RegioneLombardia
IL CONSIGLIO

INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE:

OPPORTUNITA', RISCHI, ASPETTATIVE

Policy paper

Studi e ricerche - XII Legislatura

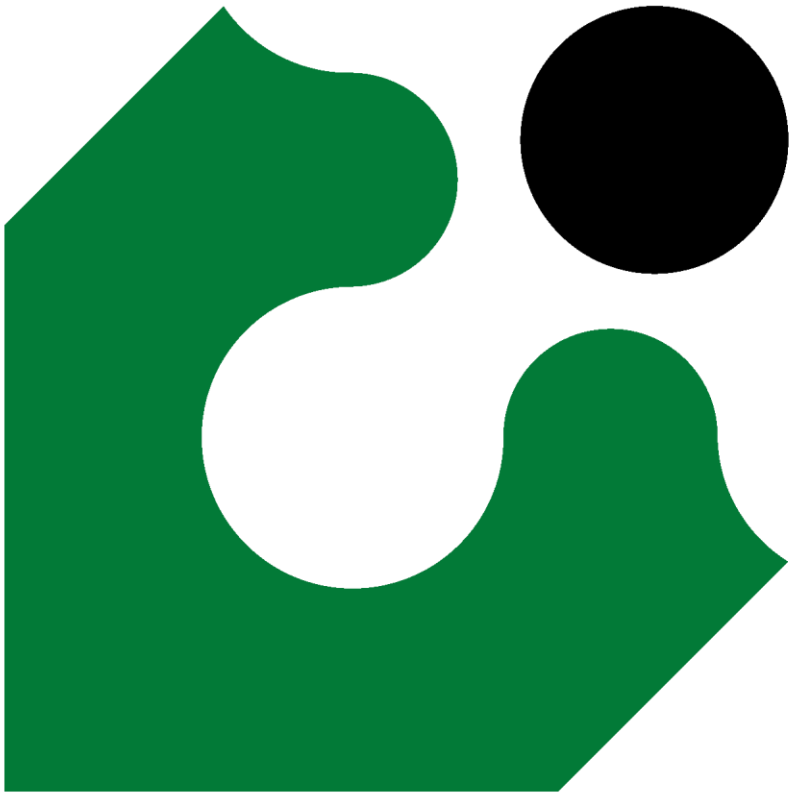
Intelligenza artificiale nella Pubblica Amministrazione: opportunità, rischi, aspettative

Policy paper

Rapporto finale

Codice PoliS-Lombardia 251325IST

Novembre 2025



Intelligenza artificiale nella Pubblica Amministrazione: opportunità, rischi, aspettative

Il Policy paper è promosso dal Consiglio Regionale della Lombardia nell'ambito delle iniziative di ricerca e studio previste dalla Convenzione per la XII legislatura con Polis-Lombardia
(Codice PoliS-Lombardia: 251325IST)

Struttura referente per il Consiglio regionale della Lombardia Servizio Studi, Valutazione delle Politiche e Qualità della Normazione
Dirigente responsabile: Silvia Snider

PoliS-Lombardia
Dirigente di riferimento: Raffaello Vignali
Project Leader: Antonio Dal Bianco

Gruppo di ricerca:
Alessio di Marco, Ioletta Pannocchia, Fondazione Promo Pa, Sebastiano Zorzi

PoliS-Lombardia è certificato UNI EN ISO 9001:2015

PoliS-Lombardia
Via Taramelli, 26 - 20124 Milano
www.polis.lombardia.it

INDICE

Capitolo 1 - Intelligenza artificiale e Pubblica amministrazione

1.1 Introduzione

L'intelligenza artificiale (IA) è divenuta, in pochi anni, un tema cruciale per l'agenda pubblica globale. Il suo impatto potenziale sul funzionamento delle amministrazioni, sull'elaborazione delle politiche e sul rapporto tra istituzioni e cittadini ha trasformato l'IA in una questione che non riguarda solo l'innovazione tecnologica, ma anche il modo in cui viene esercitato il potere pubblico e tutelata la democrazia.

In questo contesto, le pubbliche amministrazioni si trovano a confrontarsi con un duplice compito: da un lato, cogliere le opportunità offerte dall'adozione di strumenti basati sull'IA per migliorare l'efficienza, la qualità e l'accessibilità dei servizi; dall'altro, garantire che tali strumenti siano compatibili con i principi di legalità, trasparenza, responsabilità e tutela dei diritti fondamentali.

Il policy paper si colloca all'interno di questa transizione, offrendo un quadro analitico e orientativo rivolto in particolare alle amministrazioni regionali e locali. Esso si propone di supportare il Consiglio regionale della Lombardia nel valutare, con consapevolezza e competenza, le opportunità e i rischi connessi all'adozione dell'IA, sulla base delle più recenti evoluzioni normative, istituzionali e scientifiche.

Il documento non si limita a descrivere lo stato dell'arte, ma mira a fornire chiavi di lettura utili per interpretare le trasformazioni in corso, definire priorità strategiche e accompagnare le scelte pubbliche con strumenti coerenti con i valori democratici e con le specificità del contesto territoriale.

1.2 Evoluzione recente dell'IA e rilevanza pubblica

Negli ultimi cinque anni, l'intelligenza artificiale ha conosciuto un'accelerazione senza precedenti. Questa crescita ha riguardato sia le performance tecniche dei modelli, sia la loro diffusione capillare in diversi settori, pubblici e privati. L'emergere e la rapida diffusione dell'IA generativa – in particolare dei modelli linguistici di grandi dimensioni (LLM) e delle tecniche di deep learning – ha trasformato radicalmente il modo in cui vengono prodotti contenuti, prese decisioni e gestite informazioni. La disponibilità pubblica di questi modelli a partire dal 2022 ha ampliato notevolmente la platea degli utilizzatori, generando nuove capacità operative nei settori della comunicazione, dell'analisi, dell'assistenza e della progettazione (Taeihagh 2025; Capolupo Adinolfi 2023; OECD 2024 Recommendation).

Questa accelerazione tecnologica è stata accompagnata da un salto qualitativo nella maturità e affidabilità dei modelli. Secondo l'AI Index Report 2025 (Maslej et al. 2025), si osserva un miglioramento costante delle performance sui benchmark standardizzati e una crescita significativa dell'utilizzo di risorse computazionali. Parallelamente, l'interesse per l'IA nella pubblica amministrazione è cresciuto rapidamente. Non più confinata a settori come la sanità o la fiscalità, l'IA viene oggi utilizzata per supportare funzioni predittive, ottimizzare la gestione delle risorse, migliorare l'interazione con i cittadini e affiancare le decisioni amministrative (OECD 2024 – Governing with AI; Capolupo Adinolfi 2023; Menéndez Sebastián 2023).

Questo utilizzo esteso si manifesta in ambiti concreti come l'automazione dell'analisi documentale, l'impiego di assistenti virtuali, la gestione di segnalazioni, la redazione automatica di atti e la verifica di conformità normativa (Morando, 2024, OECD 2024 G7 Toolkit). Le strategie nazionali e internazionali ne riconoscono il valore strategico, promuovendo l'adozione dell'IA per innovare i processi pubblici, ridurre gli oneri burocratici e aumentare l'efficienza e la qualità dei servizi.
Questa trasformazione rende evidente che l'IA non è più una questione esclusivamente tecnica. È ormai una sfida profondamente politica e strategica. La sua adozione solleva interrogativi cruciali su trasparenza, responsabilità, imparzialità e impatto sui diritti fondamentali (UNESCO 2024; Menéndez Sebastián 2023). Come osserva l'UNESCO (2024), le tecnologie generative possono alterare le dinamiche della sfera pubblica, amplificare i rischi di disinformazione e rafforzare forme opache di influenza algoritmica, con conseguenze rilevanti sulla fiducia democratica.
Già da qualche anno, la Comunità Europea, ad esempio attraverso il lavoro del Gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG, 2020), evidenzia l'importanza di criteri come la spiegabilità, il controllo umano, la protezione dei dati e l'equità come condizioni necessarie per un utilizzo legittimo e affidabile dell'IA. L'adozione dell'IA nel settore pubblico richiede pertanto un approccio multidisciplinare e integrato, capace di combinare innovazione tecnologica, consapevolezza normativa e sensibilità istituzionale (Capolupo Adinolfi 2023).
La questione non è più se adottare l'IA, ma come farlo salvaguardando l'equilibrio tra efficienza e garanzie (Menéndez Sebastián, 2023). La trasformazione digitale della pubblica amministrazione non può prescindere da un ripensamento dei rapporti tra cittadino e istituzione, dalla valorizzazione della partecipazione e dall'affermazione dei principi della buona amministrazione. In questo senso, l'IA rappresenta una leva potenziale di innovazione pubblica, ma anche un banco di prova per la capacità delle istituzioni di governare il cambiamento secondo i valori democratici.

1.3 Implicazioni per la governance, l'amministrazione e la democrazia

L'intelligenza artificiale rappresenta una forza trasformativa per il settore pubblico, con il potenziale di rivoluzionarne il funzionamento e l'interazione con i cittadini, inserendosi nel più ampio contesto della trasformazione digitale e della "governance pubblica" (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023; UNESCO, 2024). Questo cambiamento profondo solleva dibattiti intensi, presentando sia notevoli opportunità per migliorare l'efficienza e la qualità dei servizi, sia complessi rischi e dilemmi che toccano i principi fondamentali dell'azione pubblica e i diritti dei cittadini (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023). Alla luce di queste potenzialità trasformative, è possibile individuare una serie di opportunità e rischi che l'adozione dell'intelligenza artificiale nella pubblica amministrazione comporta, tanto in termini operativi quanto per le implicazioni etiche e democratiche.

1.3.1 Opportunità

- Efficienza operativa: l'IA può migliorare l'efficienza dei processi organizzativi, ridurre i costi e ottimizzare i flussi di lavoro, contribuendo alla semplificazione amministrativa e a una gestione più rapida ed efficace (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023; Green, 2024).
- Supporto decisionale: l'analisi di grandi volumi di dati consente un processo decisionale più informato e tempestivo, favorendo la "buona amministrazione" e migliorando la

progettazione e la valutazione delle politiche pubbliche (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023; Green, 2024).

- Accessibilità ai servizi: l'impiego di assistenti virtuali e chatbot migliora l'interazione tra amministrazioni e cittadini, rendendo i servizi più accessibili e usabili, anche per utenti con minori competenze digitali (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023).
- Personalizzazione delle politiche: traendo spunto anche da esperienze del settore privato, l'IA consente la personalizzazione dei servizi pubblici e l'individuazione più precisa dei destinatari (Capolupo Adinolfi, 2023).
- Reattività istituzionale: l'IA può migliorare la gestione di emergenze e scenari complessi attraverso algoritmi predittivi, contribuendo a una allocazione più efficace delle risorse (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023).

1.3.2 Rischi e dilemmi

- Discriminazioni algoritmiche: l'uso di dati incompleti o distorti può generare effetti discriminatori, con rischi per gruppi vulnerabili. È necessario garantire audit, uso di dati di qualità e rispetto del principio di non discriminazione (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023; Maslej. 2025; UNESCO, 2024).
- Opacità: l'assenza di trasparenza e la complessità tecnica degli algoritmi ostacolano la comprensione delle decisioni automatizzate, compromettendo la motivazione degli atti e la possibilità di contestazione. Sebbene la spiegabilità perfetta non sia sempre realizzabile, la trasparenza dovrebbe essere il principio predefinito, esteso anche alla fase di progettazione.
- Accountability ambigua: la responsabilità per decisioni automatizzate può risultare frammentata o non definita. La governance dell'IA richiede chiarezza nei ruoli, tracciabilità dei processi e meccanismi di audit efficaci.
- Eccessiva delega all'IA: l'automazione non può sostituire competenze umane fondamentali come empatia e giudizio. È essenziale definire il livello accettabile di automazione e garantire una mediazione umana consapevole.
- Compromissione dei diritti: l'adozione dell'IA deve avvenire nel rispetto dei diritti fondamentali, della privacy e della protezione dei dati. Il bilanciamento tra efficienza e garanzie richiede attenzione specifica agli impatti della sorveglianza e all'equità nell'accesso ai servizi. Normative come l'AI Act mirano a proteggere i diritti fondamentali e la sicurezza.
- Tecnocrazia decisionale: l'integrazione dell'IA nella governance pubblica solleva interrogativi sul ruolo della tecnologia nei processi decisionali, specie quando l'automazione rischia di ridurre la discrezionalità e il controllo umano (Menéndez Sebastián, 2023). L'eccessiva delega a sistemi opachi può concentrare il potere in pochi attori e compromettere la trasparenza e i valori che guidano l'azione pubblica (Taeihagh, 2025). Le decisioni algoritmiche non sono neutre: richiedono un governo pubblico dei dati e una chiara distinzione tra ambiti vincolati e discrezionali (Menéndez Sebastián, 2023; Taeihagh, 2025). La governance dell'IA deve essere anche etica e politica, e includere la partecipazione dei cittadini per rafforzare la legittimità democratica (UNESCO, 2024).
- Frammentazione normativa: il quadro giuridico attuale è ancora parziale e disomogeneo. Le strategie nazionali e l'AI Act europeo cercano di armonizzare, ma permane la necessità di una

governance multilivello coerente (Capolupo Adinolfi, 2023; Menéndez Sebastián, 2023; Carta, 2024).

- Una gestione efficace e responsabile dell'IA richiede consapevolezza istituzionale, un approccio normativo solido e una governance capace di massimizzare i benefici mitigando i rischi, sempre ponendo il cittadino al centro.

1.4 Tendenze internazionali nella regolazione e nell'adozione dell'IA

L'AI Act europeo

Il Regolamento (UE) 2024/1689 costituisce il primo tentativo globale di introdurre una regolazione orizzontale e vincolante sull'intelligenza artificiale, collocandosi come normativa pionieristica in ambito internazionale (Carta, 2024; Outeda, 2024). Il suo impianto si fonda su un approccio basato sul rischio, che prevede obblighi differenziati in funzione del livello di pericolosità dei sistemi IA, con particolare attenzione alla tutela dei diritti fondamentali, della sicurezza e della democrazia.

Le implicazioni per le pubbliche amministrazioni europee sono rilevanti: esse sono riconosciute come utenti e talvolta anche fornitori di soluzioni IA e pertanto soggette a requisiti specifici in termini di trasparenza, sicurezza, controllo umano e documentazione (PSTW, 2024; OECD, 2024). L'AI Act si inserisce inoltre in un quadro etico consolidato, collegandosi direttamente alle raccomandazioni formulate dall'AI HLEG nel 2019, in favore di un'IA affidabile, antropocentrica e responsabile (AI HLEG, 2019; European Commission, 2019).

Il quadro multilaterale

Accanto all'azione normativa dell'Unione Europea, si registra il crescente coinvolgimento di organismi multilaterali nella definizione di standard e strumenti per un uso responsabile dell'IA nel settore pubblico. L'OCSE promuove principi condivisi e ha sviluppato strumenti operativi concreti, come il G7 Toolkit on AI in the Public Sector, pensato per aiutare le amministrazioni a valutare i rischi e le opportunità dell'adozione algoritmica (OECD, 2024; OECD/UNESCO, 2024).

L'UNESCO, da parte sua, sottolinea il nesso critico tra intelligenza artificiale, diritti umani e democrazia e invita a costruire una governance trasparente, partecipativa e responsabile dei sistemi intelligenti (UNESCO, 2024; UNESCO, 2022). In parallelo, il G7 sostiene il coordinamento tra Stati nella definizione di regole comuni, con particolare attenzione alle applicazioni pubbliche e ai contesti ad alto impatto sociale (OECD/UNESCO, 2024).

Le PA locali come attori chiave

Nel processo di attuazione dell'AI Act, le pubbliche amministrazioni locali assumono un ruolo centrale. Oltre a recepire le nuove disposizioni normative, sono chiamate a implementare strumenti concreti per l'adeguamento organizzativo, anche attraverso l'azione delle autorità nazionali competenti (Carta, 2024; PSTW, 2024; OECD, 2024).

Questa trasformazione comporta sfide operative e culturali significative: tra queste, la necessità di condurre valutazioni complesse dei rischi associati all'uso di IA, la formazione continua del personale e l'attivazione di modalità efficaci di coinvolgimento civico.

Al tempo stesso, il processo di adeguamento rappresenta un'opportunità di modernizzazione amministrativa. Le nuove regole possono infatti contribuire a rafforzare l'efficacia, la legittimità e la

trasparenza dell'azione pubblica, migliorando la qualità dei servizi e orientando gli acquisti verso soluzioni conformi a criteri etici e di sicurezza (PSTW, 2024; OECD, 2024).

1.5 Obiettivi e approccio del policy paper

Il presente policy paper si propone di offrire un contributo analitico e orientativo sull'utilizzo dell'intelligenza artificiale nella pubblica amministrazione, con particolare riferimento al contesto normativo, istituzionale e operativo europeo e nazionale. In un momento in cui l'IA sta assumendo un ruolo crescente nei processi decisionali pubblici, il documento intende supportare il Consiglio regionale della Lombardia e gli attori pubblici territoriali nella comprensione delle opportunità, dei rischi e delle condizioni necessarie per una sua adozione responsabile.

L'obiettivo è duplice: da un lato, delineare un quadro aggiornato delle principali trasformazioni in corso – tecnologiche, normative, istituzionali – che riguardano l'IA nel settore pubblico; dall'altro, proporre alcune direttrici strategiche per orientare l'azione delle amministrazioni locali, favorendo uno sviluppo coerente con i principi democratici, l'efficacia amministrativa e la tutela dei diritti fondamentali.

L'approccio adottato è interdisciplinare e fondato su tre assi principali:

- una ricognizione normativa e istituzionale delle principali iniziative europee e nazionali, con attenzione particolare all'AI Act (Regolamento UE 2024/1689) e alla Legge Italiana sull'intelligenza artificiale (Legge 23 settembre 2025, n. 132);
- un'analisi critica della letteratura e dei documenti disponibili, finalizzata a evidenziare sfide, ambiguità e condizioni abilitanti per l'impiego dell'IA nella PA;
- l'identificazione di elementi di contesto e casi emblematici, europei e nazionali, che possano supportare le scelte di policy delle amministrazioni regionali e locali.

Il policy paper non propone un modello precostituito né una linea unica di intervento, ma intende offrire una base di conoscenza chiara e strutturata su cui costruire riflessioni, scelte e indirizzi coerenti con la missione pubblica delle istituzioni.

Capitolo 2 Il quadro europeo

2.1 L'Artificial Intelligence Act: Quadro Normativo, Obblighi e Governance

2.1.1 Base Legislativa e Contesto Normativo dell'AI Act

Il Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale (AI Act) rappresenta uno degli interventi normativi più complessi e ambiziosi dell'Unione Europea. La sua base legislativa è duplice, fondata sugli Articoli 16 e 114 del Trattato sul Funzionamento dell'Unione Europea (TFUE) (Silva, 2024; Carta, 2024). L'Articolo 114 TFUE riguarda il ravvicinamento delle disposizioni legislative degli Stati membri che hanno per oggetto l'instaurazione e il funzionamento del mercato interno. Il ricorso a tale base giuridica si giustifica con la qualificazione che il Regolamento opera dell'Intelligenza Artificiale quale "prodotto", legando la disciplina all'uso e alle sue applicazioni (Carta, 2024). L'obiettivo è infatti quello di stabilire regole armonizzate sull'intelligenza artificiale per garantire il funzionamento del mercato interno.

Accanto a ciò, l'inclusione dell'Articolo 16 TFUE (relativo alla protezione dei dati personali) rafforza la tutela dei diritti fondamentali (Carta, 2024). Questa doppia base giuridica sottolinea l'intento del legislatore europeo di non pregiudicare la normativa vigente dell'Unione in materia di protezione dei dati, di tutela dei consumatori, dei diritti fondamentali, di occupazione e protezione dei lavoratori e di sicurezza dei prodotti, configurandosi l'AI Act come una legislazione complementare a tali sistemi normativi esistenti (Carta, 2024). L'AI Act si propone di conciliare la promozione dell'evoluzione tecnologica con il rispetto dei valori fondamentali dell'UE, quali democrazia, diritti fondamentali e Stato di diritto.

2.1.2 Percorso Evolutivo delle Proposte Normative sull'IA

L'adozione del Regolamento ha richiesto un lungo e articolato percorso legislativo. Questo processo prende avvio dalla necessità di raccogliere un'indicazione precisa formulata dalla Commissione nel Libro Bianco sull'Intelligenza Artificiale (COM(2020) 65 final) del febbraio 2020 (Carta, 2024).

Il percorso evolutivo delle proposte normative europee sull'IA fino al 2023 è stato caratterizzato da dibattiti e aggiustamenti significativi (Silva, 2024; Tommasi, 2023). Un esempio emblematico di questa evoluzione durante l'iter di approvazione è rappresentato dalla disciplina dei modelli di IA per finalità generali (GPAI), inclusi i modelli di IA generativa di grandi dimensioni (Carta, 2024; Salvo et al., 2024; Bird & Bird, 2025; Silva, 2024). Questi, inizialmente non oggetto di disciplina, sono stati inclusi nell'accordo di compromesso finale su impulso del Parlamento europeo, a seguito dell'esplosione di fenomeni come Chat GPT. Il loro inserimento nel testo finale ha reso necessaria una ridefinizione di parti del quadro normativo, come gli obblighi di trasparenza e informazione per i fornitori.

Tale percorso ha portato alla definizione di un quadro normativo che, sebbene possa essere ritenuto da alcune voci critiche[1] un compromesso rispetto a posizioni più restrittive, mira a posizionare l'Unione Europea come leader nello sviluppo di un'IA sicura ed etica su scala globale, puntando a un effetto simile a quello ottenuto con il GDPR[2] (il cosiddetto "effetto Bruxelles"3[3]).

2.1.3 L'approccio basato sul rischio

L'approccio dell'Unione Europea alla regolamentazione dell'intelligenza artificiale, concretizzatosi nell'AI Act, si basa su una logica proporzionale e cumulativa nell'imposizione di obblighi, che aumentano di pari passo con l'incremento dei rischi associati ai sistemi di IA.

