può offrire un contributo concreto in termini di accessibilità delle informazioni, analisi dei contenuti e valorizzazione del patrimonio documentale esistente.

Sulla base delle evidenze raccolte è stato progettato e realizzato, a titolo dimostrativo, un primo prototipo di [agente](#) dedicato al Dipartimento, pensato per supportare gli utenti nella consultazione della documentazione, nell'identificazione delle informazioni rilevanti, nella sintesi di testi complessi e nella predisposizione di elaborazioni strutturate utili alle attività degli uffici. Dal punto di vista tecnologico, la soluzione è stata impostata come [agente](#) specializzato integrabile nell'esperienza Microsoft 365 Copilot e configurabile tramite strumenti quali Copilot Studio e/o Azure AI Foundry, a seconda del livello di personalizzazione richiesto. L'[agente](#) utilizza basi di conoscenza documentali selezionate, capacità di ricerca semantica e meccanismi di generazione controllata delle risposte, così da fornire supporto agli uffici mantenendo tracciabilità delle fonti, governo degli accessi e supervisione umana sui contenuti prodotti.

La prova ha consentito di intravedere come l'impiego di un [agente](#) specializzato possa, in prospettiva, agevolare l'accesso alla conoscenza e ridurre i tempi necessari alla ricerca delle informazioni, mantenendo invariato il ruolo decisionale e di supervisione degli uffici

competenti. Si tratta tuttavia di una dimostrazione preliminare, non ancora sottoposta a una verifica operativa estesa: prima di un effettivo utilizzo nell'attività quotidiana sarà necessario un lavoro di affinamento, test più approfonditi sul campo e un adeguato percorso di formazione del personale.

## **Tavolo B – Uffici di diretta collaborazione del Ministro**

Per quanto riguarda gli Uffici di diretta collaborazione del Ministro e, in particolare, l'Ufficio Legislativo, il lavoro si è focalizzato sull'analisi delle attività istruttorie connesse agli atti di sindacato ispettivo, alle richieste di approfondimento e alla predisposizione di elementi informativi a supporto dell'azione istituzionale.

Nel corso del confronto è stato possibile approfondire le diverse fasi del processo di lavoro, dalla ricezione dell'atto alla ricerca dei precedenti, dalla consultazione delle fonti normative e istituzionali alla raccolta e organizzazione degli elementi utili all'istruttoria. Tale analisi ha evidenziato la centralità delle attività di ricerca documentale e di ricostruzione del contesto.

A partire da queste esigenze è stato progettato e realizzato, anch'esso a titolo dimostrativo, un secondo prototipo di agente specializzato, dedicato alle attività dell'Ufficio Legislativo. L'agente è stato configurato per assistere gli utenti nell'individuazione delle fonti rilevanti, nella ricerca di precedenti, nell'organizzazione delle informazioni raccolte e nella predisposizione di una prima struttura di analisi a supporto delle successive valutazioni dell'Amministrazione. La soluzione è stata concepita con un'impostazione più articolata, potenzialmente multi-agente, nella quale un agente principale coordina il processo istruttorio e può richiamare componenti specializzate per l'analisi normativa, giurisprudenziale e dottrinale. Tale impostazione può essere realizzata attraverso Copilot Studio per l'orchestrazione dell'esperienza utente e dei flussi conversazionali, oppure tramite Azure AI Foundry per scenari che richiedano maggiore controllo sull'orchestrazione, sui modelli, sulle basi dati e sui connettori verso fonti documentali. In entrambi i casi, l'architettura resta orientata a un utilizzo governato: fonti selezionate, permessi coerenti con l'organizzazione, citabilità delle evidenze e intervento umano nelle fasi di validazione finale.

La prova ha mostrato come gli agenti di Intelligenza Artificiale possano, in linea di principio, rappresentare uno strumento di supporto alle attività istruttorie, contribuendo a velocizzare le attività di consultazione e analisi documentale. Resta tuttavia un risultato preliminare: si è trattato di una dimostrazione delle possibilità della tecnologia, non di una soluzione testata in condizioni operative reali. Il suo eventuale impiego nell'attività quotidiana degli uffici richiederà ulteriori approfondimenti tecnici, una verifica estesa nel tempo e un percorso di formazione dedicato al personale.

## **Conclusioni**

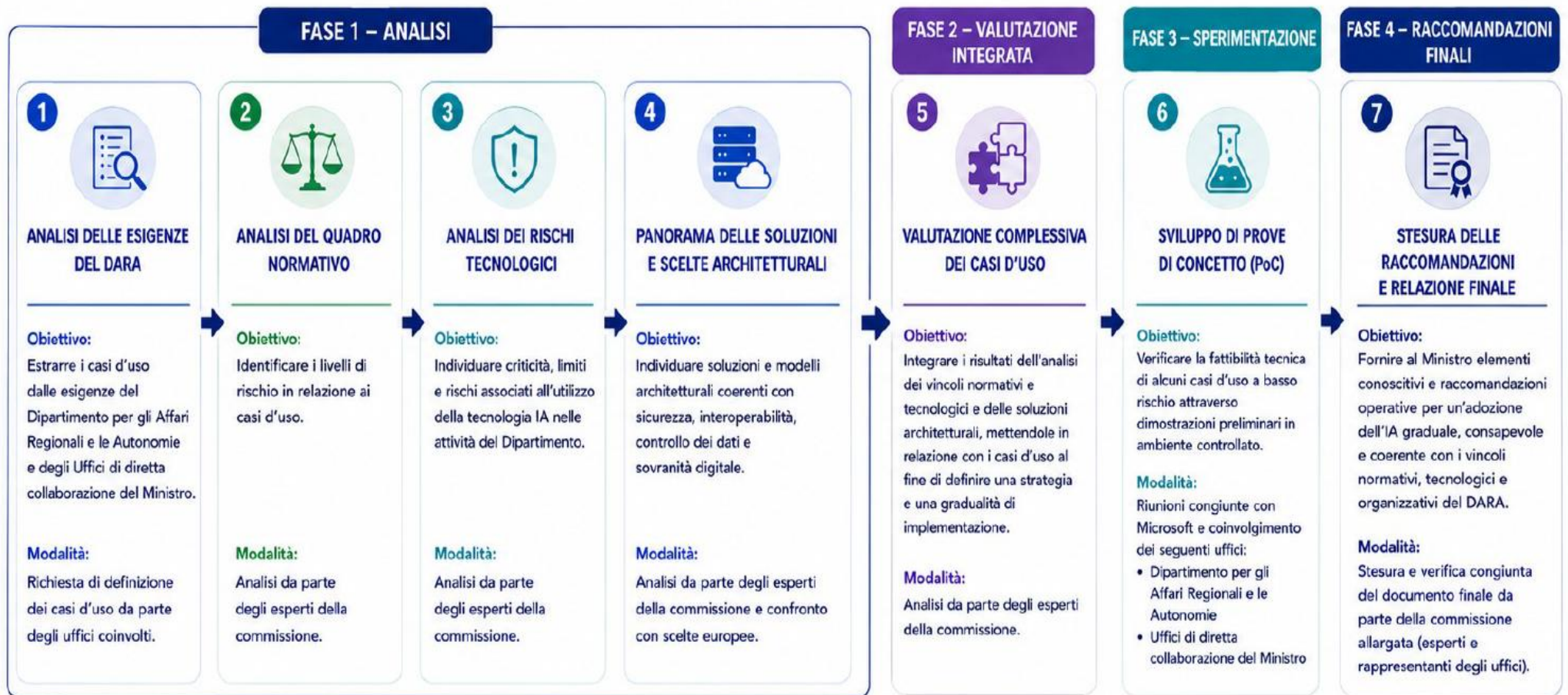
L'elemento maggiormente significativo emerso dal percorso è rappresentato dalla possibilità di tradurre esigenze operative reali in due primi prototipi di [agenti specializzati](#), costruiti in stretta collaborazione con gli uffici coinvolti. Il lavoro svolto ha consentito di passare da una fase iniziale di esplorazione delle potenzialità dell'Intelligenza Artificiale alla realizzazione di due dimostrazioni preliminari, rispettivamente a supporto del Dipartimento per gli affari regionali e le autonomie e degli Uffici di diretta collaborazione del Ministro. Si tratta, in entrambi i casi, di prove non ancora sottoposte a una verifica operativa estesa: prima di poter essere effettivamente impiegate nell'attività quotidiana degli uffici, le soluzioni individuate richiederanno un significativo lavoro di approfondimento tecnico, test più ampi sul campo e un adeguato percorso di formazione del personale coinvolto.

Le prove condotte indicano una direzione di lavoro promettente: l'adozione di strumenti basati su Intelligenza Artificiale può essere affrontata attraverso un approccio graduale, governato e aderente alle specifiche esigenze dell'Amministrazione, valorizzando il patrimonio informativo esistente. Si tratta tuttavia di indicazioni preliminari, da confermare con un percorso di sperimentazione più strutturato prima di poter trarre conclusioni operative.

In tale prospettiva, il progetto costituisce un primo esercizio dimostrativo utile e un possibile riferimento metodologico per future iniziative di collaborazione con Microsoft nella Pubblica Amministrazione, a condizione che alle prove preliminari faccia seguito un percorso di approfondimento, validazione e formazione del personale prima di qualsiasi utilizzo nell'attività amministrativa corrente.

# IL PERCORSO DI LAVORO DELLA COMMISSIONE

Un processo strutturato in sette fasi per valutare, sperimentare e orientare l'adozione dell'Intelligenza Artificiale nel DARA.



**OBIETTIVO GENERALE:** fornire al Ministro un quadro chiaro e operativo per adottare l'IA in modo sicuro, efficace e coerente con gli obiettivi di sovranità digitale e autonomia tecnologica.

# I CASI DI POSSIBILE UTILIZZO DELL'IA NEL DARA

L'Intelligenza Artificiale può supportare le principali funzioni del Dipartimento, migliorando capacità di analisi, accesso alla conoscenza e gestione dei processi documentali.

1



**UFFICIO PER LE AUTONOMIE SPECIALI  
E PER L'ESAME DI LEGITTIMITÀ  
COSTITUZIONALE DELLA LEGISLAZIONE  
DELLE REGIONI E DELLE PROVINCE  
AUTONOME (UFFICIO II)**

- Analisi automatizzata dei testi regionali
- Confronto con la giurisprudenza costituzionale
- Classificazione automatica delle materie

2



**SEGRETERIA DELLA  
CONFERENZA STATO-REGIONI  
E DELLA CONFERENZA  
UNIFICATA**

- Sintesi di documenti
- Comparazione delle posizioni delle Regioni
- Tracciamento dello stato di attuazione delle intese
- Generazione di report periodici

3



**AREE MONTANE,  
MINORANZE LINGUISTICHE,  
AUTONOMIE SPECIALI**

- Gestione di dataset territoriali eterogenei
- Monitoraggio dei programmi pluriennali
- Valutazione comparativa dell'impatto delle politiche

4



**BANCA DATI  
DELLE LEGGI REGIONALI**

- Sistema di interrogazione semantica fondato sui documenti dell'archivio (RAG)

5



**SERVIZIO PER LA  
MODERNIZZAZIONE ISTITUZIONALE  
E ATTIVITÀ INTERNAZIONALE**

- Sintesi di fonti pubbliche
- Comparazione di modelli istituzionali
- Redazione documentale multilingue

6



**SERVIZIO PNRR  
GREEN COMMUNITIES**

- Verifica documentale dei progetti
- Controllo della conformità (DNSH, CAM, milestone)
- Analisi comparativa dei procedimenti
- Rilevazione di anomalie
- Assistenza ai Comuni mediante agenti dedicati

7



**UFFICIO  
DI GABINETTO**

- Agenti tematici di supporto
- Analisi di dossier
- Ricerca e recupero di precedenti
- Sintesi documentale
- Predisposizione di briefing e note
- Supporto ai procedimenti amministrativi

8



**UFFICIO  
LEGISLATIVO**

- Ricerca intelligente di norme e precedenti
- Supporto al drafting legislativo
- Analisi di impatto della regolamentazione (AIR/VIR)
- Analisi degli atti normativi e degli emendamenti
- Redazione di testi normativi
- Predisposizione di note, appunti e testi giuridici
- Predisposizione di pareri
- Agenti dedicati alla gestione degli emendamenti parlamentari e del sindacato ispettivo



Le applicazioni dell'IA hanno finalità di supporto e non sostituiscono il giudizio e la responsabilità umana, nel rispetto della normativa vigente.