La classificazione dei sistemi di IA

L'AI Act si fonda su un approccio regolatorio basato sulla distinzione di **quattro livelli di rischio: inaccettabile, alto, limitato e minimo**. Questa classificazione, nota come **"piramide del rischio"**, struttura in modo proporzionato gli obblighi giuridici in relazione alla gravità dei potenziali impatti degli impieghi dell'intelligenza artificiale (Tommasi, 2023; Carta, 2024).

- **Rischio inaccettabile**: comprende i sistemi di IA che presentano minacce gravi e sistemiche ai diritti fondamentali. Tali pratiche sono **vietate** in modo assoluto (Tommasi, 2023). I divieti sono tra le prime disposizioni dell'AI Act a entrare in vigore (sei mesi dopo la promulgazione), in ragione della loro funzione preventiva anche rispetto ad altri ambiti normativi (Carta, 2024). Tra i casi esemplari rientrano:
  - il **predictive policing**[4],
  - il **social scoring**[5],

[1] La posizione critica è stata espressa, tra gli altri, da 44 amministratori delegati di grandi imprese europee – tra cui Airbus, BNP Paribas, Carrefour e Philips – riuniti nell'ambito della *EU AI Champions Initiative*, che rappresenta oltre cento aziende del continente. In una lettera aperta alla Presidente della Commissione Europea, hanno chiesto di posticipare l'attuazione dell'AI Act, definendolo un potenziale freno alla competitività dell'Europa rispetto a Stati Uniti e Cina. Hanno denunciato la complessità regolativa e il rischio di un effetto deterrente per le startup, temendo l'applicazione di obblighi troppo gravosi anche per chi integra modelli di IA generalista nei propri servizi, in modo non paragonabile ai grandi player come Google, Meta o OpenAI. A ciò si è aggiunta una seconda lettera di oltre 30 fondatori e investitori di startup IA europee, che hanno definito l'AI Act "una bomba a orologeria" a causa della sua vaghezza e della frammentazione applicativa prevista a livello nazionale. L'iniziativa, promossa attraverso il portale https://aichampions.eu, ha avuto ampia risonanza, in particolare sul *Financial Times*, nel contesto delle negoziazioni sul codice di condotta per i modelli GPAI.

[2] Il regolamento generale sulla protezione dei dati, ufficialmente regolamento (UE) n. 2016/679.

[3] Quell'effetto per cui le normative europee sono in grado di influenzare regolamenti a livello globale, specialmente per prodotti fisici.

[4] La polizia predittiva si riferisce, in linea generale, all'impiego di tecniche di analisi dei dati volte a elaborare previsioni relative ai luoghi in cui è altamente probabile che siano commessi reati (c.d. crime hot spots) ovvero riguardanti i soggetti più a rischio di divenire autori (potential offenders) o vittime di reati. (Pietrocarlo, 2024)

[5] Il social scoring consiste nell'uso di tecnologie di intelligenza artificiale per valutare e profilare gli individui sulla base di un punteggio ottenuto da una combinazione di dati relativi al comportamento sociale (ad esempio, azioni, comportamenti, abitudini, forme di interazione sociale, come la partecipazione a eventi culturali, il comportamento sul posto di lavoro, l'uso di determinati servizi pubblici) e a dati relativi alle caratteristiche personali o ai tratti della personalità degli individui (ad esempio, situazione finanziaria, salute, rendimento lavorativo, interessi, genere, orientamento sessuale). *Cfr. il Considerando 31 dell'IA ACT*

- l'impiego di **tecniche manipolative o subliminali** che distorcono il comportamento individuale in modo non trasparente.

- I sistemi ad alto rischio sono quelli per i quali sono previsti rigorosi obblighi prima della loro immissione nel mercato e un monitoraggio successivo. I criteri per la classificazione ad alto rischio sono definiti ope legis, ossia direttamente dalla legge, non lasciando l'individuazione delle categorie di rischio e dei meccanismi di mitigazione alla discrezionalità dei destinatari della disciplina (Carta, 2024; Tommasi, 2023). Questo approccio "top-down" rappresenta una sostanziale differenza rispetto al GDPR, norma presa a riferimento per l'approccio secondo livelli di rischio, dove la valutazione del rischio è lasciata alla discrezionalità di titolari e responsabili del trattamento (Tommasi, 2023).

Un sistema di IA è considerato ad **alto rischio** in due casi principali (Tommasi, 2023):

1. Se è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione UE elencata nell'allegato II, e tale prodotto è soggetto a una valutazione di conformità da parte di terzi relativa a rischi per la salute e la sicurezza ai fini dell'immissione sul mercato (Tommasi, 2023).
2. Se rientra nei settori elencati nell'allegato III dell'AI Act, a condizione che presenti un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche (Tommasi, 2023). L'allegato III identifica settori come: sistemi biometrici, gestione infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali (pubblici e privati), attività di contrasto, gestione migrazione/asilo/frontiere, amministrazione della giustizia e processi democratici (Tommasi, 2023).

I sistemi a **rischio limitato** sono soggetti a specifici obblighi di trasparenza: i fornitori e gli utilizzatori devono informare chiaramente gli utenti quando interagiscono con un sistema di IA, in particolare nel caso di chatbot o di contenuti generati che possono risultare ingannevoli, come immagini, audio o video manipolati. È inoltre previsto l'obbligo di preparare e conservare adeguata documentazione tecnica, al fine di garantire la consapevolezza dell'utente e promuovere un uso responsabile dell'IA, senza gli oneri più stringenti applicabili ai sistemi ad alto rischio (Bird & Bird, 2025; Silva, 2024; Novelli et al., 2024).

I sistemi a **rischio minimo** non presentano generalmente criticità rilevanti per diritti o sicurezza e sono soggetti unicamente a obblighi di trasparenza, con l'obiettivo di garantire la consapevolezza dell'utente in merito all'interazione con sistemi automatizzati (Tommasi, 2023).

L'articolo 7 dell'AI Act prevede inoltre la possibilità per la Commissione di aggiungere o modificare settori o casi d'uso nell'allegato III[6], se questi presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, sull'ambiente o sulla democrazia e sullo Stato di diritto (Tommasi, 2023).

Nonostante il Regolamento UE sull'Intelligenza Artificiale adotti un approccio innovativo basato sul rischio per regolamentare l'impiego delle tecnologie di AI, alcune analisi critiche evidenziano come tale

[6] L'Allegato III del Regolamento (UE) 2024/1689 identifica le aree e i casi d'uso in cui i sistemi di IA sono automaticamente classificati come ad alto rischio, elencando settori come infrastrutture critiche, istruzione, servizi essenziali, gestione delle risorse umane e altri ambiti sensibili. L'articolo 7 dell'AI Act attribuisce alla Commissione europea la facoltà di aggiornare l'Allegato III aggiungendo o modificando settori o casi d'uso, se emergono nuovi rischi significativi per la salute, la sicurezza, i diritti fondamentali, l'ambiente, la democrazia o lo Stato di diritto (Tommasi, 2023).

impostazione possa risultare insufficiente sotto il profilo della tutela dei diritti fondamentali. Il paper "Risks Without Rights? The EU AI Act's Approach to AI in Law and Rulemaking" (Rangone & Megale, 2025) mette in luce come l'enfasi sul rischio e la categorizzazione dei sistemi AI rischino di non garantire adeguate tutele procedurali per gli individui, in particolare quando le tecnologie incidono su diritti fondamentali come la privacy, la non discriminazione e il diritto a un giusto processo.
In particolare, lo studio sottolinea la necessità di integrare al modello basato sul rischio meccanismi più robusti di responsabilità e trasparenza, che assicurino agli utenti finali strumenti concreti per esercitare i propri diritti. Ciò include garanzie per l'accesso a spiegazioni comprensibili delle decisioni automatizzate, nonché canali efficaci per la contestazione e la revisione umana. Questa prospettiva suggerisce dunque un arricchimento normativo che coniughi l'approccio tecnico-legale con un più esplicito focus sui diritti e sulle libertà fondamentali, rafforzando la dimensione procedurale del Regolamento.
Un ulteriore approfondimento (Presno Linera & Meuwese, 2025) nato dall'analisi congiunta del Regolamento AI Act e del Framework Convention on AI[7]. Questo studio evidenzia come il quadro normativo europeo tenti di bilanciare la necessità di un'efficace gestione del rischio con un approccio più ampio, che prevede la cooperazione internazionale e la definizione di standard condivisi a livello globale.
L'approfondimento mette in rilievo che, sebbene il Regolamento disciplini con precisione vari profili tecnici e procedurali, un'effettiva tutela dei diritti fondamentali richiede un'integrazione tra misure di governance interna e un sistema coordinato di regole a livello internazionale. Ciò risulta particolarmente rilevante per garantire coerenza e compatibilità tra normative nazionali e comunitarie, minimizzando così il rischio di frammentazione e favorendo un ambiente regolatorio stabile e prevedibile per gli operatori e gli utenti.

2.1.4 I ruoli

Nel contesto dell'AI Act, le responsabilità degli attori coinvolti sono definite in relazione al posizionamento funzionale rispetto al ciclo di vita di un sistema di IA. I due ruoli principali sono quelli di fornitore (provider) e utilizzatore (deployer).

- **Fornitore o Provider**: è il soggetto che immette sul mercato o mette in servizio un sistema di IA. Tale ruolo può essere assunto non solo da sviluppatori, ma anche da soggetti che integrano un sistema in un prodotto e lo commercializzano con il proprio nome o marchio. Inoltre, la definizione include coloro che immettono sul mercato modelli di IA a finalità generali (GPAI). La responsabilità del fornitore si concentra sulla conformità del sistema ai requisiti tecnici e normativi prima del suo utilizzo o diffusione, comprese le procedure di valutazione e

[7] La Convenzione Quadro sull'Intelligenza Artificiale, i Diritti Umani, la Democrazia e lo Stato di Diritto, promossa dal Consiglio d'Europa e aperta alla firma il 5 settembre 2024, rappresenta il primo trattato internazionale giuridicamente vincolante in materia di IA. Il suo obiettivo è stabilire un quadro normativo globale per garantire che l'intero ciclo di vita dei sistemi di IA, sia nel settore pubblico che in quello privato, sia compatibile con i principi di tutela dei diritti fondamentali, del funzionamento democratico e dello stato di diritto. La Convenzione, aperta all'adesione anche di Stati non membri del Consiglio d'Europa, è stata concepita per essere complementare all'AI Act dell'Unione Europea, fungendo da standard giuridico di riferimento a livello internazionale.

marcatura richieste per i sistemi ad alto rischio (Tommasi, 2023). I fornitori di questi modelli sono tenuti a mettere a disposizione degli sviluppatori a valle una documentazione tecnica completa e aggiornata, contenente le informazioni minime indicate nell'Allegato XII del Regolamento. Queste informazioni sono essenziali per consentire agli utilizzatori successivi di adempiere correttamente ai propri obblighi normativi (Bird & Bird, 2025).

- **Utilizzatore o Deployer**: è il soggetto che utilizza un sistema di IA sotto la propria autorità, sia nel settore pubblico che privato. Il deployer può essere una persona fisica, una persona giuridica, un'autorità pubblica, un'agenzia o altro organismo (Carta, 2024). La sua responsabilità riguarda l'uso conforme del sistema dopo la sua messa in servizio, inclusa l'adozione di misure adeguate a garantirne la trasparenza, la supervisione umana, la valutazione d'impatto e la gestione del rischio nello specifico contesto applicativo (Riccio, 2024; Carta, 2024).

La specificazione di ruoli distinti è essenziale per l'attribuzione delle responsabilità e per la definizione degli obblighi specifici, in particolare per i sistemi ad alto rischio, il cui utilizzo o messa in commercio comporta un regime di compliance articolato e rigoroso.
Nel quadro regolatorio introdotto dal Regolamento, i fornitori di sistemi di intelligenza artificiale assumono un ruolo centrale nella realizzazione degli obiettivi di sicurezza, affidabilità e rispetto dei diritti fondamentali perseguiti dal legislatore europeo.
I sistemi di IA ad alto rischio rappresentano il nucleo più regolato: i fornitori sono tenuti a rispettare una serie di requisiti prima della loro immissione sul mercato o della loro messa in servizio, tra cui la valutazione di conformità e la marcatura CE (Carta, 2024).

2.1.5 Obblighi specifici per i soggetti pubblici

La qualificazione come fornitore non è limitata ai soggetti privati. Secondo la definizione normativa, rientra tra i fornitori anche qualsiasi soggetto che immetta sul mercato o metta in servizio un sistema di IA a proprio nome o marchio. Di conseguenza, una Pubblica Amministrazione può assumere questo ruolo qualora sviluppi internamente o commissioni un sistema da integrare nei propri servizi pubblici, ponendolo sotto la propria responsabilità giuridica (Carta, 2024). In tali casi, gli obblighi previsti per i fornitori si applicherebbero pienamente anche alle amministrazioni pubbliche.
L'implementazione di sistemi di intelligenza artificiale, inclusa l'IA generativa (IAG), nella Pubblica Amministrazione richiede un attento bilanciamento tra innovazione tecnologica, conformità normativa e tutela dei diritti fondamentali (Riccio, 2024). Nell'ambito dei ruoli previsti dall'AI Act, le Pubbliche Amministrazioni rientrano principalmente nella definizione di utilizzatore (deployer), ovvero il soggetto che utilizza un sistema di IA sotto la propria autorità (Guidi, 2025).
Tra gli obblighi fondamentali per i deployer di sistemi di IA ad alto rischio vi è la conduzione di una Valutazione di impatto per i diritti fondamentali (FRIA), da realizzare prima dell'uso del sistema, al fine di individuare potenziali pregiudizi per i diritti fondamentali riconosciuti nell'Unione europea (Carta, 2024; Riccio, 2024). L'introduzione della FRIA è stata sostenuta per consolidare l'obiettivo di un'IA antropocentrica, che ponga la persona al centro dei processi decisionali automatizzati.
Il Regolamento sottolinea inoltre la centralità della supervisione umana lungo l'intero ciclo di utilizzo dei sistemi di IA ad alto rischio, rimarcando la necessità di un coinvolgimento umano attivo e consapevole rispetto agli output prodotti dall'IA (Tommasi, 2023).

Sul piano della trasparenza, gli utilizzatori, incluse le Pubbliche Amministrazioni, possono essere soggetti a obblighi specifici: ad esempio, quando ricorrono a sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, devono informare le persone fisiche esposte a tali sistemi (Tommasi, 2023). Il Regolamento sancisce inoltre il diritto alla spiegazione rispetto al trattamento dei dati su cui si basa la sorveglianza, stabilendo che qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio ha diritto a una spiegazione adeguata (Van Noordt et al., 2025; Carta, 2024).

Le PA, come qualsiasi altro soggetto, sono soggette ai divieti imposti dal Regolamento per i sistemi a rischio inaccettabile (Salvo et al., 2024; Tommasi, 2023). L'uso del riconoscimento biometrico da remoto in tempo reale negli spazi pubblici è generalmente vietato, sebbene siano previste eccezioni per motivi di contrasto alla criminalità, previa autorizzazione dell'autorità giudiziaria (Salvo et al., 2024).

È stato rilevato che, pur vietando in linea di principio l'uso del riconoscimento facciale in tempo reale negli spazi pubblici, l'AI Act prevede eccezioni rigorosamente circoscritte, che possono costituire spiragli significativi all'applicazione effettiva del divieto (Silva, 2024; Bird & Bird, 2025). Tali eccezioni riguardano, ad esempio, la ricerca mirata di vittime di rapimenti o tratta di esseri umani, la prevenzione di minacce alla vita o l'individuazione di persone scomparse, sempre previa autorizzazione di un'autorità giudiziaria o amministrativa indipendente, registrazione del sistema e valutazione dell'impatto sui diritti fondamentali (Bird & Bird, 2025; Silva, 2024).

Il Regolamento proibisce inoltre la creazione o l'espansione di database di riconoscimento facciale attraverso lo scraping indiscriminato di immagini da internet o da riprese CCTV, pratica che è stata al centro di casi controversi come quello di ClearviewAI, poiché contribuisce a forme di sorveglianza di massa lesive dei diritti fondamentali (Carta, 2024; Bird & Bird, 2025). Tra i sistemi ad alto rischio individuati nell'Allegato III dell'AI Act rientrano specificamente i sistemi biometrici[8] e quelli basati su elementi biometrici (Carta, 2024).

Nei casi consentiti, il deployer pubblico, oltre ad essere tenuto a condurre la FRIA, integrandola preferibilmente con la Data Protection Impact Assessment (DPIA) prevista dal GDPR, è obbligato a registrare l'uso del sistema in un database dell'UE (Riccio, 2024; Van Pinxteren, 2024). Tali garanzie rafforzano l'esigenza di trasparenza e di supervisione indipendente sull'impiego del riconoscimento biometrico in tempo reale.

A livello statale, un obbligo cruciale derivante dal Regolamento (UE) 2024/1689 sull'intelligenza artificiale è l'istituzione o la designazione di una o più Autorità nazionali competenti responsabili dell'attuazione e del controllo dell'applicazione del Regolamento stesso (Salvo et al., 2024; Cappai, 2024; Cassano, 2024). In Italia, la scelta dell'organismo competente, individuati ai AgID e ACN, ha suscitato un ampio dibattito che ha coinvolto anche il Garante per la protezione dei dati personali, il

[8] Già nel 2021 il Garante per la protezione dei dati personali ha espresso un parere negativo sull'utilizzo del sistema SARI Real Time, sviluppato dal Ministero dell'Interno, evidenziando l'assenza di una base giuridica adeguata e i rischi eccessivi per i diritti e le libertà fondamentali. Il sistema, che analizza in tempo reale i volti ripresi da telecamere pubbliche confrontandoli con una *watch-list* fino a 10.000 soggetti, è stato ritenuto potenzialmente lesivo della libertà di riunione e di manifestazione del pensiero, oltre che idoneo a generare forme di sorveglianza indiscriminata. Si veda il Parere n. 127 del 25 marzo 2021 e il relativo Comunicato del 16 aprile 2021 del Garante per la protezione dei dati personali.

quale ha rivendicato un ruolo centrale, sottolineando la necessità che l'autorità designata sia indipendente, autonoma e dotata di poteri effettivi (Salvo et al., 2024; Guidi, 2025).
Nel quadro dell'AI Act, acquisisce particolare rilievo anche la figura dell'"autorità di contrasto" (law enforcement authority), definita all'art. 3, punto 45 del Regolamento come "qualsiasi autorità pubblica – o altro organismo o entità designata dal diritto nazionale – incaricata di esercitare funzioni relative alla prevenzione, indagine, accertamento o perseguimento di reati, o all'esecuzione di sanzioni penali, incluse le attività di salvaguardia contro le minacce alla sicurezza pubblica" (Guidi, 2025).
Secondo quanto evidenziato dalla dottrina, alcune autorità nazionali garanti della concorrenza potrebbero rientrare in questa definizione qualora dotate del potere di irrogare sanzioni assimilabili a quelle penali per violazioni in materia antitrust. In tal caso, sarebbero soggette agli obblighi specifici previsti dal Capo III del Regolamento, che disciplina in modo più stringente l'uso dei sistemi di IA da parte di tali autorità (Guidi, 2025). Ciò comporterebbe, ad esempio, limitazioni nell'impiego di strumenti algoritmici per finalità di indagine o vigilanza, al fine di tutelare i diritti fondamentali coinvolti.
È inoltre previsto che tutti i sistemi di IA destinati a essere utilizzati da autorità di contrasto, o per loro conto, siano classificati come sistemi ad alto rischio. Questo vale in particolare per le applicazioni impiegate nella valutazione di prove in procedimenti penali o amministrativi. Tale classificazione deriva dalla considerazione dello squilibrio di potere tra l'autorità e l'individuo e dei potenziali impatti negativi sulla libertà personale e altri diritti fondamentali, come nei casi di sorveglianza, arresto o detenzione (Guidi, 2025; Salvo et al., 2024). Di conseguenza, questi sistemi devono essere progettati e addestrati in conformità a requisiti rigorosi in materia di qualità dei dati, accuratezza, robustezza e tracciabilità.
In estrema sintesi, le Pubbliche Amministrazioni, principalmente nel loro ruolo di utilizzatori, sono chiamate a rispettare obblighi significativi, in particolare per l'uso di sistemi di IA ad alto rischio, che includono la valutazione di impatto sui diritti fondamentali, la garanzia di supervisione umana e la trasparenza. A livello nazionale, lo Stato deve garantire l'istituzione di un'autorità competente indipendente e promuovere lo sviluppo di capacità interne e quadri etici per l'uso dell'IA nel settore pubblico, nel rispetto dei divieti imposti dal Regolamento.

2.1.6 I meccanismi di governance previsti dall'AI Act

L'attuazione del Regolamento (UE) 2024/1689 sull'intelligenza artificiale si basa su un sistema di governance multilivello, che coinvolge autorità a livello sia nazionale che europeo, con l'obiettivo di garantire un'applicazione uniforme, coordinata ed efficace in tutti gli Stati membri (Novelli et al., 2024; (Cabrera, L. L., & McGowan, I., 2024).

2.2 Governance nazionale

Ogni Stato membro deve istituire almeno due autorità:

- **Un'autorità notificante**, incaricata di designare e monitorare gli organismi di valutazione della conformità ("notified bodies") che eseguono le verifiche sui sistemi di IA ad alto rischio. Questi organismi devono agire con imparzialità e non possono svolgere direttamente attività di valutazione. Le autorità notificanti possono sospendere o revocare la designazione se gli obblighi non sono rispettati (Novelli et al., 2024; (Cabrera, L. L., & McGowan, I., 2024).

- **Un'autorità di sorveglianza del mercato (MSA)**, che funge da punto di contatto nazionale per tutte le attività di vigilanza. Le MSAs sono competenti su tutte le categorie di IA, incluso l'alto rischio, e hanno poteri rafforzati nei settori sensibili, come l'applicazione della legge. Possono autorizzare test in ambienti reali, ricevere notifiche obbligatorie (es. per il riconoscimento biometrico in tempo reale), richiedere misure correttive o il ritiro di sistemi non conformi, e accedere a dati e codice sorgente (Novelli et al., 2024; Cabrera, L. L., & McGowan, I., 2024).