# QUADRO NORMATIVO E IMPATTO SUL DARA

L'uso dell'IA nel DARA si realizza nel rispetto delle **regole europee e nazionali** e dei principi fondamentali a tutela dei **diritti, dei dati e della qualità delle decisioni**.

## LE FONTI APPLICABILI



### AI ACT

Approccio basato sul rischio

- classificazione dei sistemi in base al rischio
- obblighi proporzionati al rischio
- supervisione umana e tracciabilità



### LEGGE ITALIANA 132/2025

L'IA come supporto all'attività umana

- conoscibilità del funzionamento
- tracciabilità dell'utilizzo
- formazione del personale



### GDPR E CODICE DEI CONTRATTI PUBBLICI

Tutela dei diritti e controllo umano

- protezione dei dati personali
- divieto di decisioni esclusivamente automatizzate
- comprensibilità delle logiche utilizzate

## PROTEZIONE DEI DATI PERSONALI E TRASFERIMENTI EXTRA-UE



### Dati pubblici e rischio di re-identificazione

Anche dati pubblici possono consentire inferenze su persone, relazioni istituzionali o strategie negoziali.



### Trasferimenti verso fornitori extra-UE

Verificare garanzie giuridiche, utilizzo dei dati e condizioni di trattamento.



### Data residency

Per documenti sensibili, preferire soluzioni con trattamento documentato entro il perimetro UE.



### DPIA

Valutazione d'impatto quando il trattamento può comportare un rischio elevato per i diritti delle persone fisiche.



### Trasparenza

Rendere conoscibile il sistema utilizzato, il suo impiego e la revisione umana effettuata.

## DIRITTO D'AUTORE



### Opere create con l'ausilio dell'IA

La tutela permane quando il risultato è frutto del lavoro intellettuale dell'autore.



### Addestramento dei modelli e text & data mining

L'utilizzo di documenti e contenuti deve rispettare i diritti dei titolari e gli eventuali opt-out.

## ETICA E SUPERVISIONE UMANA



### Supervisione umana

La validazione deve essere sostanziale e svolta da personale qualificato.



### Bias algoritmico

I sistemi possono riprodurre o amplificare squilibri presenti nei dati o nei criteri di ottimizzazione.



### Trasparenza e spiegabilità

Le decisioni devono poter essere comprese, motivate e verificate.



### Divieto di decisione interamente automatizzata

Nessuna decisione amministrativa può essere assunta esclusivamente sulla base di un output algoritmico.



Il quadro normativo rappresenta un vincolo, ma anche una garanzia: **orienta l'innovazione verso trasparenza, tutela dei diritti, protezione dei dati e responsabilità delle decisioni pubbliche.**



# CRITICITÀ E LIMITI DELLA TECNOLOGIA

L'IA offre opportunità, ma presenta rischi tecnici e di sicurezza che vanno conosciuti e gestiti con misure concrete di controllo.

## SICUREZZA INFORMATICA E SOVRANITÀ DIGITALE



### PROMPT INJECTION

Manipolazione dei comandi per alterare il comportamento del sistema e ottenere risposte non autorizzate o dannose.



### ESFILTRAZIONE DI DATI

Rischio di fuoriuscita di informazioni sensibili attraverso risposte, output o canali indiretti.



### SOCIAL ENGINEERING ASSISTITO DALL'IA

Uso dell'IA per ingannare le persone e generare contenuti falsi ma credibili.



### DEEFAKE E CLONAZIONE VOCALE

Produzione di contenuti falsi ma credibili utilizzabili per frodi, manipolazione o danni reputazionali.



### RISCHIO "MOSAICO INFORMATIVO"

Ricostruzione di informazioni sensibili derivante dalla combinazione di dati apparentemente non critici.

## SOVRANITÀ DIGITALE: MANTENERE IL CONTROLLO

Condizione per un uso responsabile dell'IA nel DARA



### CONTROLLO GIURIDICO

Garantire che i dati e i sistemi siano soggetti esclusivamente alla giurisdizione UE/italiana.



### CONTROLLO TECNICO

Preferire soluzioni con data residency in UE e architetture che assicurino la segregazione dei dati.



### CONTROLLO OPERATIVO

Preservare la capacità di gestione, monitoraggio e audit dei sistemi critici.



### RIDUZIONE DELLA DIPENDENZA DA FORNITORI ESTERI

La localizzazione dei dati non garantisce da sola il pieno controllo sulle informazioni strategiche (es. possibili effetti del CLOUD Act).

## LIMITI TECNICI DEI SISTEMI DI IA



### ALLUCINAZIONI

I sistemi di IA possono generare informazioni plausibili ma non corrette o veritiere:

- citazioni giurisprudenziali inesistenti
- norme inventate
- dati statistici falsi

Rischio particolarmente elevato in ambito giuridico.



### OPACITÀ ALGORITMICA

Difficoltà nel ricostruire le ragioni di una risposta o di una proposta decisionale.

In potenziale conflitto con l'obbligo di motivazione dell'azione amministrativa.



### NON RIPRODUCIBILITÀ DEGLI OUTPUT

Stessa domanda, stessa fonte: risposte diverse in momenti diversi. Instabilità dei modelli e mancanza di determinismo.



### VENDOR LOCK-IN

Dipendenza dal fornitore per modelli, piattaforme e formati proprietari.

Riduzione della libertà di scelta e possibili costi di uscita elevati.

## LE CONSEGUENZE PER IL DARA



Rischi per la qualità e l'affidabilità delle attività istituzionali.



Esposizione a responsabilità amministrative e reputazionali.



Impatto sulla sicurezza dei dati e sulla riservatezza delle informazioni.



Possibile perdita di fiducia da parte delle istituzioni e dei cittadini.