Le autorità nazionali[9] devono disporre di personale qualificato e risorse adeguate, con competenze in IA, protezione dei dati, cybersicurezza, diritti fondamentali, salute, sicurezza e normative pertinenti (Novelli et al., 2024). Ogni Stato può decidere se creare nuove autorità dedicate o attribuire questi compiti a enti esistenti, come le autorità per la protezione dei dati (Novelli et al., 2024).

2.2.1 Governance europea

A livello UE, il Regolamento affida la supervisione generale a una **rete di istituzioni europee**, nuove ed esistenti:

- **La Commissione Europea** ha il compito principale di attuazione: adotta atti delegati ed esecutivi, stabilisce linee guida e standard tecnici, definisce criteri per la classificazione GPAI e per i sistemi ad alto rischio e coordina l'interazione con gli altri quadri normativi UE. Quest'ultimo è un aspetto fondamentale dell'attuazione dell'AI ACT. L'AI Act non è un intervento isolato, ma si accompagna ad altre normative del mercato unico digitale, come il Digital Services Act (DSA) e il Digital Markets Act (DMA), con i quali è necessario un coordinamento. Tale coordinamento è cruciale per affrontare efficacemente le sfide poste dalle nuove tecnologie e garantire un approccio normativo coerente. Strumenti come il gruppo ad alto livello per il regolamento sui mercati digitali (High-Level Group for the Digital Markets Act), composto da diverse autorità e organismi europei, facilitano lo scambio di consulenza e competenze per promuovere tale coerenza tra DSA e AI Act. La sinergia tra DSA, DMA e AI Act contribuisce non solo a prevenire le violazioni (ad esempio dell'articolo 101 TFUE in materia di concorrenza) attraverso obblighi by design e valutazione del rischio, ma anche a rendere più agevole la loro individuazione, grazie agli ampi poteri di indagine attribuiti a Commissione e autorità nazionali e ai molteplici canali di scambio di informazioni creati. In particolare, l'AI Act impone alle autorità di vigilanza del mercato di comunicare annualmente alla Commissione e alle autorità antitrust degli Stati membri qualsiasi informazione potenzialmente rilevante per l'applicazione del diritto della concorrenza, ampliando significativamente i poteri di indagine di queste ultime.
- **L'AI Office**: l'AI Office è stato creato separatamente tramite una decisione della Commissione nel gennaio 2024 per implementare l'AI Act. La sua missione principale è stabilire regole armonizzate per implementare e applicare l'AIA in modo coerente in tutta l'UE (Novelli et al.,

[9] In base all'art. 20 del disegno di legge "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", l'Italia ha designato come autorità nazionali per l'intelligenza artificiale l'Agenzia per l'Italia Digitale (AgID), con il ruolo di autorità notificante ai sensi dell'art. 70 del Regolamento (UE) 2024/1689, e l'Agenzia per la Cybersicurezza Nazionale (ACN), con il ruolo di autorità di sorveglianza del mercato e punto di contatto unico con le istituzioni europee.

2024). Il suo ruolo sotto l'atto è stabilire standard per valutare le capacità e monitorare l'applicazione delle regole ai modelli e sistemi GPAI. È autorizzato a creare Codici di Condotta e monitorare possibili violazioni dell'AIA da parte di questi modelli e sistemi. L'AI Office è integrato all'interno della struttura amministrativa della DG Connect (DG-CNECT) della Commissione. Un aspetto importante del ruolo dell'AI Office è la supervisione delle tecnologie General-Purpose AI. L'AI Office svolge un ruolo fondamentale nell'applicazione e nell'applicazione delle normative relative alla GPAI, concentrandosi sugli sforzi di standardizzazione per armonizzare strumenti, metodologie e criteri per valutare i rischi sistemici associati alla GPAI. Monitora continuamente la GPAI per l'aderenza agli standard e i potenziali nuovi rischi, supporta le indagini sulle violazioni della GPAI e assiste nello sviluppo di atti delegati e sandbox normativi. L'AI Office fornisce supporto e consulenza alla Commissione e assiste nell'adozione di atti di implementazione e delegati. Non emette decisioni vincolanti proprie, ma supporta le decisioni della Commissione.

- **L'European AI Board**, istituito dall'articolo 65 dell'AI Act, è un organo centrale della governance europea. Composto da un rappresentante per ciascuno Stato membro, nominato per un mandato triennale rinnovabile, ha il compito di facilitare l'applicazione coerente ed efficace del Regolamento in tutta l'Unione. I membri devono disporre dell'autorità e delle competenze necessarie e fungono da punto di contatto unico per il Board e gli stakeholder nazionali. Come previsto dall'articolo 66, il Board fornisce consulenza e assistenza alla Commissione e agli Stati membri, promuovendo il coordinamento tra le autorità nazionali competenti, lo scambio di competenze tecniche e normative e la condivisione di buone pratiche. Svolge inoltre un ruolo consultivo sull'applicazione del Regolamento, inclusi i modelli GPAI. Il Board può emettere linee guida e raccomandazioni e supporta l'elaborazione di atti delegati e di implementazione. È articolato in due sottogruppi permanenti, dedicati rispettivamente alla vigilanza del mercato e alle autorità notificanti e può istituire gruppi di lavoro temporanei. La presidenza è affidata a un rappresentante degli Stati membri e l'attività è sostenuta dalla segreteria tecnica dell'AI Office, che partecipa alle riunioni in qualità di osservatore, insieme al Garante europeo della protezione dei dati (EDPS).
- **L'Advisory Forum**, nominato dalla Commissione, per coinvolgere gli stakeholders nell'attuazione del Regolamento (Outeda, 2024; Bird & Bird, 2025; Novelli et al., 2024). Funziona come organismo consultivo che offre spunti provenienti dall'industria e da altri settori, supportando sia la Commissione Europea che l'European AI Board. I suoi membri, nominati dalla Commissione Europea, rappresentano una selezione equilibrata di stakeholder: industria, start-up, PMI, società civile e mondo accademico. L'adesione è pensata per bilanciare interessi commerciali e non commerciali, con un'attenzione particolare alle PMI (Outeda, 2024). Il Forum riflette prospettive diverse della società civile e dei settori industriali e può essere visto anche come una forma istituzionalizzata di lobbying (Novelli et al., 2024). I compiti principali dell'Advisory Forum comprendono la consulenza tecnica al Board e alla Commissione, la preparazione di pareri e raccomandazioni su richiesta, nonché l'obbligo per la Commissione di consultarlo in caso di proposte di standardizzazione o nella redazione di specifiche comuni, come previsto dall'articolo 41 del Regolamento. Il Forum ha inoltre la facoltà di istituire sottogruppi permanenti o temporanei per approfondire questioni

specifiche, si riunisce almeno due volte all'anno, e può invitare esperti esterni e altri stakeholder a partecipare ai lavori.

- **Lo Scientific Panel** è un organo previsto dal quadro di governance dell'EU AI Act, la cui istituzione è obbligatoria ai sensi dell'articolo 68 del Regolamento (Bird & Bird, 2025; Novelli et al., 2024; Outeda, 2024; Silva, 2024). È creato tramite un atto di esecuzione della Commissione. È composto da esperti indipendenti selezionati dalla Commissione in consultazione con l'AI Board, sulla base della loro competenza scientifica o tecnica nel campo dell'IA, garantendo una rappresentanza equa di genere e geografica e il rispetto di criteri di imparzialità, obiettività e riservatezza. Il Panel ha il compito di supportare l'applicazione e l'attuazione dell'AI Act, in particolare per i modelli di IA per finalità generali, agendo anche come risorsa per gli Stati membri. Gli Stati membri potranno essere tenuti a pagare tariffe per il supporto ricevuto, secondo quanto sarà definito in un atto di esecuzione (Bird & Bird, 2025; Novelli et al., 2024).

2.3 Altre normative europee rilevanti e il rapporto con l'AI Act (AIA)

2.3.1 Regolamento Generale sulla Protezione dei Dati (GDPR)

L'AI Act stabilisce che i suoi obblighi si applicano in aggiunta a e senza pregiudizio per gli obblighi derivanti dal GDPR e dalla direttiva e-Privacy (Bird & Bird, 2025). L'interpretazione del concetto di "stabilimento" nell'ambito dell'AI Act è prevista essere ampia, simile all'uso di questo termine ai sensi di altra legislazione UE, come il GDPR (Bird & Bird, 2025). Con "stabilimento" si intende qualsiasi presenza stabile e continuativa nell'UE, come una filiale o un ufficio; ciò significa che qualsiasi organizzazione dotata di uno stabilimento sarà soggetta all'AI Act per le attività di sviluppo, offerta o utilizzo di sistemi di IA svolte nel contesto di tale presenza, anche se la sede principale si trova al di fuori dell'Unione.

Nel caso in cui i distributori o utilizzatori di sistemi di IA ad alto rischio siano tenuti a eseguire una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'articolo 35 del GDPR, essi devono basarsi sulle informazioni tecniche e sulla documentazione fornite dal fornitore del sistema ai sensi dell'articolo 13 dell'AI Act, che comprendono dettagli sulla progettazione, i dati di addestramento, i test e le valutazioni di rischio. Questa condivisione di informazioni è essenziale per garantire che la DPIA sia completa e accurata, permettendo al distributore o utilizzatore di adempiere agli obblighi di trasparenza e di tutela dei diritti previsti dal GDPR. Tuttavia, la diversa natura delle due discipline implica che le misure di trasparenza dell'AI Act, più orientate alla documentazione tecnica, potrebbero non essere sufficienti a soddisfare i diritti informativi degli interessati stabiliti dal GDPR (Bird & Bird, 2025; Falletta & Marsano, 2024).

Il GDPR impone l'obbligo di informare gli individui sul trattamento dei loro dati ai sensi degli articoli 13 e 14. In relazione al trattamento automatizzato, i titolari del trattamento devono spiegare la logica sottostante al processo decisionale, obbligo che si allinea con il diritto alla spiegazione previsto dall'articolo 86 dell'AI Act (Bird & Bird, 2025). Le disposizioni dell'AI Act supportano e supplementano i requisiti del GDPR, che rimane applicabile in tutte le fasi del ciclo di vita dell'IA in cui vengono trattati dati personali.

L'AI Act è stato elaborato con l'obiettivo di introdurre un quadro normativo specifico per i sistemi di IA più rischiosi, destinato a diventare un punto di riferimento globale, analogamente a quanto accaduto

con il GDPR. Il contesto italiano è stato uno dei primi a confrontarsi con la verifica della conformità dei modelli linguistici di grandi dimensioni con le norme su data justice, privacy e trasparenza. In particolare, nel marzo 2023 il Garante della Privacy italiano ha imposto a OpenAI di interrompere il trattamento dei dati personali degli utenti italiani fino alla verifica della conformità al GDPR (Garante per la protezione dei dati personali, 2023). Questo episodio ha messo in evidenza come, in assenza di una cornice armonizzata per l'intelligenza artificiale, le autorità nazionali per la protezione dei dati abbiano svolto un ruolo cruciale nel garantire i diritti fondamentali, sollevando interrogativi sull'assetto istituzionale previsto dall'AI Act (Falletta & Marsano, 2024).

L'AI Act, pur condividendo l'obiettivo di tutela dei diritti fondamentali, rappresenta un'espressione diversa dell'approccio basato sul rischio rispetto al GDPR, il quale adotta una prospettiva bottom-up fondata sull'accountability (Tommasi, 2023). Il Regolamento (UE) 2024/1689 si applica senza pregiudizio per il GDPR (Silva, 2024), i cui principi rimangono pienamente applicabili ogni volta che i sistemi di IA trattano dati personali. Inoltre, le disposizioni dell'AI Act in materia di governance dei dati, cybersecurity e documentazione tecnica (incluso l'Allegato XI) richiamano le preoccupazioni relative al trattamento dei dati personali.

Nonostante le molteplici intersezioni tra le due normative, va osservato che l'AI Act non assegna un ruolo centrale alle autorità garanti della protezione dei dati, a differenza del GDPR che ha previsto una rete europea coordinata dal Comitato europeo per la protezione dei dati. Questa scelta potrebbe condurre a una **frammentazione istituzionale** nell'applicazione dei diritti fondamentali, soprattutto nei casi in cui la valutazione d'impatto sull'IA e quella sulla protezione dei dati si sovrappongono senza chiare procedure di raccordo (Falletta & Marsano, 2024).

Analogamente al GDPR, l'AI Act prevede la possibilità per gli Stati membri di esentare gli organismi pubblici dalle multe (articolo 99/8) (Silva, 2024). Le autorità nazionali competenti per i diritti fondamentali, inclusi i garanti privacy, hanno poteri di vigilanza sui sistemi ad alto rischio (articolo 77) (Silva, 2024). L'AI Act, infine, complementa altri regolamenti europei come il GDPR e si colloca all'interno del programma strategico "Digital Decade 2030" (PSTW, 2024; 2025).

2.3.2 Digital Services Act (DSA) e Digital Markets Act (DMA)

Tra la serie degli ulteriori atti normativi cui l'AI Act si accompagna un ruolo particolare hanno il Digital Services Act (DSA) e il Digital Markets Act (DMA). Questi regolamenti condividono l'obiettivo di rafforzare la sovranità digitale dell'UE e disciplinano aspetti complementari del mercato digitale europeo. L'AI Act si caratterizza per un ambito di applicazione territoriale particolarmente ampio, ancor più esteso rispetto a quello del GDPR, del DMA e del DSA (Carta, 2024).

Il DSA classifica i fornitori di servizi digitali in base a criteri oggettivi e livelli di rischio, assegnando obblighi proporzionati (Carta, 2024). L'AI Act, da parte sua, non prevale ma complementa la normativa esistente, offrendo un quadro orizzontale e flessibile che si integra con il corpus normativo settoriale e con la tutela dei diritti fondamentali.

Le tre normative (DSA, DMA, AI Act) sono considerate strumenti sinergici per affrontare le sfide poste dagli algoritmi e dalle piattaforme digitali. Ad esempio, il DMA vieta ai gatekeeper di utilizzare dati non pubblici forniti dagli utenti commerciali delle piattaforme, limitando l'addestramento di algoritmi di pricing. Il DSA, invece, introduce obblighi specifici per le piattaforme online e i motori di ricerca di grandi dimensioni (VLOPs e VLOSEs), tra cui la valutazione dei rischi sistemici associati ai sistemi algoritmici (Guidi, 2025).

Entrambi i regolamenti prevedono poteri di indagine per la Commissione europea e le autorità nazionali, inclusi l'accesso agli algoritmi e la possibilità di svolgere ispezioni. Le autorità nazionali antitrust possono indagare sulle violazioni del DMA, collaborando con la Commissione attraverso la rete europea della concorrenza (ECN). L'AI Act impone alle autorità di vigilanza del mercato di comunicare annualmente alle autorità antitrust le informazioni rilevanti per l'applicazione del diritto della concorrenza (Guidi, 2025).
I tre regolamenti contribuiscono, ciascuno nel proprio ambito, a una regolamentazione sinergica dell'ecosistema digitale europeo (Guidi, 2025; JRC, 2024; Tommasi, 2023). I fornitori di servizi digitali che impiegano sistemi di IA rientrano potenzialmente sia nel perimetro dell'AI Act che del DSA e sono tenuti al rispetto di entrambi (Tommasi, 2023).

2.3.3 Data Governance Act (DGA) e Data Act

L'AI Act dialoga con la parte dell'ecosistema normativo europeo che comprende il Data Governance Act (DGA) e il Data Act (Carta, 2024). Questi atti contribuiscono a rafforzare la sovranità digitale europea, delineando un quadro per la gestione, condivisione e accesso ai dati. Il DGA e il Data Act mirano a costruire un mercato unico dei dati aperto, sicuro e armonizzato, favorendo la disponibilità, la qualità e l'accessibilità dei dati essenziali per lo sviluppo di sistemi di IA affidabili, trasparenti e non discriminatori (MEF, 2024; PSTW, 2024; Outeda, 2024; Mancioppi, 2024).
Il Data Governance Act (DGA) integra il quadro esistente promuovendo la fiducia nella condivisione dei dati e rafforzando i meccanismi per accrescere la disponibilità dei dati e superare gli ostacoli tecnici al loro riutilizzo (Mancioppi, 2024). Il Data Act, invece, armonizza l'accesso ai dati personali e non personali derivanti dall'uso di prodotti e servizi connessi, completando il DGA con linee guida comuni per garantire sicurezza, interoperabilità e una gestione efficace degli scambi B2B, B2C e pubblico-privati (Mancioppi, 2024). Questi strumenti normativi si pongono come pilastri della strategia europea per valorizzare i dati, considerati risorsa fondamentale per l'addestramento e il funzionamento dei sistemi di IA (Outeda, 2024).
La European Data Strategy e il White Paper sull'IA (2020) ribadiscono come i dati siano la materia prima dell'intelligenza artificiale, evidenziando l'importanza di un quadro normativo che garantisca sia la libera circolazione che la tutela dei diritti (Outeda, 2024). Tuttavia, la frammentarietà del quadro vigente e la mancanza di un'integrazione organica tra AI Act, DGA e Data Act possono generare incertezza giuridica, ostacolando l'efficienza e la fiducia nell'utilizzo dei dati e dei sistemi di IA, con potenziali ripercussioni sulla protezione dei diritti fondamentali (Mancioppi, 2024).
Per superare queste criticità, è essenziale un approccio armonizzato, antropocentrico e centrato sui diritti, che combini le esigenze di innovazione e competitività con la salvaguardia dei valori fondamentali dell'UE, tra cui la non discriminazione, la trasparenza e la certezza del diritto (Mancioppi, 2024). Il rapporto con il GDPR resta cruciale: mentre quest'ultimo disciplina il trattamento dei dati personali, l'AI Act introduce obblighi di qualità, accuratezza e completezza dei dati per i sistemi ad alto rischio (Art. 10), prescrivendo persino, all'articolo 10(5), una nuova base giuridica per il trattamento legittimo di categorie speciali di dati al fine di rilevare e correggere bias (Mancioppi, 2024). Questo si inserisce in un contesto in cui la trasparenza, seppur perseguita da entrambe le normative, si declina in modo diverso: più individuale nel GDPR, più tecnica e contestuale nell'AI Act (Falletta & Marsano, 2024).

2.3.4 Il Codice di Condotta per i modelli GPAI

Il 10 luglio 2025 la Commissione Europea ha pubblicato il General-Purpose AI Code of Practice, un documento volontario sviluppato con il contributo di oltre 1.000 stakeholder, volto ad anticipare e facilitare l'attuazione degli obblighi dell'AI Act per i fornitori di modelli di intelligenza artificiale a uso generale. Il Codice si articola in tre sezioni principali: trasparenza, sicurezza e rischio sistemico, copyright. Una volta approvato dagli Stati membri e dalla Commissione, l'adesione al Codice potrà garantire ai firmatari una riduzione dell'onere amministrativo e una maggiore certezza giuridica nel dimostrare la conformità normativa.

Il Capitolo sulla trasparenza si applica a tutti i fornitori di modelli GPAI (esclusi quelli open-source senza rischi sistemici) e definisce un modulo standard di documentazione (Model Documentation Form), obbligando a includere informazioni dettagliate su architettura, input/output, usi previsti e vietati, processo di training, caratteristiche dei dati, fonti e criteri di qualità, nonché consumo energetico e risorse computazionali. Le versioni precedenti del modello devono essere conservate per almeno 10 anni. Le informazioni sono differenziate per destinatario: alcune pubbliche, altre disponibili su richiesta per l'AI Office o autorità nazionali, e altre ancora riservate ai downstream providers per garantire l'integrazione responsabile del modello. Il Codice prevede che queste informazioni siano aggiornate, affidabili, protette da alterazioni accidentali e corredate da riferimenti a protocolli tecnici condivisi.

Il Capitolo sulla sicurezza e gestione del rischio sistemico riguarda esclusivamente i modelli considerati "ad alto impatto" ai sensi dell'art. 55 dell'AI Act. I fornitori sono tenuti ad adottare un Safety and Security Framework per la gestione dell'intero ciclo di vita del rischio, articolato in: identificazione e analisi di rischi sistemici specifici, valutazioni rigorose del modello (anche tramite red teaming), definizione di criteri di accettabilità e implementazione di misure tecniche per la mitigazione dei rischi (es. filtri sui dati di training, controllo sugli output, cybersecurity). È previsto un sistema di monitoraggio post-mercato che include canali di segnalazione, bug bounty e collaborazione con la ricerca indipendente. I fornitori devono inoltre segnalare tempestivamente eventuali incidenti gravi all'AI Office e alle autorità competenti, e redigere periodicamente Safety and Security Model Reports dettagliati.

Il Capitolo sul copyright si concentra sull'attuazione dell'art. 53(1)(c) dell'AI Act, impegnando i firmatari a sviluppare e mantenere una politica aziendale per il rispetto del diritto d'autore. Tra gli obblighi: garantire che il web crawling avvenga solo su contenuti legalmente accessibili; onorare le riserve di diritti espressi in formato leggibile da macchina (es. robots.txt, metadati); prevenire la generazione di contenuti in violazione del copyright tramite misure tecniche e policy d'uso; predisporre meccanismi trasparenti per la ricezione e gestione dei reclami da parte dei titolari dei diritti. Sebbene non equivalga a prova automatica di conformità, l'adesione al Codice rappresenta una via utile per dimostrarla in sede ispettiva.

Il dibattito accademico sul nuovo Codice di Condotta per l'IA solleva due questioni cruciali per i decisori politici.

Da un lato, una prima analisi (Carey, 2025) suggerisce che il Codice non introduce sostanziali novità, ma si limita a formalizzare pratiche che le principali aziende tecnologiche (come Google e OpenAI) hanno già adottato volontariamente. Secondo uno studio comparativo dell'Università di Oxford, la maggior parte delle misure proposte riflette lo status quo dell'industria, indicando che il Codice allinea la regolamentazione alle pratiche esistenti piuttosto che imporre standard più elevati e innovativi.