## INDICAZIONI OPERATIVE TRASVERSALI



### FORMAZIONE DEL PERSONALE

Investire in competenze per un uso consapevole, sicuro e responsabile dei sistemi di IA.



### SUPERVISIONE UMANA

Validazione sostanziale degli output da parte di personale qualificato.



### PENETRATION TEST PERIODICI

Testare regolarmente i sistemi per individuare vulnerabilità e aggiornare le misure di sicurezza.



### PRINCIPIO DEL MINIMO PRIVILEGIO

Concedere accessi e permessi solo quando necessari e limitati al minimo indispensabile.



### RAG E BASI DOCUMENTALI INTERNE

Utilizzare Retrieval Augmented Generation (RAG) e basi documentali controllate del DARA.



### PROMPT STRUTTURATI E FONTI ESPLICITE

Chiedere al modello di esplicitare fonti, passaggi logici e ragionamento seguito.



### CITAZIONE DELLE FONTI

Indicare sempre le fonti utilizzate per consentire verifica e riscontro.



### REGISTRI E AUDIT TRAIL

Documentare prompt, parametri, fonti e versioni per garantire tracciabilità e possibilità di verifica.



### STANDARD APERTI E INTEROPERABILITÀ

Preferire soluzioni che utilizzano standard aperti e permettono l'export e la migrazione dei dati e dei modelli.



Conoscere i rischi e i limiti tecnici è il primo passo per introdurre l'IA in modo responsabile:  
**controllo, competenza e supervisione umana restano insostituibili.**



# LE SOLUZIONI DISPONIBILI SUL MERCATO

Le scelte tecnologiche richiedono una valutazione congiunta di sicurezza, controllo dei dati, interoperabilità, sostenibilità economica e competenze disponibili.

## DOVE RISIEDONO SISTEMI E DATI?



### CLOUD

#### Vantaggi

- attivazione rapida
- scalabilità
- minori investimenti iniziali

#### Criticità

- minore controllo diretto
- dipendenza dal fornitore



### ON-PREMISE

#### Vantaggi

- maggiore controllo
- autonomia operativa

#### Criticità

- investimenti elevati
- necessità di competenze specialistiche



### ARCHITETTURE IBRIDE

Combinano elementi cloud e componenti sotto controllo diretto dell'amministrazione

- modelli generativi esterni
- dati e basi documentali controllati dall'ente
- maggiore equilibrio tra flessibilità e controllo

## PIATTAFORME STANDARD O SOLUZIONI PERSONALIZZATE?



### PIATTAFORME SaaS

- implementazione veloce
- minori costi iniziali
- personalizzazione limitata



### SOLUZIONI CUSTOM

- progettate sui processi dell'amministrazione
- maggiore controllo e integrazione
- tempi e costi di realizzazione più elevati

## IL MERCATO OGGI



### ECOSISTEMI INTERNAZIONALI

- OpenAI
- Microsoft
- Google
- Anthropic



### MODELLI OPEN SOURCE

- maggiore flessibilità
- personalizzazione avanzata
- necessità di competenze interne

## ESPERIENZE EUROPEE



FRANCIA



ESTONIA



GERMANIA



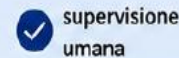
SPAGNA



PORTOGALLO



Approcci differenti, con attenzione crescente a:



supervisione umana



protezione dei dati



interoperabilità



sovranità digitale

## VERSO UN MODELLO GRADUALE DI ADOZIONE DELL'IIA



sperimentazione progressiva e controllata



architetture ibride



dati strategici sotto controllo dell'amministrazione



interoperabilità e portabilità dei dati



valorizzazione progressiva di soluzioni europee e nazionali



riduzione della dipendenza da un singolo fornitore

# RACCOMANDAZIONI DI UTILIZZO DELL'IA

CONDIZIONI DI UTILIZZO PER LE DIVERSE FUNZIONI (1/2)



L'IA SUPPORTA L'ATTIVITÀ AMMINISTRATIVA.  
LA RESPONSABILITÀ RESTA SEMPRE UMANA.

UFFICIO / FUNZIONE	APPLICAZIONI DI IA (come da relazione)	RACCOMANDAZIONI (come da relazione)
<b>1</b>  UFFICIO PER LE AUTONOMIE SPECIALI E PER L'ESAME DI LEGITTIMITÀ COSTITUZIONALE DELLA LEGISLAZIONE DELLE REGIONI E DELLE PROVINCE AUTONOME (UFFICIO II)	<ul style="list-style-type: none"> <li>Analisi automatizzata dei testi regionali</li> <li>Confronto con la giurisprudenza costituzionale</li> <li>Classificazione automatica delle materie</li> </ul>	<ul style="list-style-type: none"> <li>Supervisione umana qualificata</li> <li>Verifica del corretto riparto delle competenze ex art. 117 Cost.</li> <li>Verifica della pertinenza dei precedenti costituzionali</li> <li>Esclusione di automatismi decisionali</li> </ul>
<b>2</b>  SEGRETERIA DELLA CONFERENZA STATO-REGIONI E DELLA CONFERENZA UNIFICATA	<ul style="list-style-type: none"> <li>Sintesi di documenti</li> <li>Comparazione delle posizioni delle diverse Regioni su un tema</li> <li>Tracciamento dello stato di attuazione delle intese</li> <li>Generazione di report periodici</li> </ul>	<ul style="list-style-type: none"> <li>Utilizzo prioritario su documenti approvati o pubblici</li> <li>Revisione dei verbali e delle sintesi</li> <li>Classificazione preventiva della sensibilità dei materiali</li> </ul>
<b>3</b>  AREE MONTANE, MINORANZE LINGUISTICHE, AUTONOMIE SPECIALI	<ul style="list-style-type: none"> <li>Gestione di dataset territoriali eterogenei</li> <li>Monitoraggio dei programmi pluriennali di finanziamento</li> <li>Valutazione comparativa dell'impatto delle politiche</li> </ul>	<ul style="list-style-type: none"> <li>Utilizzo di dati aggregati e pubblicamente disponibili</li> <li>Verifica dell'assenza di bias territoriali</li> <li>DPIA preventiva per applicazioni su larga scala</li> </ul>
<b>4</b>  BANCA DATI DELLE LEGGI REGIONALI	<ul style="list-style-type: none"> <li>Sistema di interrogazione semantica dell'archivio (RAG)</li> </ul>	<ul style="list-style-type: none"> <li>Supervisione umana qualificata</li> <li>Verifica della qualità e dell'aggiornamento delle fonti</li> <li>Tracciabilità delle interrogazioni e dei risultati</li> </ul>

## COME LEGGERE I LIVELLI DI RISCHIO (rif. § 4.9)



**RISCHIO CONTENUTO**

Supporto alla ricerca, consultazione e organizzazione della conoscenza.