Dall'altro lato, emerge una critica più profonda di natura giuridica. Un'analisi pubblicata sull'European Journal of Risk Regulation (Stelling et al., 2025) sostiene che la normativa, anziché chiarire, istituzionalizza l'incertezza legale. Il concetto di "rischio sistemico" viene lasciato vago e la sua definizione concreta viene di fatto delegata alle stesse aziende private attraverso il processo di consultazione del Codice. Questo approccio crea un "punto cieco regolamentare": si rischia di dare priorità ai rischi tecnici, facilmente misurabili, trascurando minacce più complesse ma fondamentali, come l'erosione dei diritti dei cittadini. In pratica, affidando ai privati il compito di definire i rischi, si potrebbe indebolire la capacità del regolatore di proteggere l'interesse pubblico da danni non immediatamente quantificabili.
Nel suo insieme, il Codice costituisce uno strumento di soft law europeo pensato per promuovere una cultura della responsabilità e della cooperazione tra pubblico e privato nella regolazione dei GPAI, fungendo da riferimento dinamico e adattabile per l'attuazione anticipata e graduale dell'AI Act.

2.4 Implicazioni per le PA (dal quadro europeo)

2.4.1 Opportunità e vincoli

La piena implementazione dell'AI Act e delle strategie digitali europee richiede di affrontare non solo gli aspetti normativi, ma anche le capacità operative e le condizioni di contesto che abilitano un'adozione efficace e responsabile dell'IA nella pubblica amministrazione. Di seguito vengono approfondite, da un lato, le competenze e le pratiche di governance necessarie per generare valore pubblico, e dall'altro, i fattori abilitanti e le barriere sistemiche che influenzano l'adozione transfrontaliera di soluzioni digitali innovative nei servizi pubblici europei.

2.4.2 Competenze e pratiche di governance per abilitare la generazione di valore pubblico

L'adozione dell'intelligenza artificiale da parte delle amministrazioni pubbliche europee impone una profonda ristrutturazione delle competenze e delle pratiche di governance. L'integrazione efficace dell'IA nei processi amministrativi e nei servizi pubblici presuppone la capacità degli enti di ripensare le proprie architetture organizzative e decisionali, attivando un coordinamento multilivello e una supervisione proattiva.
Le competenze richieste non si limitano agli aspetti tecnici, ma comprendono anche conoscenze manageriali, giuridiche, etiche e strategiche, secondo un approccio olistico. Una ricerca del Joint Research Centre (JRC) della Commissione Europea, ha individuato 56 competenze chiave, articolate lungo tre dimensioni principali – tecnologica, manageriale e politico-normativa – e tre cluster trasversali (attitudinali, operative, alfabetizzanti) che definiscono il profilo di un'amministrazione capace di generare valore pubblico attraverso l'IA (JRC 2024a, pp. 12-13, 20, 43-44).
Le competenze tecnologiche includono la capacità di gestire la qualità dei dati, la loro raccolta, modellazione e governance, nonché la conoscenza dei fondamenti di machine learning, NLP, visione artificiale e analisi causale. Con l'avvento dell'IA generativa, si è imposta anche l'urgenza di sviluppare competenze di "prompt engineering" (JRC 2024a, pp. 48, 51-56, 90).
La dimensione manageriale comprende la leadership dei team, la lungimiranza strategica, la capacità di gestire il cambiamento e i rischi, la propensione al coinvolgimento degli utenti finali e la

valorizzazione del feedback, insieme alla promozione di approcci multidisciplinari e alla costruzione di partnership operative (JRC 2024a, pp. 57-65).
Le competenze giuridico-etiche e di policy abilitano un'implementazione conforme e responsabile. Tra queste rientrano la capacità di progettare politiche compatibili con l'uso dell'IA, l'auditing dei sistemi per verificarne la compliance, la "literacy" in materia di procurement pubblico per soluzioni IA e la comprensione della teoria delle politiche e delle normative specializzate, come l'AI Act (JRC 2024a, pp. 66-72).
Le pratiche di governance, complementari e interdipendenti rispetto al patrimonio di competenze, sono definite come l'insieme delle capacità organizzative necessarie per governare le strategie tecnologiche in coerenza con gli obiettivi istituzionali. Il modello proposto identifica 34 pratiche articolate lungo tre dimensioni (procedurale, strutturale e relazionale) e tre livelli operativi (strategico, tattico, operativo) (JRC 2024a, p. 14).
Le pratiche procedurali riguardano la predisposizione di processi per la riusabilità dei modelli, lo sviluppo di linee guida etiche e l'adozione di meccanismi di monitoraggio. Quelle strutturali includono l'istituzione di figure chiave come i data stewards, la creazione di comitati etici, registri degli algoritmi, barriere di sicurezza, codici di condotta e forme di supervisione umana. Le pratiche relazionali rafforzano i legami con gli stakeholder attraverso attività di formazione, co-progettazione, costruzione di comunità di pratica e alleanze per lo sviluppo condiviso di know-how (JRC 2024a, pp. 75-80).
La relazione tra competenze e governance è bidirezionale e circolare: la carenza di una delle due componenti compromette la sostenibilità dell'adozione dell'IA. Le amministrazioni si trovano spesso sotto pressione per interpretare e applicare norme complesse come l'AI Act, in contesti organizzativi frammentati e con limitate capacità amministrative, soprattutto nei livelli locali e periferici (JRC 2024a, pp. 17, 20, 81).
Per affrontare queste sfide, il JRC state proposte sei raccomandazioni prioritarie articolate in diciotto azioni, che includono la creazione di programmi formativi interdisciplinari, il finanziamento di ricerca applicata, l'adozione di strategie di reclutamento dedicate, lo sviluppo di reti collaborative, la promozione di ambienti di apprendimento attivo e la partecipazione strutturata degli stakeholder pubblici e privati nei processi decisionali (JRC 2024a, pp. 84-110).

2.4.3 Adozione e implementazione transfrontaliera di soluzioni digitali innovative (GovTech)

Negli ultimi anni si è affermato, anche in Europa, un modello di innovazione amministrativa che valorizza la collaborazione strutturata tra amministrazioni pubbliche e soggetti privati – in particolare start-up e piccole imprese – per progettare, sviluppare e acquisire soluzioni digitali volte a migliorare i servizi pubblici. Questo approccio, spesso indicato con il termine GovTech, integra la capacità tecnologica esterna con l'obiettivo di rendere le amministrazioni più agili, accessibili e centrate sull'utente, contribuendo alla maturità digitale della pubblica amministrazione (JRC 2024b, pp. 10–11).
L'adozione e la diffusione su scala europea di tali soluzioni incontrano oggi una serie di ostacoli sistemici. Secondo un quadro analitico elaborato dal Joint Research Centre, i fattori critici che condizionano lo sviluppo di queste collaborazioni digitali si articolano lungo sette direttrici: regolazione, finanza, cultura, supporto istituzionale, capitale umano, mercati e tecnologia (JRC 2024b, p. 151). Di queste, la dimensione normativa e politica assume un ruolo predominante.

Nonostante l'esistenza di regolamenti comuni, come l'AI Act e l'Interoperable Europe Act, permangono disomogeneità regolative significative tra Stati e tra livelli di governo. Tali divergenze generano incertezza giuridica e aumentano i costi di compliance, ostacolando la scalabilità delle soluzioni digitali sviluppate in un Paese verso altri contesti amministrativi. Differenze nell'interpretazione del GDPR, mancanza di linee guida operative accessibili e limitata attenzione all'adozione di standard aperti e interoperabili aggravano il quadro (JRC 2024b, pp. 168, 186–230).

A questi vincoli si aggiungono criticità economiche. I costi di sviluppo, adattamento e scalabilità delle soluzioni sono spesso elevati e difficilmente sostenibili per le imprese innovative, in particolare se obbligate a partecipare a numerosi progetti pilota senza garanzie di adozione stabile. L'accesso ai mercati pubblici esteri risulta limitato, sia per mancanza di visibilità nelle piattaforme di procurement europee, sia per la difficoltà di instaurare relazioni con i decisori pubblici al di fuori del proprio contesto nazionale. In molti casi, la presenza di misure di favore verso fornitori locali agisce da barriera implicita alla concorrenza (JRC 2024b, pp. 170–259).

Anche i fattori culturali rappresentano un ostacolo rilevante. Le amministrazioni pubbliche tendono a privilegiare interlocutori già noti, mostrando diffidenza verso soluzioni sviluppate all'estero. A ciò si aggiunge la resistenza al cambiamento, le difficoltà linguistiche e le differenze nei modelli istituzionali, che complicano la replicabilità e l'adattamento delle soluzioni digitali tra territori diversi (JRC 2024b, pp. 238–240).

Il capitale umano, da entrambi i lati della collaborazione, rappresenta un punto critico. Le imprese incontrano difficoltà nell'assunzione transfrontaliera, a causa della frammentazione normativa e degli oneri amministrativi. Le pubbliche amministrazioni, dal canto loro, spesso non dispongono delle competenze necessarie per valutare, acquisire e gestire soluzioni digitali complesse. Questo divario di capacità è aggravato dall'assenza di programmi formativi mirati e da una professionalizzazione ancora debole del "cliente pubblico" (JRC 2024b, pp. 249–275).

Dal punto di vista infrastrutturale e di supporto, molte imprese innovative non hanno accesso a servizi legali, finanziari e di networking adeguati a operare su scala europea. Manca un ecosistema che le supporti nell'accreditamento e nella costruzione di fiducia con nuovi interlocutori pubblici. Le difficoltà di integrazione con le infrastrutture IT locali, unitamente all'assenza di standard tecnici condivisi per dati e API, limita fortemente l'interoperabilità (JRC 2024b, pp. 260–277).

Per superare queste barriere, il rapporto propone una serie articolata di raccomandazioni. Tra le priorità strategiche figurano l'armonizzazione dei requisiti normativi a livello europeo, la promozione di pratiche di procurement aperto e orientate alla concorrenza, l'introduzione di certificazioni europee per soluzioni digitali ad uso pubblico e la creazione di fondi dedicati all'acquisizione di tecnologie sviluppate da imprese europee. Sul piano operativo, è auspicabile la diffusione di programmi di formazione per i funzionari pubblici, piattaforme di networking, strumenti per l'assunzione transfrontaliera e meccanismi per aumentare la visibilità delle soluzioni digitali nei mercati pubblici (JRC 2024b, pp. 231–278).

Un ambiente abilitante per l'adozione di soluzioni digitali innovative nei servizi pubblici non può prescindere da un'azione coordinata a livello europeo che rimuova gli ostacoli regolativi, istituzionali e culturali. Promuovere una governance dell'innovazione che includa la dimensione transfrontaliera significa rafforzare la capacità della pubblica amministrazione di affrontare le sfide sistemiche e, al contempo, sostenere lo sviluppo di un mercato digitale europeo più competitivo, inclusivo e orientato al valore pubblico.

Capitolo 3 – Il quadro nazionale

3.1 La Legge italiana sull'IA: principi e finalità

La Legge 23 settembre 2025, n. 132, pubblicata nella Gazzetta Ufficiale n. 223 del 25 settembre 2025, rappresenta il principale intervento del legislatore nazionale per disciplinare in maniera organica la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione dei sistemi e modelli di intelligenza artificiale, garantendone un utilizzo coerente con i principi dell'Unione Europea e con il Regolamento (UE) 2024/1689 (AI Act) (Cassano, 2024; PDCDM, 2024). Il Capo I della Legge (articoli 1-6) definisce le finalità generali e i principi fondamentali che devono informare l'intero ciclo di vita dei sistemi di IA, ponendo al centro la tutela dei diritti fondamentali e la promozione di un'innovazione responsabile.
La Legge persegue un approccio antropocentrico, volto a un utilizzo corretto, trasparente e responsabile dell'IA, capace di coglierne le opportunità tecnologiche e al contempo vigilare sui rischi economici, sociali e sull'impatto sui diritti fondamentali (Cassano, 2024). I principi generali sanciti comprendono:

- il rispetto dei diritti e delle libertà fondamentali previsti dalla Costituzione e dal diritto dell'Unione Europea;
- i principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità;
- lo sviluppo e l'applicazione dei sistemi di IA in modo conforme all'autonomia e al potere decisionale umano, garantendo la conoscibilità, la spiegabilità e la sorveglianza da parte di esseri umani (human-in-the-loop), per prevenire eventuali danni (Cassano, 2024).

La Legge specifica che l'utilizzo di sistemi di IA non deve compromettere il regolare svolgimento democratico della vita istituzionale e politica, né l'esercizio delle funzioni da parte delle istituzioni territoriali, a tutela dei principi di autonomia e sussidiarietà. Particolare attenzione è riservata alla cybersicurezza, considerata precondizione essenziale lungo tutto il ciclo di vita dei sistemi e modelli di IA, secondo un approccio proporzionale e basato sul rischio, con specifici controlli volti a garantirne la resilienza contro tentativi di alterazione o compromissione della sicurezza (Perlusz, 2025).
La Legge afferma inoltre la necessità di garantire alle persone con disabilità il pieno accesso ai sistemi di IA e alle relative funzionalità, in condizioni di uguaglianza e senza discriminazioni, in conformità con la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (Cassano, 2024). Per quanto riguarda l'ambito dell'informazione e della tutela della privacy, il testo stabilisce che l'utilizzo dell'IA deve rispettare la libertà e il pluralismo dell'informazione, la libertà di espressione e i principi di obiettività, completezza e imparzialità, assicurando un trattamento lecito, corretto e trasparente dei dati personali (Cassano, 2024).
In chiave economica, la Legge riconosce l'importanza dell'IA come leva di sviluppo e stabilisce che le autorità pubbliche debbano promuoverne l'uso per accrescere la produttività, migliorare l'interazione uomo-macchina e favorire la creazione di un mercato innovativo e competitivo. Tra le misure indicate, viene previsto che le piattaforme di e-procurement delle pubbliche amministrazioni possano privilegiare soluzioni che garantiscano la localizzazione e l'elaborazione dei dati strategici presso data center situati in Italia, al fine di tutelare la sovranità e la sicurezza dei dati.

Per quanto riguarda le definizioni centrali, l'Articolo 2 del Testo ha subito una rilevante modifica durante il suo iter parlamentare: da definizioni autonome per “sistema di intelligenza artificiale” e “modelli di intelligenza artificiale”, si è passati a un rinvio diretto alle corrispondenti definizioni contenute nell’AI Act. Questa scelta, caldeggiata dalla Commissione europea e sostenuta dal parere del Comitato per la legislazione, ha mirato a garantire armonia e coerenza normativa tra la disciplina nazionale e quella europea, evitando contraddizioni o duplicazioni (Comitato per la legislazione, Camera dei Deputati). In particolare:

- il sistema di intelligenza artificiale è quello definito dall’art. 3, punto 1) del Regolamento (UE) 2024/1689;
- il modello di intelligenza artificiale corrisponde alla definizione dell’art. 3, punto 63) del Regolamento[10];
- il dato viene definito come qualsiasi rappresentazione digitale di atti, fatti o informazioni, anche sotto forma di registrazioni sonore, visive o audiovisive.

Infine, l’Articolo 6 stabilisce esclusioni specifiche per le attività di sicurezza nazionale, cybersicurezza e difesa, nonché per le attività delle forze di polizia, che restano al di fuori dell’ambito di applicazione della legge, pur dovendo essere condotte nel rispetto dei diritti fondamentali. La Legge, all'articolo 5, indirizza le pubbliche amministrazioni a privilegiare, nelle procedure di acquisto, soluzioni che garantiscano la localizzazione dei dati strategici presso data center situati in Italia, al fine di tutelare la sovranità e la sicurezza nazionale (Cassano, 2024).

3.1.1 Disposizioni settoriali (Capo II, artt. 7-15)

Il Capo II della Legge italiana sull’Intelligenza Artificiale disciplina l’utilizzo dell’IA in settori chiave, con l’obiettivo di bilanciare innovazione tecnologica e tutela dei diritti fondamentali. Le disposizioni riguardano la sanità e la disabilità, il lavoro, le professioni intellettuali, la pubblica amministrazione e l’attività giudiziaria, delineando un quadro normativo che solleva al contempo questioni critiche di compatibilità con il diritto europeo e di concreta attuazione (Cassano, 2024).

3.1.2 Sanità e disabilità (artt. 7-10)

La Norma stabilisce che i sistemi di IA devono contribuire al miglioramento del sistema sanitario, supportando prevenzione, diagnosi e cura delle malattie, nel rispetto dei diritti e della protezione dei dati personali. È vietato selezionare o condizionare l’accesso alle prestazioni sanitarie con criteri discriminatori. Viene sancito il diritto dell’interessato a essere informato sull’impiego dell’IA, ribadendo che la decisione finale spetta sempre al professionista medico. I dati utilizzati devono essere affidabili e aggiornati per garantire la sicurezza dei pazienti.

La Legge promuove inoltre sistemi di IA per migliorare l’inclusione delle persone con disabilità, agevolandone accessibilità, autonomia e sicurezza. Viene disciplinata la ricerca scientifica, autorizzando l’uso secondario di dati personali privi di identificativi diretti, previa informativa generale

[10] L'articolo 3, punto 63) dell'AI Act definisce un "modello di IA per finalità generali" (general purpose AI model) come un modello di IA addestrato con grandi quantità di dati, che utilizza l'autosupervisione su larga scala, caratterizzato da una significativa generalità e capace di svolgere un'ampia gamma di compiti distinti. Questa definizione include anche i modelli che possono essere integrati in una varietà di sistemi o applicazioni a valle, ma esclude quelli utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.

online e approvazione dei comitati etici, con obbligo di comunicazione al Garante per la protezione dei dati personali. La gestione dei dati è funzionale anche alla realizzazione di una piattaforma nazionale di IA per l'assistenza territoriale, assegnata all'AGENAS, al fine di uniformare i servizi sanitari digitali[11]. Tra le criticità emerse, sono evidenziati il rischio di sovrapposizione con il GDPR per gli obblighi informativi, la possibile contraddizione con il Codice della privacy in materia di ricerca e la mancanza di una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) nazionale per i sistemi sanitari IA, necessaria per garantire adeguate misure di tutela (Perlusz, 2025; GPDP, 2023; Burelli, 2025).

3.1.3 Lavoro (artt. 11-12)

Il Testo prevede che l'IA sia impiegata per migliorare le condizioni lavorative, tutelare l'integrità psicofisica dei lavoratori, accrescere qualità e produttività, assicurando un utilizzo sicuro, affidabile e rispettoso della dignità umana e della privacy. Il datore di lavoro ha l'obbligo di informare il lavoratore sull'uso dell'IA, garantendo il rispetto dei diritti inviolabili e prevenendo discriminazioni basate su caratteristiche personali o sociali (Cassano, 2024).

Per monitorare l'impatto dell'IA sul mercato del lavoro e definire strategie adeguate, è istituito presso il Ministero del Lavoro un Osservatorio sull'adozione dell'IA, incaricato anche di promuovere attività formative per lavoratori e datori di lavoro, senza nuovi oneri per la finanza pubblica. Si evidenziano criticità legate all'assenza di vincoli specifici per limitare un uso invasivo dell'IA e ai dubbi sulla reale efficacia dell'Osservatorio in assenza di risorse dedicate (Cassano, 2024; Di Salvo, 2024).

3.1.4 Professioni intellettuali (art. 13)

Nelle professioni intellettuali, l'IA è ammessa solo come supporto strumentale, con la prevalenza del lavoro intellettuale del professionista, al fine di preservare il rapporto fiduciario con il cliente. Il professionista ha l'obbligo di informare il cliente sull'uso dell'IA con linguaggio chiaro ed esaustivo (Cassano, 2024).

Le principali criticità riguardano l'ambiguità del concetto di "prevalenza del lavoro intellettuale", termine considerato ambiguo e privo di parametri oggettivi, la mancanza di dettagli sulle modalità dell'informativa e l'assenza di sanzioni in caso di violazione, elementi che rischiano di rendere inefficace la norma e compromettere la fiducia tra professionista e cliente (Di Salvo, 2024).

3.1.5Pubblica amministrazione (art. 14)

La Legge disciplina l'uso dell'IA nella pubblica amministrazione per incrementare l'efficienza dei procedimenti, ridurre i tempi e migliorare la qualità dei servizi offerti. È previsto l'obbligo di garantire la conoscibilità del funzionamento dell'IA e la tracciabilità del suo utilizzo, assicurando che l'IA resti uno strumento di supporto e che la responsabilità decisionale ricada unicamente sul funzionario umano (Cassano, 2024).

Le PA devono adottare misure tecniche, organizzative e formative per un utilizzo responsabile dell'IA, pur senza ulteriori oneri a carico della finanza pubblica. La clausola di invarianza finanziaria suscita

[11] Il Garante ha espresso perplessità sull'attribuzione ad AGENAS della titolarità dei trattamenti effettuati tramite la piattaforma prevista dal DDL, osservando che tale funzione andrebbe ricondotta al Ministero competente, in quanto titolare effettivo dei poteri provvedimentali e decisionali (Provvedimento n. 477 del 2 agosto 2024).

perplessità, nella bibliografia critica, sulla reale possibilità di attuare queste misure senza risorse adeguate, mentre la dottrina evidenzia l'urgenza di investimenti nella formazione del personale e nelle competenze digitali (Cassano, 2024; Mancarella, 2023).

3.1.6 Attività giudiziaria (art. 15)

Nell'attività giudiziaria, l'IA può essere utilizzata per supportare l'organizzazione e la semplificazione del lavoro, ma resta ferma la centralità del magistrato nelle decisioni relative all'interpretazione della legge, alla valutazione dei fatti e all'adozione dei provvedimenti. Il Ministero della Giustizia è incaricato di disciplinare gli impieghi dell'IA e promuovere la formazione dei magistrati e del personale amministrativo, in linea con le classificazioni di alto rischio previste dall'AI Act (Perlusz, 2025) per i sistemi IA destinati alla giustizia (Cassano, 2024).

Tra le criticità segnalate figurano l'eccessiva genericità della norma, che non affronta questioni come la polizia predittiva, il rischio di sovrapposizioni con l'AI Act, la mancanza di un divieto esplicito per l'uso dell'IA nella redazione dei provvedimenti giudiziari e l'ambiguità sulla competenza esclusiva delle sezioni specializzate in materia di impresa (Cassano, 2024; Burelli, 2025; Di Salvo, 2024).

D'Angiolella (2025) evidenzia come l'articolo 15 della legge 132/2025 colmi le lacune dell'AI Act europeo in materia di giustizia, introducendo il principio di **"riserva della giurisdizione umana"**. L'autrice rileva che la disciplina europea, pur classificando i sistemi IA giudiziari come "ad alto rischio", non limita il potere discrezionale dei giudici né definisce la prevalenza del giudizio umano sull'assistenza algoritmica.