**RISCHIO MEDIO**

Supporto all'istruttoria e alla predisposizione di atti, con validazione umana.



**RISCHIO ELEVATO**

Supporto ad attività che incidono su decisioni istituzionali o valutazioni giuridiche.

## CATEGORIE DI RACCOMANDAZIONE (rif. § 4.9)



**ASPETTI GIURIDICI**

Corretta applicazione delle norme, utilizzo di fonti ufficiali, verifiche di legittimità.



**CONTROLLO UMANO**

Supervisione, validazione e responsabilità delle decisioni.



**TECNOLOGIA E QUALITÀ DEI DATI**

Qualità delle basi documentali, affidabilità delle fonti, tracciabilità.



**ARCHITETTURA E GOVERNANCE**





Protezione dei dati, classificazione delle informazioni, audit e misure organizzative.

# RACCOMANDAZIONI DI UTILIZZO DELL'IA

CONDIZIONI DI UTILIZZO PER LE DIVERSE FUNZIONI (2/2)



L'IA SUPPORTA L'ATTIVITÀ AMMINISTRATIVA.  
LA RESPONSABILITÀ RESTA SEMPRE UMANA.

UFFICIO / FUNZIONE	APPLICAZIONI DI IA (come da relazione)	RACCOMANDAZIONI (come da relazione)
<b>5</b>  <b>SERVIZIO PER LA MODERNIZZAZIONE ISTITUZIONALE E ATTIVITÀ INTERNAZIONALE</b>	<ul style="list-style-type: none"> <li>Sintesi di fonti pubbliche</li> <li>Comparazione di modelli istituzionali</li> <li>Redazione documentale multilingue</li> </ul>	<ul style="list-style-type: none"> <li>Supervisione umana qualificata</li> <li>Verifica dell'attendibilità e della pertinenza delle fonti</li> <li>Tracciabilità dei contenuti prodotti</li> <li>Utilizzo di fonti ufficiali e aperte</li> </ul>
<b>6</b>  <b>SERVIZIO PNRR GREEN COMMUNITIES</b>	<ul style="list-style-type: none"> <li>Verifica documentale dei progetti</li> <li>Controllo della conformità (DNSH, CAM, milestone)</li> <li>Analisi comparativa dei procedimenti</li> <li>Rilevazione di anomalie</li> <li>Assistenza ai Comuni mediante agenti dedicati</li> </ul>	<ul style="list-style-type: none"> <li>Validazione umana di ogni esito rilevante</li> <li>Rispetto della normativa PNRR e dei principi (DNSH, CAM)</li> <li>Qualità e aggiornamento continuo delle basi documentali</li> <li>Tracciabilità delle verifiche e dei controlli effettuati</li> </ul>
<b>7</b>  <b>UFFICIO DI GABINETTO</b>	<ul style="list-style-type: none"> <li>Ricerca e recupero di precedenti</li> <li>Sintesi documentale</li> <li>Analisi di dossier</li> <li>Predisposizione di briefing e note</li> <li>Supporto ai procedimenti amministrativi</li> </ul>	<ul style="list-style-type: none"> <li>Supervisione umana qualificata su ogni documento e output</li> <li>Utilizzo di fonti ufficiali e riservate secondo classificazione</li> <li>Protezione dei dati e rispetto delle misure di sicurezza</li> <li>Tracciabilità delle attività e conservazione dei log</li> </ul>
<b>8</b>  <b>UFFICIO LEGISLATIVO</b>	<ul style="list-style-type: none"> <li>Ricerca intelligente di norme e precedenti</li> <li>Supporto al drafting legislativo</li> <li>Analisi di impatto della regolamentazione (AIR/VIR)</li> <li>Analisi degli atti normativi e degli emendamenti</li> <li>Redazione di testi normativi</li> <li>Predisposizione di note, appunti e testi giuridici</li> <li>Predisposizione di pareri</li> <li>Agenti dedicati alla gestione degli emendamenti parlamentari e del sindacato ispettivo</li> <li>Contributi al contenzioso costituzionale</li> </ul>	<ul style="list-style-type: none"> <li>Supervisione e validazione umana di testi, pareri e atti</li> <li>Verifica di legittimità, correttezza normativa e coerenza sistematica</li> <li>Qualità, aggiornamento e autorevolezza delle fonti giuridiche</li> <li>Tracciabilità delle operazioni e conservazione delle versioni</li> </ul>

## COME LEGGERE I LIVELLI DI RISCHIO (rif. § 4.9)

### RISCHIO CONTENUTO

Supporto alla ricerca, consultazione e organizzazione della conoscenza.

### RISCHIO MEDIO

Supporto all'istruttoria e alla predisposizione di atti, con validazione umana.

### RISCHIO ELEVATO

Supporto ad attività che incidono su decisioni istituzionali o valutazioni giuridiche.

## CATEGORIE DI RACCOMANDAZIONE (rif. § 4.9)



### ASPETTI GIURIDICI

Corretta applicazione delle norme, utilizzo di fonti ufficiali, verifiche di legittimità.



### CONTROLLO UMANO

Supervisione, validazione e responsabilità delle decisioni.



### TECNOLOGIA E QUALITÀ DEI DATI

Qualità delle basi documentali, affidabilità delle fonti, tracciabilità.



### ARCHITETTURA E GOVERNANCE

Protezione dei dati, classificazione delle informazioni, audit e misure organizzative.

# CASO D'USO: SPERIMENTAZIONE DELL'ECOSISTEMA MICROSOFT

Scelta dettata da praticità – Casi selezionati a basso rischio

**i** La sperimentazione dell'ecosistema Microsoft costituisce un caso di studio e una prova di fattibilità. Non rappresenta una raccomandazione esclusiva né una strategia centrata su un singolo fornitore.



## 1) UTILIZZO DELL'ECOSISTEMA MICROSOFT PER MOTIVI DI PRATICITÀ

L'ecosistema Microsoft è già disponibile e integrato negli strumenti in uso al DARA, con adeguati standard di sicurezza e conformità.



## 2) CASI D'USO A BASSO RISCHIO

I casi selezionati riguardano attività documentali e di ricerca con limitato impatto decisionale, quindi classificati a basso rischio secondo l'AI Act.



## OBIETTIVO DELLA SPERIMENTAZIONE

Valutare l'efficacia operativa, i benefici in termini di efficienza e la qualità dei risultati, assicurando sempre controllo umano e supervisione.

## I DUE PoC SPERIMENTATI (DIMOSTRAZIONI PRELIMINARI SU CASI A BASSO RISCHIO)



### TAVOLO 1 – Dipartimento Ricerca e Documentazione

#### OBIETTIVO

Supportare l'attività di ricerca, consultazione e sintesi documentale per migliorare tempi e qualità dell'analisi.

#### DESCRIZIONE del PoC

È stato progettato e realizzato, a titolo dimostrativo, un primo prototipo di agente dedicato al Dipartimento, pensato per supportare gli utenti nella consultazione della documentazione, nell'identificazione delle informazioni rilevanti, nella sintesi di testi complessi e nella predisposizione di elaborazioni strutturate utili alle attività degli uffici.

#### FUNZIONALITÀ PRINCIPALI

- Ricerca semantica su documenti e fonti interne.
- Sintesi di documenti e produzione di riassunti strutturati.
- Supporto nella preparazione di note, bozze e schemi preliminari.
- Individuazione di informazioni chiave e collegamenti tra temi.



### TAVOLO 2 – Dipartimento Analisi e Contenzioso

#### OBIETTIVO

Assistere le attività di analisi e preparazione dei documenti in ambito contenzioso e normativo.

#### DESCRIZIONE del PoC

È stato sviluppato, a titolo dimostrativo, un primo prototipo di agente specializzato nel supporto alle attività di analisi giuridica e contenziosa, per agevolare la ricerca di precedenti, la redazione di bozze e la strutturazione di documenti di lavoro.

#### FUNZIONALITÀ PRINCIPALI

- Ricerca di precedenti e riferimenti normativi.
- Analisi di documenti e estrazione di elementi rilevanti.
- Supporto alla redazione di bozze di memorie, osservazioni e pareri.
- Organizzazione e strutturazione di atti e documenti complessi.



### DIMOSTRAZIONI PRELIMINARI – NON ANCORA SOTTOPOSTE A VERIFICA OPERATIVA ESTESA

I due PoC rappresentano dimostrazioni preliminari di fattibilità su casi d'uso a basso rischio. Non sono ancora stati sottoposti a una verifica operativa estesa. La loro estensione o adozione richiederà valutazioni ulteriori in termini di efficacia, sicurezza, integrazione e impatti sui processi.



### LEZIONE PRINCIPALE

La sperimentazione consente di apprendere, misurare e orientare le scelte future verso architetture flessibili, interoperabili e coerenti con gli obiettivi di sovranità digitale e autonomia tecnologica.

# RACCOMANDAZIONI OPERATIVE PER L'ADOZIONE DELL'IA

*Dalle sperimentazioni ai sistemi operativi:  
una strategia graduale, interoperabile e orientata alla sovranità digitale.*



LA COMMISSIONE NON RACCOMANDA  
UNA PIATTAFORMA SPECIFICA.

La piattaforma è meno importante  
dell'architettura e della strategia:  
è preferibile evitare dipendenze  
da un singolo ecosistema  
ed evitare di dipendere  
da un unico fornitore.

1

**ADOTTARE UN  
APPROCCIO  
GRADUALE**



- ✓ Partire dai casi d'uso a rischio contenuto.
- ✓ Definire criteri di successo prima della sperimentazione.
- ✓ Estendere l'utilizzo solo dopo verifica dei risultati.

2

**DIFFERENZIARE  
LE SOLUZIONI  
IN BASE AL RISCHIO**



- **ATTIVITÀ DOCUMENTALI E DI RICERCA**  
→ possibile utilizzo di piattaforme SaaS mature.
- **ATTIVITÀ ISTRUTTORIE**  
→ maggiore controllo delle basi documentali.
- **ATTIVITÀ GIURIDICHE, CONTENZIOSO E NEGOZIATI**  
→ massime garanzie di controllo, tracciabilità e supervisione.

3

**COSTRUIRE  
ARCHITETTURE  
IBRIDE**



- ✓ Modelli generalisti anche in cloud.
- ✓ Dati strategici e basi documentali sotto controllo diretto.
- ✓ Interoperabilità e portabilità dei dati.
- ✓ Clausole di exit e reversibilità.

4

**RAFFORZARE  
LA SOVRANITÀ  
DIGITALE**



- ✓ Evitare il vendor lock-in.
- ✓ Diversificare i fornitori.
- ✓ Utilizzare standard aperti.
- ✓ Sviluppare competenze interne.
- ✓ Mantenere capacità di scelta autonoma.

5

**VALORIZZARE  
L'ECOSISTEMA  
EUROPEO E NAZIONALE**



- ✓ Valutare progressivamente, accanto alle piattaforme internazionali, soluzioni europee e nazionali.
- ✓ Favorire interoperabilità e controllo dei dati.
- ✓ Rafforzare autonomia tecnologica e resilienza.

**ESEMPI DI ECOSISTEMA  
EUROPEO E NAZIONALE**



**MISTRAL AI**  
(Francia)



**MINERVA**  
(Italia)



**ALTRI MODELLI  
E SERVIZI**  
conformi ai requisiti  
europei di sovranità  
digitale



**MESSAGGIO  
CHIAVE**

Sperimentare sui casi d'uso a rischio contenuto, adottare progressivamente soluzioni interoperabili e mantenere nel tempo il controllo su dati, processi e scelte tecnologiche.