La norma italiana stabilisce una gerarchia precisa: il **comma** 1 riserva "sempre" al magistrato ogni decisione su interpretazione della legge, valutazione di fatti/prove e adozione di provvedimenti; **il comma 2** limita l'IA a organizzazione, semplificazione e attività amministrative accessorie; **il comma 3** affida al Ministero della Giustizia l'autorizzazione all'uso dell'IA negli uffici giudiziari; **il comma 4** prevede formazione obbligatoria per magistrati e personale.

Dal punto di vista costituzionale, D'Angiolella radica l'approccio antropocentrico negli artt. 2, 101, 107 e 111 della Costituzione, sostenendo che l'interpretazione giuridica non può essere ridotta a logica algoritmica poiché il diritto è "scienza sociale e umana" che richiede valutazione della "peculiarità del fatto" e degli "interessi concreti delle parti" attraverso un processo mentale che sfugge alla sussunzione meccanica.

3.1.7 Governance nazionale (Capo III, artt. 19-20)

Il Capo III della Norma definisce la governance nazionale, stabilendo un modello che integra le disposizioni del Regolamento (UE) 2024/1689 con misure specifiche per il contesto italiano. L'obiettivo è guidare lo sviluppo e l'adozione dell'IA nel Paese, promuovendo un utilizzo responsabile, trasparente e coerente con i principi europei, garantendo al contempo il coordinamento tra le istituzioni coinvolte (Cassano, 2024; Cappai, 2024).

3.1.8 Strategia nazionale per l'Intelligenza Artificiale (Art. 19)

L'Articolo 19 istituisce la Strategia nazionale per l'Intelligenza Artificiale, documento programmatico volto a orientare lo sviluppo, l'adozione e la regolazione dell'IA in Italia. La strategia è predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, d'intesa con le Autorità nazionali per l'IA designate all'articolo 20.

Sono consultati il Ministero delle Imprese e del Made in Italy, il Ministero dell'Università e della Ricerca e il Ministero della Difesa, mentre il Garante per la protezione dei dati personali (GPDP) ha espresso l'esigenza di essere coinvolto stabilmente nel processo di definizione della strategia (Cappai, 2024).
La strategia è approvata con cadenza almeno biennale dal Comitato Interministeriale per la Transizione Digitale e mira a:

- favorire la collaborazione tra amministrazioni pubbliche e soggetti privati nello sviluppo di sistemi IA;
- coordinare le attività delle amministrazioni pubbliche;
- promuovere la ricerca e la diffusione della conoscenza;
- orientare le misure di sostegno e gli incentivi per lo sviluppo industriale e imprenditoriale;
- assicurare il rispetto dei principi del diritto internazionale umanitario nello sviluppo di sistemi IA.

La Presidenza del Consiglio cura il coordinamento e il monitoraggio dell'attuazione della strategia, avvalendosi dell'Agenzia per l'Italia Digitale (AGID) e, per i profili di cybersicurezza, dell'Agenzia per la Cybersicurezza Nazionale (ACN), trasmettendo i risultati del monitoraggio annualmente alle Camere.

3.1.9 Autorità nazionali per l'IA (Art. 20)

L'Articolo della Legge designa l'Agenzia per l'Italia Digitale e l'Agenzia per la Cybersicurezza Nazionale come Autorità nazionali per l'intelligenza artificiale, incaricate di garantire l'applicazione e l'attuazione della normativa europea e nazionale in materia. La disposizione si allinea all'AI Act, che prevede la designazione, da parte degli Stati membri, di almeno un'autorità nazionale competente e di un'autorità di vigilanza del mercato, oltre a un punto di contatto unico con le istituzioni europee (artt. 70 e 74).
Nel quadro previsto dalla Norma:

- AGID è designata come autorità di notifica ai sensi dell'AI Act. È responsabile di promuovere lo sviluppo dell'intelligenza artificiale, definire le procedure di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi IA, anche con riferimento agli aspetti organizzativi e documentali.
- ACN è designata come autorità di vigilanza del mercato e punto di contatto unico con la Commissione europea e le autorità degli altri Stati membri. Svolge funzioni ispettive e sanzionatorie, in particolare per i profili di cybersicurezza.

Le due autorità condividono inoltre la responsabilità dell'istituzione e gestione congiunta di spazi di sperimentazione per i sistemi IA conformi alla normativa europea e nazionale, in raccordo con i ministeri competenti per i sistemi a duplice uso o per finalità giudiziarie.
Per assicurare il coordinamento tra i soggetti istituzionali, la Legge prevede l'istituzione, presso la Presidenza del Consiglio, di un Comitato di coordinamento, composto dai direttori generali di AGID e ACN e dal Capo del Dipartimento per la Trasformazione Digitale. In caso di necessità, possono essere coinvolti rappresentanti di Banca d'Italia, CONSOB e IVASS. I componenti del Comitato operano senza compenso.
Restano ferme le competenze settoriali delle autorità di vigilanza finanziaria, in coerenza con l'AI Act.
La Legge (art. 20) designa AGID e ACN come Autorità nazionali, ripartendone i compiti, e fa salve le competenze specifiche del Garante per la protezione dei dati personali. Il coordinamento strategico è

invece affidato a un Comitato istituito presso la Presidenza del Consiglio (art. 19), con una composizione prettamente politica e ministeriale. Resta quindi da verificare sul piano operativo come si svilupperà la collaborazione tra le autorità tecniche (AGID, ACN) e l'autorità di garanzia sui dati personali.
Come evidenziato anche da Cappai (2024), è evidente la necessità di rafforzare la dimensione multilivello e interistituzionale della governance dell'IA, garantendo una cooperazione stabile tra autorità tecniche e indipendenti, nell'interesse dell'efficacia regolativa e della tutela dei cittadini.

3.1.10 Disposizioni penali (Capo V, art. 26)

Il Capo V della Legge introduce nuove disposizioni penali volte a contrastare abusi e illeciti connessi all'uso dell'IA, rafforzando la tutela in settori sensibili e aggiornando il quadro normativo esistente (Cassano, 2024).
Tra le principali misure:

- **Aggravanti comuni**: è prevista una nuova circostanza aggravante generale per i reati commessi con sistemi di IA che abbiano costituito mezzo insidioso, ostacolato la difesa o aggravato le conseguenze del reato.
- **Reato di diffusione illecita di deepfake**: viene introdotto l'art. 612-quater c.p., che punisce la diffusione non consensuale di contenuti audio-visivi generati o manipolati con IA idonei a trarre in inganno, con pena da uno a cinque anni di reclusione.
- **Modifiche ad altri reati**: sono previste aggravanti specifiche per truffa, frode informatica e reati finanziari, oltre a un inasprimento delle pene per l'aggiotaggio se realizzato con IA (Coppola, 2024).
- **Diritto d'autore**: viene ribadito che la tutela è riservata alle opere dell'ingegno umano anche se create con l'ausilio dell'IA, escludendo la protezione per opere generate integralmente da sistemi automatici; è disciplinato l'uso di testo e dati per addestrare modelli IA e introdotte sanzioni in caso di violazioni (Cassano, 2024).

Diverse criticità sono emerse:

- **Gold-plating e sovrapposizioni**: alcune norme, come l'obbligo di identificazione dei contenuti generati dall'IA, appaiono più restrittive rispetto all'AI Act e potrebbero configurare un'ipotesi di eccesso regolatorio nazionale (Burelli, 2025).
- **Rischio di superfluità**: la nuova fattispecie di diffusione illecita di deepfake potrebbe sovrapporsi a reati già previsti come diffamazione o stalking (Coppola, 2024).
- **Incertezza giuridica**: l'imposizione di obblighi più gravosi per operatori italiani rispetto a quanto previsto dall'AI Act può generare disparità di trattamento e conflitti con il diritto UE (Burelli, 2024; Di Salvo, 2024).

Box – Criticità trasversali e questioni aperte sul DDL IA

Al termine dell'analisi delle disposizioni contenute nella Legge italiana sull'Intelligenza Artificiale, si ritiene utile proporre un quadro riepilogativo delle principali criticità emerse dalle fonti dottrinali, dai documenti istituzionali e dagli atti ufficiali esaminati. Molte di queste criticità sono già state evidenziate nei paragrafi settoriali, mentre altre sono emerse in modo trasversale nel confronto con i pareri espressi in sede parlamentare e le osservazioni di autorità nazionali e comunitarie. Il

presente box offre una sintesi organica delle questioni ancora aperte, con l'obiettivo di evidenziare i possibili rischi di incoerenza normativa e le difficoltà attuative che potrebbero compromettere un'implementazione efficace e armonica dell'IA nella pubblica amministrazione e nei settori strategici.

- **Incompatibilità con l'AI Act**: obblighi più restrittivi (es. watermarking) e definizioni non perfettamente allineate, con rischio di gold-plating e violazione dell'armonizzazione europea (Cassano, 2024; Burelli, 2025).
- **Sovrapposizione normativa**: disposizioni specifiche in sanità, lavoro e giustizia che rischiano di duplicare o contrastare regole già previste dal GDPR e dall'AI Act (Di Salvo, 2024).
- **Responsabilità legale**: mancanza di chiarezza su chi risponda in caso di danni causati da sistemi IA, con potenziali incertezze per sviluppatori, produttori e utenti (Di Salvo, 2024).
- **Sorveglianza biometrica**: la delega al Governo per disciplinarla solleva criticità, data la rilevanza per i diritti fondamentali e l'assenza di un confronto parlamentare diretto (Di Salvo, 2024).
- **Localizzazione dei data center**: la preferenza per server nazionali, pur motivata da esigenze di sicurezza, potrebbe limitare la libera circolazione dei dati nell'UE e suscitare obiezioni a livello comunitario (Burelli, 2025).
- **Riforma a "costi zero"**: il vincolo di invarianza finanziaria rischia di compromettere la reale attuazione della riforma senza investimenti in risorse, formazione e infrastrutture (Cassano, 2024).
- **Intempestività dell'intervento**: l'anticipo del legislatore italiano rispetto alla piena attuazione dell'AI Act europeo potrebbe generare incoerenze e problematiche di conformità futura (Burelli, 2024).

3.2 Strategia italiana per l'Intelligenza Artificiale 2024-2026

La Strategia italiana per l'Intelligenza Artificiale 2024-2026, pubblicata dall'AGID, si pone l'obiettivo generale di accelerare lo sviluppo del Paese attraverso l'impiego dell'IA, potenziando la produttività delle imprese e l'efficacia della Pubblica Amministrazione. Questa visione strategica mira a consolidare la posizione scientifica dell'Italia, valorizzare la sua tradizione industriale e costruire tecnologie IA "su misura" per le specificità nazionali, evitando di limitarsi all'importazione di soluzioni esterne (AGID, 2024).

La strategia si articola in tre macro-obiettivi strategici:

- **Sostenere la realizzazione e l'adozione di applicazioni di IA**, per supportare pratiche gestionali, modelli produttivi e progetti di innovazione, con particolare attenzione allo sviluppo di sistemi IA "country-specific" per mantenere i vantaggi competitivi italiani.
- **Promuovere l'attività di ricerca scientifica**, fondamentale e applicata, incentivando la connessione con piattaforme internazionali e lo sviluppo di applicazioni IA coerenti con le esigenze competitive e il benessere sociale (welfare, patrimonio culturale, educazione, salute).

- **Creare condizioni favorevoli** per valorizzare il potenziale generativo dell'IA, concentrandosi sulla crescita di talenti con competenze adeguate e sull'efficientamento dei servizi della PA.

Questi macro-obiettivi sono suddivisi in quattro macroaree interconnesse: Ricerca, Pubblica Amministrazione, Imprese e Formazione, sostenute da azioni abilitanti sia infrastrutturali sia di coordinamento. Tra queste spiccano la creazione di un Patrimonio di Conoscenza Nazionale, un registro di dataset e modelli affidabili e riusabili, e l'istituzione di una Fondazione per l'Intelligenza Artificiale, soggetto deputato a gestire fondi, supervisionare il registro, promuovere lo sviluppo dell'IA e coordinare attività di sensibilizzazione e certificazione.

- Obiettivi e linee d'azione per la Pubblica Amministrazione

La Strategia individua l'IA come fattore centrale nella trasformazione digitale della PA, con l'obiettivo di migliorare l'efficienza interna e la qualità dei servizi ai cittadini, attraverso un approccio strutturato, sistematico e multidisciplinare che eviti la frammentazione delle soluzioni e promuova l'interoperabilità.

Gli obiettivi specifici per la PA comprendono:

- supportare i processi amministrativi, ottimizzando la gestione delle risorse pubbliche e finanziando progetti pilota nazionali;
- favorire la fruizione dei servizi per cittadini e imprese, garantendo privacy, trasparenza dei processi e promuovendo la neutralità tecnologica.

Per conseguire tali obiettivi, la Strategia prevede **sei azioni strategiche principali (PA.1 - PA.6)**:

- **Linee guida per l'adozione dell'IA nella PA (PA.1)**, per orientare le amministrazioni verso un uso consapevole, promuovendo best practices e definendo standard minimi funzionali. Il Piano Triennale prevede la redazione di queste linee guida entro dicembre 2024, con l'avvio di almeno 150 progetti di innovazione con IA entro il 2025 e 400 entro il 2026.
- **Linee guida per il procurement di IA (PA.2)**, integrando le normative ICT esistenti e accompagnando le PA nella definizione delle specifiche tecniche per garantire sicurezza e conformità normativa.
- **Linee guida per la realizzazione di applicazioni IA (PA.3)**, finalizzate a incentivare lo sviluppo di soluzioni IA interne alle PA, promuovendo la formazione del personale e il rispetto delle normative UE. Il Piano Triennale prevede la realizzazione di almeno 50 progetti IA entro il 2025 e 100 entro il 2026.
- **Semplificazione per cittadini e imprese (PA.4)**, tramite soluzioni IA che agevolino la fruizione dei servizi pubblici, come la compilazione automatica di moduli o l'automazione di processi.
- **Efficientamento dei processi interni (PA.5)**, mediante lo sviluppo di sistemi IA per la verifica degli atti, la digitalizzazione e la gestione documentale. Il Piano prevede il dispiegamento su scala nazionale entro il 2026.
- **IA nelle scuole per la PA (PA.6)**, con percorsi di upskilling e la creazione di un Dipartimento dedicato presso la Scuola Nazionale dell'Amministrazione, includendo corsi post-laurea e attività di monitoraggio dell'impatto formativo.

3.2.1 Le altre macroaree strategiche: Ricerca, Imprese e Formazione

A fianco dell'ambito Pubblica Amministrazione, la Strategia italiana per l'Intelligenza Artificiale 2024-2026 individua altre tre macroaree prioritarie di intervento: Ricerca, Imprese e Formazione. Queste aree, interconnesse tra loro e con le azioni previste per la PA, sono essenziali per costruire un ecosistema nazionale dell'IA in grado di valorizzare le specificità italiane, rafforzare la competitività industriale e promuovere una cultura diffusa dell'innovazione, in linea con i principi europei di affidabilità, trasparenza e centralità della persona (AGID, 2024).

Nell'area **Ricerca**, la strategia intende rafforzare investimenti sia nella ricerca fondamentale che applicata, consolidando iniziative come il Partenariato Esteso FAIR, coinvolgendo università, enti di ricerca e stakeholder industriali, per sviluppare modelli linguistici italiani, progetti interdisciplinari legati al benessere sociale, e programmi competitivi ispirati alle grandi challenge internazionali. È previsto un piano straordinario per attrarre e trattenere talenti, insieme a investimenti per potenziare collaborazioni con partner europei e internazionali.

Sul fronte delle **Imprese**, la strategia punta a stimolare l'adozione di soluzioni IA, con un focus su PMI e start-up, rafforzando la competitività del comparto ICT nazionale. Tra le azioni previste figurano la creazione di facilitatori territoriali per l'IA, fondi dedicati allo sviluppo e all'adozione di tecnologie, laboratori di IA applicata per favorire la sperimentazione congiunta tra imprese, università e centri di ricerca, e la realizzazione di spazi di sperimentazione normativa (sandbox) per testare innovazioni in contesti regolati.

Infine, nella macroarea **Formazione**, la strategia promuove percorsi di alfabetizzazione digitale e iniziative di upskilling e reskilling, con un'attenzione particolare alla riduzione del divario di genere nelle discipline STEM. Sono previsti corsi per docenti e studenti fin dalle scuole primarie, percorsi universitari e post-laurea, programmi di mobilità, sostegno al Dottorato Nazionale in IA e attività di sensibilizzazione per un uso consapevole dell'IA da parte dei cittadini. L'obiettivo è sviluppare un capitale umano qualificato e aggiornato, in grado di accompagnare la trasformazione digitale di PA e imprese.

A sostegno di tutte le aree, la strategia prevede un sistema di monitoraggio con indicatori di performance e l'analisi di progetti bandiera (flagship projects) per valutare l'impatto delle azioni. Sono individuati rischi come la possibilità di un approccio timido o meramente imitativo, l'omogeneizzazione culturale con modelli esteri, l'iper-regolazione che potrebbe portare a incoerenze con l'AI Act europeo, il divario digitale, la trasformazione del mercato del lavoro e l'inefficacia derivante dalla rapidità evolutiva dell'IA. Per ciascuno di questi rischi sono delineate misure di mitigazione, come percorsi di formazione, investimenti in tecnologie conformi ai valori europei e sistemi di coordinamento tra attori pubblici e privati (AGID, 2024).

3.3 Il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026: focus sull'Intelligenza Artificiale

Il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026, i cui contenuti sono stati aggiornati al 2025, dedica ampio spazio all'Intelligenza Artificiale, riconoscendola come una leva strategica per la modernizzazione del settore pubblico italiano. L'IA è trattata in particolare nel Capitolo 5 – Dati e Intelligenza Artificiale della Parte Seconda (Componenti tecnologiche) e nella Parte

Terza – Strumenti, delineando un quadro organico di principi, obiettivi, strumenti operativi e casi concreti.
Nel Capitolo 5, la valorizzazione del patrimonio informativo pubblico è individuata come obiettivo strategico per abilitare soluzioni IA efficaci. L'IA viene definita come un catalizzatore di cambiamento per migliorare l'efficienza e l'efficacia dei processi amministrativi, con potenzialità che spaziano dall'automazione di attività ripetitive all'aumento delle capacità predittive e alla personalizzazione dei servizi. Il Piano si pone in coerenza con il Regolamento (UE) 2024/1689 (AI Act), recependo la classificazione dei rischi (inaccettabile, elevato, limitato, minimo) e l'obbligo di trasparenza per i grandi modelli generalisti di IA, e con la Strategia Italiana per l'Intelligenza Artificiale 2024-2026, richiamando le quattro macroaree strategiche (Ricerca, Pubblica Amministrazione, Industria, Formazione) e le relative azioni abilitanti.
Il Piano valorizza le esperienze già avviate nella PA italiana, come gli algoritmi di machine learning di Agenzia delle Entrate e INAIL per l'analisi di comportamenti sospetti, i chatbot di INPS per semplificare l'interazione con gli utenti, o i progetti ISTAT sull'uso dell'IA generativa per migliorare la gestione e l'interoperabilità dei dati. Per diffondere l'adozione responsabile dell'IA, AGID promuove la creazione di Ambienti di Sperimentazione e Sviluppo, hub nazionali e regionali in cui le amministrazioni possano apprendere, testare e sviluppare soluzioni IA, con la possibilità di riuso dei risultati tra enti.
Il Piano individua alcuni principi generali per l'uso dell'IA nella PA, tra cui: migliorare i servizi e ridurre i costi; adottare un approccio basato sul rischio; garantire trasparenza, responsabilità e supervisione umana; assicurare inclusività, privacy e sicurezza; valutare la sostenibilità ambientale; e considerare standard tecnici internazionali ed europei. Tali principi sono declinati in obiettivi e risultati attesi come l'Obiettivo 5.4, dedicato ad aumentare la consapevolezza delle PA nell'adozione dell'IA attraverso linee guida, e l'Obiettivo 5.5, che punta allo sviluppo di basi di dati nazionali strategiche per la conoscenza condivisa.
Nella Parte Terza – Strumenti, il Piano propone modelli, buone pratiche e checklist per supportare le amministrazioni nell'adozione dell'IA. Lo Strumento 5 – Intelligenza Artificiale nella PA offre linee guida per navigare il quadro normativo (AI Act, GDPR), promuovendo digitalizzazione, efficienza e una governance trasparente. Sono illustrati contributi significativi come quelli di CINI, INAIL, INPS e ISTAT, che descrivono casi concreti di IA applicata: dall'analisi del rischio e la gestione dei dati, alla classificazione automatica della PEC e allo sviluppo di ontologie da linguaggio naturale.
Tra gli esempi concreti individuati e trattati dal piano, lo Strumento 13 approfondisce l'approccio di INAIL all'IA, descrivendo progetti di automazione, analisi predittiva per la prevenzione degli infortuni e supporto alle attività legali, mentre lo Strumento 14 illustra l'esperienza della Regione Puglia, che ha istituito un Centro di Competenza Regionale sull'IA per presidiare le applicazioni nella PA, sviluppare linee di indirizzo e garantire un uso sicuro, trasparente e tracciabile delle tecnologie IA, collaborando attivamente con AGID e la Strategia nazionale.

3.4 Linee guida AGiD per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione

Le Linee guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, attualmente in fase di definizione da parte dell'Agenzia per l'Italia Digitale (AGID), rappresentano uno strumento essenziale per accompagnare le amministrazioni pubbliche italiane verso un utilizzo consapevole,

responsabile e conforme dell'IA nei processi e nei servizi offerti a cittadini e imprese. La redazione di queste linee guida si inserisce in un quadro strategico e normativo delineato dalla Strategia Italiana per l'Intelligenza Artificiale 2024-2026 e dal Piano Triennale per l'Informatica nella PA 2024-2026, che individuano l'IA come fattore abilitante per la trasformazione digitale e come tecnologia prioritaria per l'innovazione del settore pubblico (AGID, 2024).
La necessità di un documento organico che orienti la PA nell'adozione dell'IA deriva anche dalle disposizioni previste dal Disegno di Legge sull'Intelligenza Artificiale, che attribuisce ad AGID un ruolo centrale nella definizione di procedure, strumenti e standard per l'utilizzo dell'IA in ambito pubblico, in linea con quanto stabilito dall'AI Act (Regolamento UE 2024/1689). Le linee guida si propongono di colmare il divario tra il quadro normativo europeo e l'implementazione concreta dell'IA nelle amministrazioni, assicurando coerenza con i principi di trasparenza, responsabilità e supervisione umana sanciti dall'AI Act e dal GDPR.
A conferma dell'approccio inclusivo e partecipativo adottato, la bozza delle linee guida è stata sottoposta a consultazione pubblica dal 18 febbraio al 20 marzo 2025, con l'obiettivo di raccogliere contributi da amministrazioni, imprese, esperti, associazioni e cittadini, così da costruire uno strumento condiviso e rispondente alle esigenze concrete degli enti pubblici, in linea con le migliori pratiche nazionali e internazionali. In questo contesto, le linee guida rappresentano non solo un supporto tecnico e metodologico per le PA, ma anche uno strumento per favorire l'adozione armonizzata dell'IA sul territorio nazionale, riducendo il rischio di frammentazione normativa e promuovendo un'innovazione tecnologica etica, sostenibile e rispettosa dei diritti fondamentali.

3.4.1 Finalità delle Linee guida AGID per l'adozione dell'IA nella Pubblica Amministrazione

Le Linee guida AGID per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione perseguono tre finalità principali che delineano il quadro di riferimento per un utilizzo dell'IA responsabile, etico e conforme alle normative.
La prima finalità è guidare le amministrazioni nell'acquisizione, sviluppo e gestione di soluzioni IA, orientandole nelle modalità di adozione dei sistemi intelligenti, con particolare attenzione agli aspetti di conformità normativa e all'impatto organizzativo. Le Linee guida, come precedentemente discusso previste dal Piano Triennale per l'Informatica nella PA 2024-2026, forniscono indicazioni per definire obiettivi operativi chiari, pianificare le attività, assegnare responsabilità, determinare risorse finanziarie, tecnologiche e umane adeguate e monitorare i risultati. Le amministrazioni sono chiamate a strutturare processi, politiche e strumenti per governare il ciclo di vita dei sistemi IA, integrando un approccio sistematico e documentato di project management.
La seconda finalità è promuovere l'uso etico, sicuro, responsabile e trasparente dell'IA nella PA. Le Linee guida sottolineano la necessità di adottare l'IA nel pieno rispetto delle normative europee e nazionali, monitorando l'evoluzione regolatoria per garantirne la conformità. Le amministrazioni devono implementare politiche di gestione del rischio per prevenire violazioni dei diritti fondamentali, proteggere i dati personali e assicurare la responsabilità ultima delle decisioni. La trasparenza è un requisito fondamentale, da garantire sia nella comprensibilità del funzionamento dei sistemi, sia nell'informazione agli utenti che interagiscono con l'IA, rendendoli consapevoli di capacità e limiti delle soluzioni adottate. Particolare attenzione è dedicata alla sicurezza cibernetica: le PA devono tutelare i sistemi IA da tentativi di alterazione o uso illecito. Le Linee guida promuovono inoltre la definizione di

codici etici interni per un uso equo e responsabile dell'IA, in coerenza con i principi europei e senza abbassare le tutele previste dalle normative vigenti.
La terza finalità è favorire l'interoperabilità, la standardizzazione e il riuso di soluzioni IA tra enti pubblici. A tal fine, le amministrazioni sono invitate ad allinearsi agli standard tecnici nazionali, europei e internazionali, per garantire interoperabilità, manutenibilità e sicurezza dei sistemi IA. Le Linee guida incoraggiano la collaborazione tra enti pubblici per sperimentare e sviluppare soluzioni comuni, promuovendo la partecipazione a learning communities per stimolare il capacity building e la condivisione di buone pratiche, così da replicare o scalare progetti di successo. È inoltre valorizzata la riutilizzabilità dei modelli IA, con la definizione di procedure chiare e la gestione dei dati finalizzata a favorire la circolazione e il riuso di dataset pubblici. In linea con la Strategia Italiana per l'Intelligenza Artificiale 2024-2026, le Linee guida sostengono la creazione di un registro di dataset e modelli riusabili, costruiti secondo principi di trasparenza e fairness, per accelerare lo sviluppo di soluzioni innovative. La capacità di rendere i dati interoperabili e "parlanti" rappresenta infine un elemento strategico per estendere la base di conoscenza della PA, abilitando nuove opportunità di utilizzo intelligente del patrimonio informativo pubblico.

3.4.2 Contenuti principali delle Linee guida AGID per l'adozione dell'IA nella Pubblica Amministrazione

Le Linee guida AGID propongono un approccio strutturato che accompagna le amministrazioni lungo tutte le fasi del ciclo di vita di un sistema di IA, definito secondo il modello dell'OCSE, che copre dalla pianificazione iniziale alla dismissione. Questo ciclo comprende:

- **Pianificazione e design**, in cui si stabiliscono obiettivi, requisiti, dati necessari e architettura del sistema;
- **Raccolta e processamento dei dati**, con attività di pulizia, integrazione e trasformazione;
- **Costruzione o addestramento dei modelli**, con eventuale uso di modelli pre-addestrati e tecniche di transfer learning;
- **Testing, verifica e validazione**, per controllare che il sistema soddisfi i requisiti e correggere anomalie;
- **Messa a disposizione e integrazione**, quando il sistema è reso operativo nei processi della PA;
- **Operatività e monitoraggio**, fase in cui si verifica il corretto funzionamento, si rilevano anomalie e si effettuano riaddestramenti;
- **Ritiro o disattivazione**, per gestire in modo sicuro la chiusura del sistema e i dati associati (AGID, Linee guida, 2024).

Le Linee guida individuano **principi fondamentali** che ogni PA deve rispettare nell'adozione dell'IA, tra cui:

- **Conformità normativa**, con obbligo di rispettare AI Act, GDPR e normativa nazionale;
- **Rispetto dei valori fondamentali dell'UE**, come dignità, libertà, uguaglianza e giustizia;
- **Gestione del rischio**, tramite politiche adeguate per prevenire violazioni dei diritti fondamentali;
- **Protezione dei dati personali**, garantendo qualità, affidabilità e aggiornamento dei dati;
- **Responsabilità umana**, con obbligo per la PA di mantenere la responsabilità finale delle decisioni e identificare chiaramente i ruoli di tutti gli attori coinvolti;

- **Inclusività e accessibilità**, assicurando equità, parità di genere, rispetto delle diversità culturali e prevenzione di bias algoritmici;
- **Trasparenza**, intesa come spiegabilità delle decisioni e funzionamento dei sistemi, con informazioni chiare agli utenti sull'interazione con l'IA;
- **Sicurezza cibernetica**, per proteggere i sistemi IA da attacchi e utilizzi illeciti;
- **Supervisione umana**, per garantire la possibilità di verifica, correzione o sostituzione del sistema da parte del personale;
- **Adozione di standard tecnici nazionali e internazionali**, per garantire interoperabilità e manutenibilità;
- **Sostenibilità ambientale**, valutando l'impatto energetico e ambientale dell'IA (AGID, Linee guida, 2024).

Le Linee guida approfondiscono anche la gestione dei dati, sottolineando come la qualità, la rappresentatività, la disponibilità e la tracciabilità siano prerequisiti essenziali per costruire sistemi IA affidabili. Viene distinta la gestione di dati di addestramento, validazione e prova, provenienti da fonti interne o esterne alla PA, con la raccomandazione di pubblicare come open data quelli non sensibili, rilasciati con licenze permissive per favorirne il riuso.

Un altro punto cruciale è la sicurezza cibernetica, per la quale le Linee guida identificano specifiche tassonomie di attacco – come evasion attacks, poisoning attacks, privacy attacks e abuse attacks – e richiedono alle PA di adottare un approccio di gestione del rischio che possa essere conforme al framework NIST AI RMF[12]. Le PA devono integrare la sicurezza in ogni fase del ciclo di vita del sistema IA e adottare misure per proteggere asset, modelli, dati e identità, nonché predisporre piani di risposta agli incidenti.

Sul piano della conformità normativa, le Linee guida ribadiscono l'obbligo per le PA di classificare i sistemi IA in base al livello di rischio previsto dall'AI Act (vietati, ad alto rischio, rischio limitato, minimo o nullo), adempiere agli obblighi di supervisione umana e documentazione e realizzare, quando richiesto, la Valutazione d'Impatto sui Diritti Fondamentali (FRIA) e la Valutazione d'Impatto sulla Protezione dei Dati (DPIA).

Le Linee guida affrontano anche la necessità di investire nella formazione e nelle competenze: le PA devono promuovere l'AI literacy tra i propri dipendenti, affiancando alla conoscenza di base una padronanza delle normative e delle pratiche operative. Sono identificate figure professionali chiave come data engineer, machine learning engineer, AI ethicist ed esperto di protezione dei dati personali, e viene raccomandata la partecipazione a learning communities per condividere buone pratiche e sviluppare una cultura diffusa dell'IA.

Viene inoltre introdotto un modello di maturità, uno strumento pratico sviluppato dagli Osservatori Artificial Intelligence e Agenda Digitale del Politecnico di Milano. Basato sull'analisi di numerosi casi di implementazione dell'IA nel settore pubblico, il modello ha l'obiettivo di aiutare le amministrazioni a

[12] Il *NIST Artificial Intelligence Risk Management Framework (AI RMF)*, pubblicato dal National Institute of Standards and Technology (NIST) degli Stati Uniti (NIST.AI.100-1, 2023), è un modello di riferimento internazionale che definisce principi, processi e controlli per la gestione dei rischi legati all'adozione dell'IA, articolati in quattro funzioni principali: GOVERN, MAP, MEASURE e MANAGE. Il framework aiuta le organizzazioni a integrare la gestione del rischio dell'IA in tutte le fasi del ciclo di vita dei sistemi, promuovendo sicurezza, trasparenza e responsabilità.

identificare le aree chiave di intervento, definire gli elementi essenziali dei diversi stadi di preparazione e delineare un percorso consapevole per diventare una PA AI-ready, ovvero pronta a integrare l'IA nei propri processi.
Il modello si articola su cinque dimensioni, ciascuna con quattro livelli di progressiva maturità:

- Dati e patrimonio informativo, che valuta la qualità e disponibilità dei dati essenziali per lo sviluppo di soluzioni IA, distinguendo fasi che vanno dall'assenza di infrastrutture fino a una gestione di dati di alta qualità, completi e aggiornati.
- Metodologia e algoritmi, che riguarda la capacità della PA di sviluppare o personalizzare algoritmi per i propri progetti: dal livello più basso, in cui manca la conoscenza di base, fino alla capacità di sviluppare soluzioni ad hoc interne, integrate eventualmente con risorse esterne.
- Organizzazione e competenze, che misura la presenza di figure e risorse specializzate, passando dall'assenza totale di competenze all'istituzione di un vero e proprio centro di hcompetenza formalizzato per la gestione dell'IA.
- Cultura aziendale, che esamina la consapevolezza e apertura dell'organizzazione all'innovazione: dai contesti incentrati solo sul core business, alla consapevolezza diffusa dei benefici dell'IA e alla disponibilità dei dipendenti a rivedere le proprie mansioni per integrarsi con le nuove tecnologie.
- Relazione con cittadini e imprese, che valuta il coinvolgimento degli utenti finali nei progetti IA, andando dall'assenza di iniziative di comunicazione fino al coinvolgimento attivo e alla raccolta di feedback diretto per co-creare servizi pubblici più efficaci e innovativi.

Questo modello permette alle amministrazioni di auto-valutarsi o di essere valutate esternamente, fornendo una mappatura precisa del proprio stato di maturità e supportando la definizione di priorità e obiettivi di miglioramento. È essenziale considerare tutte le dimensioni con una visione integrata: un'adozione equilibrata e coordinata dell'IA evita interventi frammentari che rischierebbero di ostacolare la crescita complessiva dell'organizzazione. Il modello è flessibile e tiene conto delle diverse dimensioni delle PA italiane: mentre per piccoli enti potrebbe non essere necessario ambire al massimo livello in ogni area, le amministrazioni di maggiore complessità potrebbero puntare a una maturità avanzata e armonica in tutte le dimensioni.

3.4.3 Approccio metodologico per l'adozione dell'IA nella Pubblica Amministrazione

Le Linee guida AGID per l'adozione dell'IA nella PA sono state sviluppate nell'ambito del Tavolo di concertazione del Piano Triennale per l'Informatica nella PA, un gruppo di lavoro ampio e rappresentativo che ha coinvolto agenzie nazionali (AgID, ACN, ANAC), associazioni di enti locali (ANCI, Conferenza delle Regioni e delle Province autonome, UPI), ministeri, dipartimenti centrali e grandi enti pubblici come INAIL, INPS, ISTAT e IPZS. Questa partecipazione estesa riflette un approccio collaborativo che mira a promuovere strategie condivise per l'adozione dell'IA, favorendo modelli comuni o replicabili e incentivando la cooperazione tra amministrazioni.
L'approccio metodologico delle Linee guida incoraggia le PA a coinvolgere attivamente tutti gli stakeholder rilevanti:

- Definire codici etici sull'uso dell'IA con il contributo di società civile, università, centri di ricerca e associazioni di tutela dei diritti.
- Promuovere formazione e comunità di pratica, come le learning communities per i Responsabili della Transizione Digitale (RTD) e i loro uffici (UTD), valorizzando progetti come ReTe Digitale di AgID per lo scambio di buone pratiche.
- Stabilire collaborazioni con altre PA, partecipando a progetti di ricerca congiunti con università e centri di competenza per sperimentare soluzioni IA innovative.
- Coinvolgere cittadini e imprese secondo un modello multistakeholder, riducendo asimmetrie informative e promuovendo attività di society-in-the-loop come consultazioni pubbliche e feedback attivi. La comunicazione istituzionale deve essere trasparente, rendendo i cittadini consapevoli dell'uso dell'IA nei servizi pubblici.
- Gestire i dati in modo integrato, creando gruppi di lavoro trasversali che coinvolgano responsabili dei vari domini, il Responsabile della Protezione dei Dati (RPD) e, se possibile, referenti di hub nazionali o regionali che aggregano infrastrutture, servizi e contratti a beneficio del territorio.

Le Linee guida sono progettate con una struttura modulare e aggiornabile, che consente di adeguare gli allegati tecnici (strumenti) al rapido evolversi del contesto tecnologico e normativo. Tra gli allegati principali figurano strumenti pratici come il succitato modello di maturità, la valutazione del rischio e d'impatto, il codice etico, i casi d'uso e le norme tecniche di riferimento, che possono essere aggiornati senza modificare l'impianto complessivo del documento. Questa flessibilità, prevista anche dall'art. 14-bis del CAD, permette di adattare il quadro operativo delle PA al progresso dell'IA e alle future evoluzioni dell'AI Act.

Le Linee guida delineano inoltre ambiti prioritari di applicazione e funzionalità dell'IA nella PA, frutto dell'analisi di esperienze nazionali ed europee e delle sperimentazioni in corso: miglioramento dell'efficienza operativa (es. supporto decisionale, gestione documentale), qualità dei servizi per cittadini e imprese (es. personalizzazione, accessibilità), e sicurezza dei dati e delle infrastrutture. Tra le funzionalità chiave individuate figurano l'analisi e classificazione di testo e contenuti multimediali, la generazione di nuovi contenuti, i sistemi di raccomandazione, le decisioni basate sui dati e l'orchestrazione di processi complessi. Questi esempi offrono un quadro pratico di come l'IA può trasformare i servizi pubblici, stimolando la diffusione di buone pratiche replicabili.

Come anticipato, le Linee guida sono state progettate come strumento operativo e dinamico, destinato a diventare il riferimento per le amministrazioni pubbliche italiane nell'adozione, sviluppo e gestione dei sistemi di IA. La loro struttura modulare, corredata da allegati aggiornabili, consente di adattarle ai rapidi cambiamenti tecnologici e normativi, in coerenza con il quadro legislativo nazionale sul digitale (dunque in coerenza con il quadro normativo definito dal Piano Triennale per l'Informatica nella PA, che attribuisce ad AgID la responsabilità di redigere e aggiornare le Linee guida in materia di digitalizzazione e con l'art. 14-bis CAD - Codice dell'amministrazione digitale).

Il documento stabilisce che AgID non si limita a redigere e pubblicare le Linee guida, ma assume un ruolo centrale nel supportare concretamente le PA, promuovendo attività di accompagnamento come la partecipazione dei Responsabili della Transizione Digitale a learning communities (es. ReTe Digitale), la raccolta e il monitoraggio dei casi d'uso e la diffusione capillare delle Linee guida presso i soggetti decisori. Questo supporto mira a favorire l'adozione consapevole e armonizzata dell'IA, assicurando

che le amministrazioni siano in grado di implementare soluzioni coerenti con i principi di eticità, responsabilità e sicurezza.
Il percorso attuativo delineato dalle Linee guida richiede alle PA di integrare questi riferimenti nei propri strumenti di programmazione strategica e organizzativa (come i PIAO), di sviluppare percorsi formativi interni e di collaborare attivamente con AgID per monitorare e migliorare l'efficacia delle applicazioni di IA nella Pubblica Amministrazione.

Capitolo 4: Adozione, Applicazioni e Lezioni per le Policy in Europa e in Italia

4.1 Introduzione

Dopo aver delineato, nei capitoli precedenti, il complesso quadro normativo e strategico che regola lo sviluppo dell'intelligenza artificiale a livello europeo e nazionale, il presente capitolo sposta l'analisi dal piano astratto a quello operativo. L'obiettivo è comprendere come l'IA stia effettivamente prendendo forma all'interno delle amministrazioni pubbliche, passando dalla "teoria" delle regole alla "pratica" delle implementazioni concrete.
La finalità di questo capitolo non è quella di realizzare un censimento esaustivo di tutte le applicazioni esistenti, un compito tanto vasto quanto potenzialmente sterile. Si è scelto, piuttosto, di procedere con un'analisi qualitativa mirata, selezionando una serie di casi di studio emblematici che possano offrire spunti di riflessione e lezioni strategiche utili per i decisori pubblici.
La metodologia di analisi adottata è composita. Si basa su una ricognizione di fonti istituzionali e report di settore (come quelli prodotti dal Joint Research Centre della Commissione Europea e dagli Osservatori nazionali specializzati) e sulla cosiddetta "letteratura grigia".
Il capitolo si apre con una panoramica sullo stato generale di adozione dell'IA nelle amministrazioni locali e regionali a livello europeo, per fornire un contesto ampio sulle tendenze in atto. Successivamente, l'analisi si focalizzerà su specifici casi di studio nazionali ed europei esplorando le iniziative in corso e le potenzialità ancora inespresse.

4.2 Lo stato di adozione dell'IA nelle amministrazioni locali: un quadro generale

Prima di esaminare i singoli casi di studio, è fondamentale inquadrare le tendenze generali che caratterizzano l'adozione dell'intelligenza artificiale e dell'IA generativa (GenAI) da parte delle amministrazioni locali e regionali (LRA) in Europa. Un recente studio del Comitato Europeo delle Regioni (European Committee of the Regions et al., 2024), basato su un'ampia indagine, offre una fotografia dettagliata del panorama attuale, evidenziando i livelli di maturità, gli ambiti di applicazione, le sfide e i fattori abilitanti che accomunano gli enti pubblici a livello subnazionale.
L'analisi presentata si fonda su un approccio metodologico misto, che combina diverse fonti per garantire la robustezza dei risultati. Il fulcro della ricerca è costituito da un'indagine su larga scala (survey) distribuita a tutte le amministrazioni locali e regionali dei 27 Stati membri dell'Unione Europea, tradotta in 23 lingue ufficiali per massimizzare la partecipazione. L'indagine, che ha raccolto 119 risposte complete e valide, è stata affiancata da un'approfondita revisione della letteratura accademica e istituzionale, e arricchita da 12 interviste semi-strutturate con esperti e funzionari del settore. La raccolta dei dati si è svolta tra settembre 2023 e febbraio 2024, offrendo così una visione aggiornata del fenomeno.

4.2.1 Risultati Chiave dello Studio: Tendenze e Sfide nell'Adozione dell'IA

L'indagine del Comitato delle Regioni delinea un quadro ricco di spunti, evidenziando le dinamiche attuali e le traiettorie future dell'adozione dell'IA a livello subnazionale.

- **Tassi di Adozione e Utilizzo**: Lo studio registra un tasso di adozione significativo, con circa il 27% delle amministrazioni locali e regionali (LRA) che dichiara di utilizzare soluzioni di IA. L'adozione è direttamente correlata alla dimensione demografica dell'ente, con una concentrazione maggiore nelle LRA più grandi e un'applicazione prevalente nell'Europa Occidentale. L'uso più comune della tecnologia è finalizzato a migliorare i "servizi basati sull'IA per la pubblica amministrazione", e di conseguenza il beneficio più frequentemente riscontrato è l'"ottimizzazione della gestione interna".
- **Sfide e Fattori Determinanti**: Il principale motore (driver) che spinge le amministrazioni verso l'IA è la ricerca di un "Miglioramento dell'Efficienza Amministrativa". Le barriere più significative, tuttavia, non sono di natura politica ma strutturale e trasversale: la "mancanza di competenze ed esperienza", i "vincoli di bilancio" e una "scarsa conoscenza dei processi di standardizzazione". Al contrario, la mancanza di interesse politico o di coinvolgimento degli stakeholder sono percepiti come ostacoli minori, a riprova di una volontà di innovare che si scontra con limiti operativi concreti.
- **Priorità Future ed Elementi Emergenti**: Emerge una chiara discrepanza tra lo stato attuale e le aspirazioni future. Se oggi il focus è sull'efficienza interna, le LRA credono che la priorità di domani debba essere quella di "migliorare l'erogazione dei servizi pubblici e l'interazione cittadino/governo". Un dato rilevante riguarda l'uso dell'IA per i processi decisionali, visto con una certa cautela dalla maggior parte degli enti. Infine, l'analisi evidenzia l'importanza crescente di fattori quali le considerazioni etiche e la sostenibilità ambientale (Green AI) come elementi chiave per un'adozione di successo.