## *Presidenza del Consiglio dei Ministri*

Istituzione di una Commissione di studio con il compito di svolgere attività di supporto e consulenza al Ministro sull'applicazione dell'Intelligenza Artificiale alle questioni e ai temi di competenza concernenti gli affari regionali e le autonomie.

### IL MINISTRO PER GLI AFFARI REGIONALI E LE AUTONOMIE

- VISTA la legge 23 agosto 1988, n. 400, recante "Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri";
- VISTO il decreto legislativo 30 luglio 1999, n. 303, recante "Ordinamento della Presidenza del Consiglio dei ministri, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59" e, in particolare, l'articolo 4, comma 3, che prevede un apposito Dipartimento per gli affari regionali ai fini dell'esercizio dei compiti del Presidente del Consiglio in materia di rapporti con il sistema delle autonomie;
- VISTO il decreto legislativo 30 marzo 2001, n. 165, recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";
- VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- VISTO il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale";
- VISTA la legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la regressione della corruzione e dell'illegalità della pubblica amministrazione";
- VISTO il decreto legislativo 8 aprile 2013, n. 39, recante "Disposizioni in materia inconfiribilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012 n. 190";



## *Presidenza del Consiglio dei Ministri*

- VISTO** il decreto del Presidente della Repubblica 16 aprile 2013, n. 62, concernente “Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell’articolo 54 del decreto legislativo 30 marzo 2001, n. 165”, come modificato dal decreto del Presidente della Repubblica 13 giugno 2023, n. 81;
- VISTO** il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- VISTO** il decreto del Ministro per gli affari regionali e le autonomie 1° settembre 2016, recante “Organizzazione e funzionamento del Dipartimento per gli affari regionali e le autonomie”, come, da ultimo, modificato dal decreto del Ministro per gli affari regionali e le autonomie del 28 marzo 2023, a seguito dell’adozione del decreto del Presidente del Consiglio dei Ministri 3 marzo 2023, di modifica, tra l’altro, dell’articolo 12 del decreto del Presidente del Consiglio dei Ministri 1° ottobre 2012, recante “Ordinamento delle strutture generali della Presidenza del Consiglio dei ministri”;
- VISTO** il decreto del Presidente della Repubblica 21 ottobre 2022, con il quale il Sen. Roberto Calderoli è stato nominato Ministro senza portafoglio;
- VISTO** il decreto del Presidente del Consiglio dei ministri 23 ottobre 2022, con cui al Ministro Roberto Calderoli è stato conferito l’incarico per gli affari regionali e le autonomie;
- VISTO** il decreto Presidente del Consiglio dei ministri 12 novembre 2022, con cui al Ministro Roberto Calderoli sono state delegate le funzioni in materia di affari regionali e autonomie, e, in particolare, l’articolo 2, comma 1, lettera b), secondo cui il Ministro per gli affari regionali e le autonomie è delegato a costituire e regolare commissioni di studio e consulenza e gruppi di lavoro nelle materie oggetto del decreto medesimo, nominandone altresì i componenti;



## *Presidenza del Consiglio dei Ministri*

- VISTO** il decreto del Presidente del Consiglio dei ministri 12 gennaio 2024, recante “Piano triennale per l’informatica nella Pubblica amministrazione 2024-2026”, come modificato dal decreto del Presidente del Consiglio dei ministri 3 dicembre 2024, recante “Aggiornamento 2025 del Piano triennale 2024-2026”;
- VISTO** il decreto del Presidente del Consiglio dei ministri 10 aprile 2024, recante “Regolamento di autonomia finanziaria e contabile della Presidenza del Consiglio dei ministri”;
- VISTO** il decreto del Presidente del Consiglio dei ministri 13 dicembre 2024, recante “Codice di comportamento e di tutela della dignità e dell’etica dei dirigenti e dei dipendenti della Presidenza del Consiglio dei ministri”;
- VISTO** il decreto del Presidente del Consiglio dei ministri 23 dicembre 2024, concernente l’approvazione del bilancio di previsione della Presidenza del Consiglio dei ministri per l’anno 2025 e per il triennio 2025-2027;
- VISTA** la legge 30 dicembre 2024, n. 207 recante “Bilancio di previsione dello Stato per l’anno finanziario 2025 e bilancio pluriennale per il triennio 2025 – 2027”;
- VISTO** il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull’Intelligenza Artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull’Intelligenza Artificiale);
- VISTA** la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01);
- VISTO** il documento recante la “Strategia italiana per l’Intelligenza Artificiale 2024-2026”, pubblicato il 12 luglio 2024;
- VISTO** il decreto legislativo 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione europea;



## *Presidenza del Consiglio dei Ministri*

**RITENUTA** la necessità di avvalersi, per le iniziative che potranno essere promosse in materia di Intelligenza Artificiale, di una Commissione di studio, composta da qualificati esperti, a fini di supporto tecnico e di consulenza sulle prospettive dell'Intelligenza Artificiale riferita alle attività di competenza del Ministro per gli affari regionali e le autonomie e del Dipartimento per gli affari regionali e le autonomie quali: redazione di testi normativi, gestione amministrativa del personale, rapporti Stato, Regioni ed enti locali nell'ambito delle Conferenze, esame delle leggi regionali;

### **DECRETA**

#### **Articolo 1**

*(Istituzione e compiti)*

1. È istituita, presso la Presidenza del Consiglio dei ministri – uffici del Ministro per gli affari regionali e le autonomie, una Commissione di studio con il compito di svolgere attività di elaborazione, supporto e consulenza al Ministro sull'applicazione dell'Intelligenza Artificiale alle questioni e ai temi di competenza, concernenti gli affari regionali e le autonomie.
2. La Commissione opera in piena autonomia. Nell'ambito dei compiti di cui al comma 1, la Commissione esamina le prospettive di utilizzo dell'Intelligenza Artificiale, riferite alle attività di competenza del Ministro per gli affari regionali e le autonomie e del Dipartimento per gli affari regionali e le autonomie, ai fini degli eventuali adattamenti organizzativi e funzionali conseguenti.
3. La Commissione, a conclusione della propria attività, predispone una relazione al Ministro per gli affari regionali e le autonomie, con la quale dà conto dell'attività svolta e formula proposte relative agli adattamenti e agli interventi ritenuti necessari. La Commissione, prima della relazione conclusiva, può predisporre propri documenti e analisi.
4. In relazione ai temi oggetto di approfondimento, la Commissione può procedere ad audizioni e acquisire documenti, contributi e proposte da rappresentanti di organi dello Stato, di Regioni e Province autonome ed enti locali nonché da qualificati esperti e operatori nei settori oggetto dell'attività.