4.2.2 Raccomandazioni per una Governance efficace dell'IA a Livello Locale

Sulla base dei risultati emersi, lo studio formula otto raccomandazioni politiche strategiche, che delineano un percorso d'azione coordinato per i diversi livelli di governo. Un ruolo di primo piano viene attribuito proprio alle Amministrazioni Locali e Regionali (LRA), chiamate a essere protagoniste attive nel governare la transizione verso l'IA, con un focus particolare sulla governance interna, sul rafforzamento della fiducia pubblica e sulla garanzia di un'adozione inclusiva.

L'analisi sottolinea come una delle sfide più critiche per le LRA sia la necessità di superare la frammentazione interna. A questo proposito, la settima raccomandazione (R7) invita esplicitamente gli enti a investire nella creazione di legami più forti tra i vari dipartimenti, in particolare tra i team manageriali e politici e i team tecnici e informatici. Una maggiore cooperazione interna è vista come il presupposto fondamentale per migliorare la flessibilità, la resilienza e, in ultima analisi, l'efficacia nello sviluppo e nell'implementazione di soluzioni di IA.

Strettamente legata alla governance interna è la capacità di costruire fiducia e legittimità sociale attorno all'uso dell'IA. La seconda raccomandazione (R2) è interamente dedicata a questo aspetto e si rivolge alle LRA, esortandole a coinvolgere attivamente i cittadini nel processo di sviluppo dell'IA. Tale coinvolgimento non deve limitarsi a una consultazione formale, ma tradursi in pratiche concrete di co-creazione, nella raccolta continua di feedback dagli utenti e nell'organizzazione di sessioni di test aperte. L'obiettivo è duplice: da un lato, rendere i servizi più inclusivi e realmente rispondenti ai bisogni

della comunità; dall'altro, aumentare la trasparenza e l'accettazione pubblica di queste nuove tecnologie.
Lo studio pone un forte accento sulla responsabilità delle LRA nel prevenire che l'IA diventi un fattore di esclusione. La quarta raccomandazione (R4), rivolta sia agli enti locali che agli Stati membri, insiste sulla necessità di implementare pratiche inclusive per evitare che l'adozione dell'IA aggravi il divario digitale. Tra le azioni suggerite vi sono la predisposizione di guide online chiare e accessibili, l'organizzazione di percorsi di formazione specifici per i gruppi più vulnerabili della popolazione e la garanzia di accesso a strumenti digitali a prezzi accessibili.
In sintesi, le raccomandazioni delineano per le amministrazioni locali un ruolo non da semplici utilizzatrici di tecnologia, ma da attori strategici con la responsabilità di plasmare un'adozione dell'IA che sia organizzativamente solida, socialmente legittimata e fondamentalmente equa.

4.3 Prospettive europee e nazionali: modelli a confronto

L'analisi dei casi europei più avanzati rivela l'emergere di archetipi strategici distinti. Invece di un approccio unico, le regioni di successo stanno adottando modelli diversi a seconda dei loro obiettivi, del contesto e della maturità del loro ecosistema. La prima e forse più sofisticata strategia identificata è quella della Regione come "abilitatore" di ecosistemi: un modello in cui l'ente pubblico non si limita a essere un consumatore o uno sviluppatore di tecnologia, ma agisce a un livello superiore, creando le condizioni di contesto – legali, organizzative, etiche e tecniche – affinché l'innovazione possa prosperare in modo diffuso e sostenibile. I casi seguenti illustrano diverse sfaccettature di questo approccio.

4.3.1 Modello 1: la Regione come "abilitatore" di ecosistemi

Caso di studio: Baden-Württemberg (Germania) – Il "Living Lab" sanitario

- **Contesto e biettivo strategico**: il Land del Baden-Württemberg, una delle aree economicamente più forti d'Europa, si è posto l'obiettivo di accelerare l'adozione dell'IA nel settore sanitario, un ambito caratterizzato da alta regolamentazione e cicli di innovazione lenti. La sfida principale identificata non era la mancanza di soluzioni tecnologiche, ma la difficoltà per le imprese (in particolare le PMI e le startup) di testare, validare e certificare i propri algoritmi in un ambiente reale, a causa dei rigidi vincoli su privacy e sicurezza dei dati (GDPR) e delle future normative sull'IA (AI Act). L'obiettivo strategico della Regione è stato quindi quello di agire come "de-risker", creando un ponte tra il sistema sanitario pubblico e il tessuto innovativo privato(KI-Reallabor, 2025).
- **La soluzione: il progetto ROUTINE**: la Regione, attraverso il suo Ministero degli Affari Sociali, della Salute e dell'Integrazione, ha lanciato il progetto ROUTINE. Non si tratta di un'applicazione di IA, ma di un "laboratorio di dati reali" (Real-World Data Lab). In sostanza, è un ambiente di sperimentazione controllato, un sandbox normativo e tecnico, dove le aziende possono accedere a dati sanitari anonimizzati e di alta qualità per addestrare e validare i loro modelli di IA. Il progetto, gestito in collaborazione con un consorzio di ospedali universitari e centri di ricerca, garantisce che l'intero processo di sviluppo sia conforme ex-ante alle

normative vigenti. L'ente pubblico non compra un prodotto finito, ma offre un servizio cruciale: l'accesso sicuro ai dati e la validazione clinica.

- **Lezioni per le Policy**: il modello del Baden-Württemberg è un buon esempio di **innovazione pre-appalt**o. Invece di definire un capitolato rigido per una soluzione specifica, la Regione investe nella creazione di un'infrastruttura che stimola il mercato a produrre soluzioni migliori e più sicure. Questo approccio riduce il rischio per le imprese, che possono sviluppare prodotti già conformi alle regole del settore pubblico, e per l'amministrazione, che può valutare l'efficacia delle soluzioni in un ambiente controllato prima di procedere a un acquisto su larga scala. È un modello che trasforma la PA da semplice acquirente a partner dell'innovazione.

Caso di studio: Galizia (Spagna) – Il modello "Governance-First"

- **Contesto e obiettivo strategico**: la regione autonoma della Galizia ha adottato un approccio pionieristico, decidendo di affrontare la sfida dell'IA partendo dalle fondamenta: le regole. Consapevole che l'incertezza normativa rappresenta uno dei maggiori freni all'adozione dell'IA, sia per gli attori pubblici che per quelli privati, la Xunta de Galicia si è posta l'obiettivo di creare un quadro di certezza giuridica ed etica prima ancora di avviare un'adozione massiccia della tecnologia. La strategia è stata quella di utilizzare la leva normativa non come un limite, ma come un vantaggio competitivo per attrarre investimenti e posizionare la regione come un hub europeo per l'IA affidabile (trustworthy AI) (Xunta de Galicia, 2025a, 2025b).
- **La soluzione: la legge regionale sull'IA**: il 25 marzo 2025, il parlamento della Galizia ha approvato la Legge 2/2025, del 2 aprile, per lo sviluppo e l'impulso dell'intelligenza artificiale in Galizia, una delle prime normative di questo tipo a livello regionale in Europa. La legge non si sovrappone all'AI Act europeo ma ne adatta e sviluppa i principi nel contesto locale. La legge istituisce un Registro Regionale delle Iniziative di IA, promuove la creazione di sandbox regolatorie locali e definisce principi etici chiari per l'uso dell'IA nel settore pubblico galiziano. Vengono create due figure specifiche, l'Ufficio di intelligenza artificiale, con compiti di coordinamento e supervisione, e il Commissario per l'intelligenza artificiale, con il ruolo di vigilare sul rispetto dei principi etici. Queste strutture regionali sono distinte dall'Agenzia Spagnola di Supervisione dell'Intelligenza Artificiale (AESIA), l'autorità di vigilanza nazionale che, sebbene abbia sede proprio in Galizia (A Coruña), opera a livello statale. La strategia è inoltre supportata da un piano di investimenti da 330 milioni di euro e dalla creazione di un'Agenzia per la Supervisione dell'IA, anticipando di fatto le strutture di governance richieste a livello nazionale dall'AI Act.
- **Lezioni per le policy**: il caso della Galizia mostra quanto la governance non sia un corollario, ma un prerequisito per un'innovazione di successo. Un approccio "Governance-First" permette di ridurre l'incertezza per tutti gli attori dell'ecosistema, di guidare gli investimenti pubblici e privati verso soluzioni etiche e conformi e di costruire un rapporto di fiducia con i cittadini. Per una regione, dotarsi di un quadro normativo chiaro e di strutture di governance dedicate significa creare un asset strategico in grado di differenziarla a livello europeo, trasformando un obbligo normativo in un'opportunità di sviluppo.

Caso di studio: Catalogna (Spagna) – L'approccio "Ecosystem-Builder"

- **Contesto e obiettivo strategico**: La Catalogna, una regione con un forte tessuto industriale e di ricerca, ha interpretato l'IA non come una singola tecnologia da applicare, ma come un

nuovo paradigma che richiede un intervento sistemico. L'obiettivo strategico del governo catalano non è stato quello di sviluppare una specifica applicazione "killer", ma di costruire un ecosistema completo e autosufficiente, in grado di supportare l'intera catena del valore dell'IA: dalla ricerca di base al trasferimento tecnologico, fino all'adozione da parte delle imprese e della pubblica amministrazione, garantendo al contempo un solido presidio etico (Juncà, 2024; AIRA, 2025; CIDAI, 2025; OEIAC, 2025).

- **La soluzione**: la strategia CATALONIA.AI e le sue Istituzioni: La risposta della Catalogna è stata la creazione di una strategia olistica, denominata CATALONIA.AI. Il cuore di questa strategia non è un progetto, ma la fondazione di un insieme di organizzazioni permanenti e specializzate, ciascuna con una missione specifica. Tra queste spiccano l'AIRA (Artificial Intelligence Research Alliance), che coordina e potenzia la ricerca scientifica sull'IA; il CIDAI (Centre of Innovation for Data Tech and Artificial Intelligence), che agisce come un hub per il trasferimento tecnologico, connettendo la ricerca con le esigenze delle imprese e della PA; e l'OEIAC (Observatory of Ethics in Artificial Intelligence of Catalonia), un ente indipendente dedicato alla supervisione etica.
- **Lezioni per le Policy**: Il modello catalano è un esempio di "state-building" istituzionale applicato all'innovazione. Mostra che per governare una trasformazione così profonda come quella dell'IA, non basta finanziare progetti a termine. È necessario creare istituzioni stabili, competenti e specializzate che possano agire come punti di riferimento permanenti per l'intero ecosistema. Questo approccio garantisce continuità, accumula conoscenza nel tempo e crea un ambiente in cui le diverse componenti (ricerca, imprese, PA, società civile) possono dialogare e collaborare in modo strutturato. Per un'amministrazione regionale, questo significa investire non solo in tecnologia, ma soprattutto in capitale organizzativo e istituzionale.

4.3.2 Modello 2: la regione come "partner strategico"

Caso di studio: Île-de-France (Francia) – il modello "anchor institution"

- **Contesto e obiettivo strategico**: l'AP-HP (Assistance Publique - Hôpitaux de Paris) è uno dei più grandi sistemi ospedalieri universitari d'Europa e gestisce 38 ospedali nella regione dell'Île-de-France. Questa scala dimensionale, unita a un'enorme quantità di dati clinici e a un’alta concentrazione di competenze mediche, rappresenta un asset strategico unico. L'obiettivo dell'AP-HP non era semplicemente acquistare una soluzione di IA per la radiologia, ma sfruttare la propria posizione per catalizzare lo sviluppo di una tecnologia francese di livello mondiale, in grado di risolvere un problema concreto: l'aumento del carico di lavoro dei radiologi e il rischio di errori diagnostici (AP-HP, 2025).
- **La soluzione: la partnership tra AP-HP e GLEAMER**: invece di pubblicare una gara d'appalto tradizionale, l'AP-HP ha agito come una "istituzione di riferimento" (anchor institution) per GLEAMER, una startup parigina specializzata in IA per l'imaging medico. L'AP-HP ha fornito a GLEAMER un accesso regolamentato e sicuro ai propri archivi di dati anonimizzati, essenziali per addestrare e validare l'algoritmo ChestView, progettato per rilevare anomalie nelle radiografie del torace. Inoltre, i radiologi dell'AP-HP hanno collaborato con la startup per

testare e perfezionare la soluzione, garantendone l'affidabilità clinica. Una volta validato, il sistema è stato adottato dall'AP-HP stessa.

- **Lezioni per le policy**: il caso dell'Île-de-France dimostra come un grande ente pubblico possa utilizzare i propri asset non solo per erogare servizi, ma per plasmare attivamente il mercato dell'innovazione. Agendo come partner e primo cliente di una startup locale, l'AP-HP ha ottenuto un triplice risultato: ha acquisito una tecnologia all'avanguardia per migliorare i propri servizi, ha contribuito a creare un campione nazionale nel settore dell'IA medicale (GLEAMER è oggi uno dei leader di mercato) e ha generato un ritorno economico per il proprio territorio. Questo modello richiede una visione strategica del procurement, che possa andare oltre la logica del mero acquisto al prezzo più basso per abbracciare quella dell'investimento nell'ecosistema locale.

Caso di studio: Regione Capitale della Danimarca – il "partecipante a consorzio di ricerca"

- **Contesto e obiettivo strategico**: la Regione Capitale della Danimarca, che include Copenaghen, è una delle aree più digitalmente avanzate d'Europa, con un sistema sanitario completamente digitalizzato e registri di dati longitudinali di altissima qualità. La regione affronta una sfida sanitaria rilevante: la gestione del diabete di tipo 2. L'obiettivo strategico non era sviluppare una soluzione in autonomia, ma sfruttare la propria maturità digitale e la qualità dei propri dati per attrarre finanziamenti e competenze di livello europeo, inserendosi in un progetto di ricerca collaborativa per affrontare il problema in modo innovativo (CORDIS, 2025).
- **La soluzione: il progetto MELISSA (Horizon Europe)**: la regione non ha agito da sola, ma è diventata un partner chiave del progetto MELISSA, finanziato dal programma quadro di ricerca e innovazione dell'Unione Europea, Horizon Europe. All'interno di questo consorzio, che include università, centri di ricerca e aziende da tutta Europa, la regione danese svolge il ruolo di "terreno di prova clinico". Utilizzando i propri dati sanitari anonimizzati, contribuisce allo sviluppo di modelli di IA per la medicina personalizzata nel trattamento del diabete. I modelli sviluppati dal consorzio vengono poi testati e validati nel contesto reale del sistema sanitario regionale.
- **Lezioni per le policy**: il caso dimostra come una regione, anche di dimensioni contenute, possa giocare un ruolo da protagonista nell'innovazione europea se possiede asset strategici di alta qualità, come i dati. Partecipare a grandi consorzi di ricerca europei permette di raggiungere diversi obiettivi: importare innovazione e finanziamenti esterni, evitando di sostenere interamente i costi di sviluppo; accedere a competenze scientifiche di eccellenza a livello internazionale; sviluppare soluzioni all'avanguardia che sono direttamente applicabili e validate per i bisogni specifici del proprio territorio. Per una regione, investire nella qualità e nell'accessibilità dei propri dati (nel rispetto della privacy) è un prerequisito fondamentale per poter partecipare con successo a queste reti di innovazione aperta.

4.3.3 Modello 3: la regione come "sviluppatore diretto" di piattaforme sovrane

Caso di studio: Emilia-Romagna (Italia) – il "policy simulator"

- **Contesto e obiettivo strategico**: la regione Emilia-Romagna ospita il Tecnopolo di Bologna, una delle più grandi concentrazioni di supercomputer in Europa. Questa infrastruttura pubblica di calcolo ad alte prestazioni (HPC) costituisce un asset strategico unico. L'obiettivo

della regione non era semplicemente quello di ottimizzare un servizio esistente, ma di sfruttare questa immensa capacità di calcolo per portare la governance a un livello superiore: passare da una logica reattiva a una predittiva, simulando ex-ante gli impatti delle politiche pubbliche per renderle più efficaci e mirate.

- **La soluzione: il gemello digitale Amartya**: la regione ha promosso lo sviluppo di Amartya, un gemello digitale (digital twin) dell'intero tessuto socio-economico regionale. A differenza di altri gemelli digitali focalizzati su infrastrutture fisiche, Amartya integra dati eterogenei (demografici, economici, sanitari, ambientali) per creare un modello virtuale dinamico della società regionale. Questa piattaforma permette ai policy maker di testare scenari "what-if": ad esempio, simulare gli effetti di un nuovo incentivo economico su diverse fasce della popolazione o l'impatto di una politica sanitaria su specifiche aree del territorio prima della sua implementazione.
- **Lezioni per le policy**: il caso dell'Emilia-Romagna rappresenta la frontiera dell'uso dell'IA nella governance. Insegna che, in presenza di asset strategici come le infrastrutture di supercalcolo, l'ambizione può spostarsi dalla semplice efficienza amministrativa alla simulazione strategica delle policy. Questo approccio trasforma l'IA in uno strumento di supporto alle decisioni (decision support system) di altissimo livello. La lezione chiave è che l'investimento in infrastrutture digitali pubbliche non solo migliora i servizi attuali, ma abilita capacità di governo completamente nuove, consentendo di anticipare i problemi e di progettare interventi pubblici con maggiore precisione.

Caso di studio: Baden-Württemberg (Germania) – lo "strumento sovrano open-source"

- **Contesto e obiettivo strategico**: come molte altre amministrazioni, il Land del Baden-Württemberg si è trovato di fronte alla necessità di aumentare l'efficienza dei processi interni, in particolare per compiti cognitivi ripetitivi. L'obiettivo strategico, però, non era semplicemente acquistare una licenza da un grande fornitore tecnologico esterno, ma sviluppare una soluzione che garantisse la piena sovranità sui dati e sulla tecnologia, evitando il rischio di lock-in e assicurando che i dati sensibili dell'amministrazione rimanessero sotto il controllo pubblico (Baden-Württemberg, 2025; F13, 2025).
- **La soluzione: l'assistente ia generativa "f13"**: il Land, attraverso la sua agenzia digitale IT-BW, ha sviluppato "F13", un assistente basato su IA generativa e modelli linguistici di grandi dimensioni (LLM). La piattaforma è progettata per funzionare interamente sui server del Land (on-premise), garantendo il massimo controllo sui dati, ed è stata addestrata specificamente per le esigenze del lavoro amministrativo. Offre funzionalità avanzate come la capacità di sintetizzare testi lunghi (leggi, pareri, report) e di supportare la redazione di bozze per diverse tipologie di documenti, dalle note interne alle delibere. Uno degli strumenti più potenti integrati è un assistente di ricerca che opera secondo il paradigma RAG (Retrieval-Augmented Generation): l'utente può caricare una base di conoscenza specifica, come un insieme di atti parlamentari, e interrogare il sistema per ottenere risposte precise basate esclusivamente su quel contenuto, complete di citazione delle fonti. A queste capacità si affianca una funzione di chat più generica. La scelta cruciale del progetto, tuttavia, è stata quella di renderlo interamente open-source. Il codice e i modelli sono stati rilasciati pubblicamente,

permettendo a qualsiasi altra amministrazione in Germania (e non solo) di adottarlo, modificarlo e contribuire al suo miglioramento.

- **Lezioni per le policy**: il caso "F13" è un manifesto della sovranità digitale. La lezione più importante è che quando un ente pubblico sviluppa una soluzione tecnologica, può scegliere di trasformarla in un "bene pubblico digitale". L'approccio open-source permette di mutualizzare i costi di sviluppo tra più amministrazioni, di accelerare il miglioramento del software grazie ai contributi della community e, soprattutto, di garantire il pieno controllo pubblico sulla tecnologia, un aspetto cruciale quando si trattano dati dei cittadini. Per una regione, investire in soluzioni open-source non è solo una scelta tecnica, ma una decisione politica che afferma il principio della sovranità e promuove un modello di innovazione collaborativo e trasparente.

4.4 La situazione italiana

4.4.1 La Strategia della Regione Toscana per l'IA, un modello integrato

La Regione Toscana si distingue nel panorama nazionale per aver affrontato il tema dell'intelligenza artificiale attraverso un ciclo di policy completo e strutturato, che va dalla normazione all'attuazione partecipata. Questo percorso ha avuto inizio con l'approvazione della Legge Regionale n. 57/2024, che all'articolo 8 ha fornito la base giuridica per una governance regionale dell'IA, incaricando la Giunta di definire le modalità operative per la sua adozione.

In attuazione di tale mandato, la Regione ha elaborato le "Indicazioni operative per l'adozione di soluzioni di Intelligenza Artificiale", un documento strategico che recepisce i principi dell'AI Act europeo e fornisce un quadro pratico per gli enti del territorio. A corredo di queste linee guida, è stato redatto un apposito allegato contenente esempi di possibili implementazioni di soluzioni di IA, pensato per illustrare concretamente gli ambiti applicativi e le potenzialità della tecnologia. Coerentemente con un approccio aperto, le indicazioni operative sono state sottoposte a una consultazione pubblica sulla piattaforma Partecipa Toscana, permettendo di raccogliere contributi da cittadini, imprese e mondo accademico per costruire una strategia regionale antropocentrica ed etica. La Legge Regionale e gli allegati sono brevemente discussi nella parte successiva.

4.4.2 La Legge Regionale 57/2024 e i suoi allegati

A fondamento della governance dell'innovazione digitale in Toscana si pone la Legge Regionale n. 57 del 9 dicembre 2024 (Regione Toscana, 2024). Questa legge quadro stabilisce i principi e gli strumenti per guidare la trasformazione digitale dell'intero sistema pubblico regionale, che include la Regione stessa, gli enti locali, il servizio sanitario e le società controllate. L'obiettivo è creare un ecosistema digitale coordinato, inclusivo e sicuro, basato su principi di interoperabilità, qualità dei dati, promozione del software open-source e adozione di tecnologie cloud per evitare la dipendenza da specifici fornitori (lock-in tecnologico).

La legge non si limita a enunciare principi, ma definisce una precisa architettura di governance operativa. Istituisce il CSIRT Toscana per la gestione della cybersicurezza, in accordo con l'Agenzia per la Cybersicurezza Nazionale (ACN), e individua nel consorzio "in house" Metis il braccio operativo per supportare gli ambiti strategici dell'innovazione. Inoltre, formalizza la Rete Telematica Regionale Toscana (RTRT) come comunità di coordinamento per la transizione digitale degli enti locali.