#### **Articolo 2**



# *Presidenza del Consiglio dei Ministri*

*(Composizione)*

1. La Commissione è così composta:
  - a) Pres. Mario Luigi Torsello, Presidente di Sezione del Consiglio di Stato a.r., che la presiede;
  - b) Prof.ssa Barbara Caputo, Professore ordinario di Ingegneria automatica e Informatica presso il Politecnico di Torino;
  - c) Prof. Paolo Ferragina, Professore ordinario di Informatica presso la Scuola superiore Sant'Anna di Pisa;
  - d) Prof. Gianluigi Greco, Professore ordinario di Informatica presso l'Università della Calabria;
  - e) Prof. Oreste Pollicino, Professore ordinario di Diritto costituzionale e Regolazione dell'Intelligenza Artificiale, presso l'Università Bocconi di Milano;
  - f) Prof.ssa Paola Velardi, Professore ordinario di Informatica presso l'Università La Sapienza di Roma;
  - g) Ing. Mario Nobile, Direttore generale dell'Agenzia per l'Italia digitale-AGID.
  
2. Fanno altresì parte della Commissione, per l'amministrazione di riferimento:
  - a) Cons. Maria Schininà, Capo del settore legislativo del Ministro per gli affari regionali e le autonomie;
  - b) Dott.ssa Carolina Anecchiarico, Vice Capo di Gabinetto del Ministro per gli affari regionali e le autonomie, coordinatrice della segreteria della Commissione;
  - c) Min. Plen. Pierluigi Trombetta, Consigliere diplomatico del Ministro per gli affari regionali e le autonomie;
  - d) Cons. Valerio Di Porto, Consigliere per l'autonomia differenziata e il PNRR del Ministro per gli affari regionali e le autonomie;
  - e) Dott. Gian Luca Berruti, Consigliere del Ministro per gli affari regionali e le autonomie per l'Intelligenza Artificiale e la Cybersicurezza nazionale;
  - f) Ing. Daniele Pianura, coordinatore del Servizio per la comunicazione, nell'ambito dell'Ufficio per gli affari giuridici, le autonomie locali, le minoranze linguistiche e la comunicazione del Dipartimento per gli affari regionali e le autonomie;
  - g) Dott. Luca Colombatto, coordinatore del Servizio I presso il Nucleo PNRR Stato-Regioni, istituito nell'ambito del Dipartimento per gli affari regionali e le autonomie;
  
3. Fanno inoltre parte della Commissione i seguenti rappresentanti tecnici:



## *Presidenza del Consiglio dei Ministri*

- a) Dott. Danilo Capitanio, funzionario responsabile dei Rapporti con il Parlamento della Conferenza delle Regioni e delle Province autonome, in rappresentanza della stessa;
  - b) Dott.ssa Claudia Giovannini, Capo area, responsabile delle Conferenze nell'ambito dell'Associazione nazionale comuni italiani (ANCI), in rappresentanza della medesima associazione;
  - c) Prof. Fabrizio Silvestri, in rappresentanza dell'Unione delle Province d'Italia (UPI).
4. Possono partecipare ai lavori della Commissione il cons. Claudio Tucciarelli, Capo di Gabinetto del Ministro per gli affari regionali e le autonomie nonché il Cons. Paola D'Avena, Capo del Dipartimento per gli affari regionali e le autonomie.
  5. Le funzioni di segreteria della Commissione sono svolte dall'Ufficio di Gabinetto del Ministro per gli affari regionali e le autonomie e, ove necessario, da ulteriori unità di personale degli Uffici di diretta collaborazione del medesimo Ministro.

### **Articolo 3**

*(Profili organizzativi e durata)*

1. La Commissione si riunisce presso gli Uffici del Ministro per gli affari regionali e le autonomie ovvero da remoto, in videoconferenza.
2. La Commissione è convocata dal Presidente, che ne determina le modalità organizzative e il funzionamento.
3. Il Presidente e i componenti della Commissione svolgono la propria attività a titolo gratuito, salvo l'eventuale rimborso, a richiesta, delle spese di trasporto, adeguatamente giustificate e documentate, per i soli componenti non residenti né domiciliati nel territorio di Roma Capitale che partecipino alle riunioni della Commissione in presenza. Per i componenti non residenti né domiciliati nel territorio di Roma Capitale che partecipino in presenza alle riunioni della Commissione è, altresì, previsto l'eventuale rimborso, a richiesta, delle spese di soggiorno e per i pasti, opportunamente giustificate e documentate, secondo i criteri dettati dalla vigente normativa applicata nella Presidenza del Consiglio dei ministri. I relativi oneri gravano sul capitolo 442 del Centro di responsabilità 7 – Affari regionali e autonomie del bilancio di previsione della Presidenza del Consiglio dei ministri per l'anno 2025 e per il triennio 2025-2027. I rimborsi delle spese di cui al primo e al secondo periodo del presente



## *Presidenza del Consiglio dei Ministri*

comma sono riconosciuti nel limite delle risorse disponibili, previa verifica della capienza dello stanziamento.

4. La Commissione conclude i propri lavori entro il 30 giugno 2026, salvo proroga.
5. Il presente decreto è comunicato ai componenti della Commissione a cura del Dipartimento per gli affari regionali e le autonomie, che provvede altresì alla trasmissione agli organi di controllo per gli adempimenti di competenza.

Il presente decreto è trasmesso ai competenti organi di controllo.

Roma, 11 settembre 2025

*Roberto Calderoli*



Firmato digitalmente da  
CALDEROLI ROBERTO  
C=IT  
O= PRESIDENZA CONSIGLIO DEI  
MINISTRI