Di particolare rilevanza per il tema dell'intelligenza artificiale, la legge identifica l'IA come un ambito strategico fondamentale. L'articolo 8 incarica esplicitamente la Regione di promuovere regole per la progettazione e l'utilizzo consapevole dei sistemi di IA, nel rispetto dei principi di etica, trasparenza, non discriminazione e protezione dei dati personali. Cruciale è anche l'introduzione delle Regulatory Sandboxes, ambienti controllati per la sperimentazione di tecnologie innovative come l'IA, offrendo così un quadro normativo che bilancia l'esigenza di innovare con quella di governare i rischi. Attraverso il consolidamento di norme precedenti e l'istituzione di un modello di governance chiaro, la legge mira a creare un quadro unificato per la trasformazione digitale del territorio.

In diretta attuazione del mandato conferito dalla Legge Regionale 57/2024, la Regione Toscana ha pubblicato nell'aprile 2025 le "Indicazioni operative per l'adozione di soluzioni di Intelligenza Artificiale" (Regione Toscana, 2025°). Questo documento traduce in pratica i principi della legge, fornendo agli enti del territorio una guida concreta per implementare sistemi di IA in modo sicuro, etico e conforme all'AI Act europeo. Il suo approccio è pragmatico e si fonda su un insieme di principi guida chiari: la centralità dell'essere umano (human-in-the-loop), la responsabilità, la non discriminazione, la trasparenza (tramite la Explainable AI) e la preferenza per soluzioni open source.

Il cuore del documento è un modello operativo basato sulla classificazione del rischio mutuata dall'AI Act. Le indicazioni guidano gli utilizzatori (deployer) a identificare il livello di rischio di un sistema di IA (proibito, alto, limitato o minimo) e, a seconda della categoria, prescrivono adempimenti specifici. Per supportare questo processo, il documento è corredato da una serie di strumenti pratici sotto forma di allegati, tra cui modelli per la classificazione del rischio, un modello dettagliato di Valutazione d'Impatto sui Diritti Fondamentali (FRIA) per i sistemi ad alto rischio e modelli semplificati di valutazione e documentazione per le altre categorie. In questo modo, la Regione non si limita a dettare regole, ma fornisce un vero e proprio toolkit per accompagnare le pubbliche amministrazioni toscane nel complesso percorso di adozione dell'IA, garantendo che l'innovazione tecnologica sia sempre allineata alla tutela dei diritti dei cittadini.

A completamento delle indicazioni operative, la Regione Toscana ha redatto un allegato tecnico (Regione Toscana, 2025b) che delinea le architetture e le strategie di implementazione per l'IA, offrendo un quadro pratico per passare dalla teoria alla pratica. Il documento distingue tra due principali ambiti di applicazione: da un lato, gli strumenti per la produttività individuale (es. sintesi di testi, analisi dati), per i quali la Regione sottolinea la necessità di un'attenta analisi dei termini d'uso e la creazione di un catalogo di software sicuri e approvati. Dall'altro, i fabbisogni più "evoluti" che integrano l'IA nei processi dell'ente (es. chatbot, classificazione documentale), per i quali si raccomanda di perseguire la sovranità sui dati e ridurre la dipendenza da specifici fornitori (vendor lock-in).

Per rispondere a queste esigenze complesse, la Regione sta sperimentando un'architettura basata sul framework open source Cheshire Cat, che implementa il modello RAG (Retrieval-Augmented Generation). Questo approccio è strategico perché permette di utilizzare modelli linguistici di grandi dimensioni (LLM) esterni mantenendo la base di conoscenza (i documenti e i dati sensibili dell'ente) al sicuro sulle proprie infrastrutture (on-premise). In questo modo, si risolve una delle principali criticità legate alla privacy e alla sicurezza.

Per ultimo, l'allegato analizza le diverse opzioni architetturali per sostenere la capacità computazionale richiesta dall'IA, confrontando soluzioni on-premise, full-cloud, SaaS e ibride. La soluzione raccomandata è un modello ibrido ottimale, che bilancia costi, sicurezza e performance: i dati e la

logica di controllo restano on-premise, mentre le operazioni più onerose, come l'inferenza dei modelli, vengono eseguite su istanze GPU in cloud. Questo approccio pragmatico dimostra una chiara strategia per adottare tecnologie avanzate in modo sostenibile e sicuro.

4.3.3 Prospettive e sfide nell'attuazione della strategia toscana

Fonte: Intervista con il Dott. Savio Picone (Segretario generale del consiglio regionale) e il Dott. Mauro Caliani (Responsabile di settore Informatica, archivio e protocollo, comunicazione web, urp), Consiglio Regionale della Toscana, 26/09/2025.

Dopo aver analizzato il quadro normativo e strategico definito dai documenti ufficiali, è fondamentale comprendere come questi indirizzi si traducano in azioni concrete. Per esplorare le sfide operative, le opportunità e la visione che guida l'attuazione sul campo, abbiamo dialogato direttamente con i protagonisti del percorso di innovazione della Regione.

Una visione di governance centralizzata per superare i silos

Il primo pilastro di questa riflessione strategica riguarda la necessità di una governance centralizzata. L'approccio all'IA viene inquadrato non come un tema meramente informatico, ma come un tema strategico trasversale che impatta l'economia, la sanità e i servizi al cittadino. La discussione parte da una criticità ben nota: il rischio della frammentazione. Lasciare la gestione dell'IA alle singole direzioni rischia di portare verso iniziative disallineate e a una dispersione di risorse. Per superare questi "silos" autonomi e non relazionati, la prospettiva suggerita è l'istituzione di un Dipartimento per l'IA in posizione di staff alla Presidenza o alla Direzione Generale. Sul modello di quanto fatto per la cybersecurity con l'Agenzia Nazionale, si avverte la necessità di un presidio unico e autorevole che definisca standard e strategie, garantendo un allineamento gerarchico con le emergenti strutture nazionali ed europee.

Il change management e l'alfabetizzazione sull'IA

Questa visione istituzionale si poggia su un pilastro umano e culturale. L'esperienza toscana insegna che l'adozione dell'IA è prima di tutto un'operazione di change management. L'obiettivo non è formare il personale sull'uso di un software, ma accompagnarlo verso un nuovo modo di concepire il lavoro. Un pilastro irrinunciabile di questo processo è l'alfabetizzazione sull'IA (AI Literacy), ovvero la consapevolezza di base dello strumento, del suo funzionamento e dei suoi limiti. Per superare resistenze e timori, l'IA viene presentata come un "collega esperto": uno strumento che potenzia le capacità individuali, facendosi carico dei compiti ripetitivi per liberare energie umane. Questa filosofia si traduce in una strategia formativa basata sul mentoring diffuso, identificando "pionieri" in ogni ufficio che mostrino ai colleghi i benefici concreti della tecnologia su casi reali.

Il valore pubblico come equità di accesso

Un terzo elemento fondante può rispondere a una domanda cruciale: qual è il fine ultimo dell'IA nel settore pubblico? La risposta della Regione Toscana è netta: il principale indicatore di successo è l'aumento dell'equità di accesso ai servizi. In questo ambito, la visione si è già tradotta in realizzazioni concrete. L'applicazione pratica di questo principio si è concretizzata nel progetto dell'URP Digitale multicanale del Consiglio (Matilde, Consiglio Regionale della Toscana, 2025). È stato sviluppato un assistente virtuale il cui motore è in grado di gestire in modo centralizzato le richieste di informazioni su bandi, avvisi e attività istituzionali. La stessa base di conoscenza alimenta diversi canali di accesso, pensati per platee eterogenee: dal portale web e social network come Telegram per l'utenza digitale, fino a un canale telefonico dedicato che, tramite tecnologie voice-to-text, permette anche ai cittadini

meno digitalizzati di interagire con l'assistente. Con un unico investimento, si dialoga con fasce di popolazione diverse, garantendo che nessuno resti escluso.

La Regione come "hub" di competenza per il territorio

La prospettiva emersa dalla discussione si estende inoltre a un futuro ruolo che la Regione possa ricoprire: quello di "hub" di competenza per il territorio. Riconoscendo che i piccoli Comuni non hanno le risorse per avviare autonomamente progetti di IA, correndo il rischio di finire “in balia” dei fornitori privati, si delinea un modello di sussidiarietà. In questa prospettiva, si potrebbe immaginare la creazione di un catalogo di servizi di IA centralizzati e "chiavi in mano". Utilizzando la metafora dei "mattoncini LEGO", la Regione potrebbe sviluppare soluzioni standard (come il succitato URP virtuale) che i Comuni possano adottare facilmente, promuovendo una digitalizzazione omogenea e permettendo anche agli enti più piccoli di accedere a tecnologie innovative. La Regione potrebbe inoltre svolgere una funzione di garanzia, andando a “bollinare” le soluzioni per certificare che non presentino rischi inaccettabili, dando così tranquillità agli amministratori locali.

Le sfide del contesto normativo e tecnologico

Questo approccio rischia di scontrarsi con le sfide del contesto esterno. Emergono due criticità rilevanti. La prima è il disallineamento tra la velocità dell'evoluzione tecnologica (che raddoppia le capacità ogni sei mesi) e i tempi della produzione normativa. Questa rapida evoluzione rischia, ad esempio, di rendere le linee guida, ad esempio quelle formulate in un'era pre-IA generativa, rapidamente obsolete, suggerendo la necessità di un "gruppo di lavoro continuo" per l'aggiornamento. La seconda, sul versante privacy, è la tendenza a un'interpretazione eccessivamente restrittiva della normativa privacy (GDPR) da parte dei DPO, che rischia di frenare la sperimentazione. Emerge quindi la necessità di un dialogo più stretto con i regolatori per ottenere “regole chiare” che siano al tempo stesso garanti dei diritti e abilitanti per l'innovazione.

Capitolo 5 - Le applicazioni dell'IA nell'amministrazione regionale

5.1 Introduzione

Oggi si assiste a una crescente interesse per le possibili applicazioni dell'IA di tipo generativo alle politiche pubbliche. L'IA può contribuire ad efficientare i processi della Pubblica amministrazione, automatizzando i controlli e le ispezioni, digitalizzando i dati e gli archivi, favorendo la gestione dei pagamenti e dei tributi, rilevando le frodi o le anomale solo per citarne alcuni. L'IA può anche supportare il policy maker nella programmazione delle politiche pubbliche, con lo sviluppo di sistemi predittivi in grado di simulare diversi scenari di intervento etc.
La pervasività delle applicazioni dell'IA e i potenziali rischi evidenziati dalla letteratura e ripresi dalla normativa europea e italiana richiedono che le PA si attrezzino per affrontare un cambiamento epocale che rischia di impattare su diritti fondamentali dei cittadini.
Regione Lombardia, anche sulla scorta della esperienza maturata con lo sviluppo della blockchain, ha avviato all'interno dell'Amministrazione regionale alcuni progetti per integrare l'intelligenza artificiale nei sistemi informativi regionali e al tempo stesso per sperimentare le tecnologie emergenti in ambiti di intervento predefiniti.
Con l'obiettivo di garantire il coordinamento delle iniziative relative all'utilizzo dell'intelligenza artificiale all'interno dell'amministrazione regionale è stato istituito un gruppo di lavoro interdirezionale composto da rappresentanti della Presidenza, (DC PNRR, Olimpiadi e Digitalizzazione, DC Affari istituzionali, generali e società, partecipate, DC Programmazione e Relazioni Esterne, UO Sistema dei controlli, prevenzione della corruzione e trasparenza, UO Audit fondi UE e responsabile, protezione dei dati) della DG Università Ricerca e Innovazione, della DG Welfare, della DG Trasporti e Mobilità sostenibile, ARIA e POLIS-Lombardia.
A questa iniziativa rivolta per lo più all'interno dell'Amministrazione regionale, si affianca l'iniziativa Lombard-IA che, attraverso la costituzione di un board di grandi esperti conosciuti a livello nazionale e internazionale sui temi dell'Intelligenza Artificiale, intende promuovere uno sviluppo e un utilizzo consapevole e sostenibile dell'IA nel mondo della ricerca e delle imprese.
Il capitolo presenta le più significative sperimentazioni di Intelligenza artificiale in Regione Lombardia. Si tratta di un resoconto, costruito a partire da interviste e incontri con alcuni referenti per la digitalizzazione di Regione Lombardia e del sistema regionale[13], che non ha la pretesa di esaurire la ricchezza delle iniziative in atto all'interno del sistema regionale, ma viene fatta soprattutto allo scopo di chiarire quali sono le sfide che la Pubbliche amministrazioni devono affrontare quando decidono di integrare questi strumenti all'interno delle loro procedure, soprattutto in quei settori che la normativa

[13] In particolare si desidera ringraziare per il supporto: il Responsabile Divisione Funzionamento della PA, Semplificazione e Digitalizzazione Servizi per la Pubblica Amministrazione di ARIA S.p.A.**;** il CEO di Camelot biomedical systems S.r.l., la funzionaria alle Politiche e Strategie di Trasformazione digitale e di Semplificazione della Pubblica Amministrazione presso la UO Trasformazione digitale per la modernizzazione e la semplificazione della DC PNRR, Olimpiadi e digitalizzazione; il Referente inventario delle emissioni di inquinanti atmosferici e gas climalteranti ARPA Lombardia -U.O. Aria e Supporto Political Decision Maker; il responsabile e la referente della UO Sistemi informativi e sanità digitale della DG Welfare.

europea considera ad alto rischio. Il trattamento dei dati personali (rispetto privacy) e il potenziale rischio per i diritti fondamentali delle persone fisiche sono i limiti principali entro cui si muovono le sperimentazioni in corso in Regione Lombardia.

5.2 Le sperimentazioni dell'IA all'interno dell'Amministrazione regionale

All'interno dell'amministrazione regionale lo sviluppo di progetti che adottano tecnologie di IA è curata da ARIA che ha deciso di coniugare e bilanciare, da un lato, la centralizzazione strategica nella scelta degli strumenti abilitanti e delle soluzioni più efficaci e, dall'altro lato, un approccio di forte «personalizzazione» operativa, coinvolgendo tutte le Direzioni Generali responsabili dei servizi erogati o dei processi da ottimizzare.
L'approccio di ARIA all'IA si basa su alcuni pilastri fondamentali che anticipano alcuni dei principi enunciati nella legge 132/2025. Innanzitutto è stato adottata una visione antropocentrica dell'Intelligenza artificiale. Tutti i modelli di intelligenza artificiale non sono concepiti per sostituire le competenze e le decisioni dell'operatore umano, bensì per supportarne l'attività, semplificando e velocizzando le fasi operative a basso valore aggiunto. La decisione finale resta sempre di competenza dell'essere umano (human in the loop), che mantiene il controllo sul processo e sul risultato. L'IA rappresenta dunque uno strumento di ausilio e potenziamento delle capacità decisionali, non un sostituto dell'intervento umano.
Un altro principio che contraddistingue la strategia regionale è quella della verifica di conformità delle sperimentazioni ai requisiti previsti dall'IA Act e dalla legge nazionale. Uno dei principali ambiti di attenzione riguarda la tutela della privacy e la gestione dei dati personali e sensibili, la cui analisi automatizzata deve essere rigorosamente conforme ai principi costituzionali nazionali e ai regolamenti europei in materia di protezione dei dati. Nella valutazione dei progetti di Intelligenza artificiale viene prestata attenzione anche agli impatti delle tecnologie di IA sui diritti fondamentali dei cittadini. Infatti algoritmi non adeguatamente addestrati o monitorati possono introdurre bias e distorsioni nei processi decisionali, generando disparità di trattamento o discriminazioni involontarie.
Considerato che la PA opera nel rispetto dei principi di equità, imparzialità e giustizia sociale, diventa fondamentale garantire la trasparenza dei modelli e la tracciabilità dei processi decisionali automatizzati, principi ribaditi anche nelle Linee guida in approvazione da parte di AGID.
Allo stesso tempo ARIA svolte un'importante attività di scouting e monitoraggio del mercato delle soluzioni tecnologiche di IA per la pubblica amministrazione. Si tratta infatti di un mercato in rapida evoluzione, dove i prodotti esistenti tendono a invecchiare velocemente grazie all'arrivo di nuovi modelli più accurati che possono contare su migliore capacità linguistica e efficienza computazionale.

Ad oggi si contano 22 progetti di IA nell'amministrazione regionale con diversi stadi di sviluppo. Il panorama delle soluzioni proposte abbraccia soprattutto i processi interni nell'ottica di ridurre i tempi delle istruttorie, automatizzare le fasi a basso valore aggiunto e ridurre i costi della macchina amministrativa. Tuttavia, sarebbe riduttivo pensare che il ricorso all'IA serva esclusivamente ad automatizzare le procedure interne. In realtà queste tecnologie richiedono spesso un ripensamento dei processi esistenti e devono essere accompagnati da cambiamenti organizzativi.

Progetti in fase di sviluppo maturo in procinto di rilascio:

1. Automazione dell'incrocio tra domanda (curriculum vitae) e offerta di lavoro (job vacancy): progetto IDO
2. Supporto all'analisi di contratti passivi (test interno ad ARIA)
3. Smart chat a supporto degli utenti esperti di normativa in ambito energetico
4. Assistente Virtuale per il supporto all'uso della piattaforma EDMA
5. Valutazione e proposta di risposta per le mail inviate dai cittadini alla casella di posta per il bando Dote Scuola
6. Sistema di supporto agli operatori sanitari in tema di farmaceutica convenzionata
7. Strumenti di ricerca avanzata e analisi automatica per il prezzario dei lavori pubblici
8. Assistenti virtuali avanzati, per ampliare la capacità dei canali CRM Regionali
9. Clinical Decision Support System

Progetti in fase di sviluppo prototipale sperimentato in campo:

1. Creazione di dati sintetici in ambito healthcare per minimizzare il rischio di identificazione diretta degli individui
2. Traduttore per comunicazioni in materia di Protezione Civile
3. Sympton checker per il cittadino
4. AI generativa a supporto delle valutazioni istruttorie per i fondi FESR e FSE
5. Automazione a supporto dei controlli desk associati ai bandi e ai procedimenti
6. AI per la Gestione e Pubblicazione Sicura dei Documenti, a valle dell'anonimizzazione automatica
7. Gemello Digitale Lombardo: use case Turismo
8. AI generativa per la vigilanza sanitaria – progetto SIAN

Progetti in fase di progettazione preliminari e analisi:

1. Nuova Digital Experience per i Servizi del Lavoro
2. Supporto all'Imaging e alla Telemedicina
3. Controlli fatture/importi cross-domanda e confronto fatture conto terzi a supporto dell'attività di controllo svolta da DGA e OPR
4. REG4AI-DEFAI- dati ed ecosistemi federati per applicazioni all'Ambiente e alla Mobilità
5. Algoritmi di AI generativa per l'associazione degli Atti alle azioni per il monitoraggio e la valutazione dei programmi PRSS.

Di alcuni di questi progetti viene presentata una breve descrizione

Incontro domanda e offerta di lavoro (IDO)

Tra i progetti, assume particolare rilievo **IDO**, un sistema avanzato di *matching* tra domanda e offerta di lavoro, che utilizza algoritmi di intelligenza artificiale per migliorare l'efficienza dei processi di intermediazione lavorativa.

Il motore di IA di IDO analizza le caratteristiche dei curricula dei candidati confrontandole con le posizioni lavorative pubblicate dalle imprese e individuando le corrispondenze più pertinenti in modo rapido, accurato e trasparente.
Questo approccio consente di ridurre i tempi di ricerca, migliorare la qualità degli abbinamenti e sostenere in modo concreto le politiche attive del lavoro. Il sistema IDO è in fase di test e una volta superata la fase di valutazione della compatibilità con la normativa (Ai ACT) verrà essere messo a disposizione dei centri per l'impiego. Si tratta di un'applicazione che lavora in un settore ad alto rischio secondo la normativa comunitaria perché oltre a trattare dati personali, potrebbe potenzialmente discriminare i diritti delle persone. IDO ordina infatti i CV in base alla pertinenza dell'offerta di lavoro dando un punteggio ranking ai diversi curricula, proponendo questo ranking all'operatore del centro per l'impiego che potrebbe avvalersi di questa valutazione di matching per facilitare l'incontro di domanda e offerta di lavoro.
IDO risponde a una esigenza dei Centri per l'impiego di disporre di strumenti che consentano di efficientare la parte di scrematura dei curricula sulle selezioni aperte, riducendo il lavoro degli operatori e quindi anche i tempi per l'erogazione dei servizi di collocamento.

IA generativa a supporto delle valutazioni istruttorie per i fondi FESR e FSE

Questo progetto riguarda applicazioni dell'IA nella fase di istruttoria dei bandi. Nella fase di ammissione del bando, è stato fatto uno studio preliminare dove si è valutato come i modelli di IA possano fornire un supporto nell'analisi dei progetti. Vengono effettuate scremature automatiche sui requisiti preliminari e poi estratte informazioni puntuali e quantitative legate ai requisiti di merito per facilitare la valutazione da parte del nucleo di valutazione. Nella seconda fase del bando, ovvero la fase di esecuzione, è stato condotto uno studio per supportare gli operatori nelle verifiche su Timesheet e fatture tramite l'estrazione di dati da documenti scansionati e un controllo automatico basato su requisiti specifici. È stato scelto di focalizzarsi sulla fattibilità tecnica della soluzione utilizzando per il test campioni fittizi e non reali.
La Sperimentazione ha permesso di verificare l'efficacia tecnica del sistema IA (OCR+CONTROLLI AUTOMATICI), testandone la funzionalità e la capacità di ottimizzare i processi di controllo. Questa fase di sperimentazione ha prodotto risultati incoraggianti sull'efficienza del sistema e ipotesi di miglioramento del sistema e del processo di controllo.
I punti di forza del progetto sono l'efficienza:
Efficienza interna: IA e automazione supportano i funzionari, che possono lavorare con maggiore precisione.
Efficienza esterna: I beneficiari ottengono vantaggi da processi più rapidi e semplificati (in linea con le indicazioni previste dal Reg. 1060/2021), con un effetto volano sul tessuto socioeconomico grazie ad un più rapido rientro degli investimenti da parte dei beneficiari che hanno investito nelle innovazioni.

Il passaggio da dati non strutturati a dati strutturati, permette la semplificazione dei processi – come richiesto dalla Commissione – riducendo gli errori e rendendo possibile non solo velocizzare i controlli ma anche avere dati quantitativi per valutazioni e report. Inoltre la soluzione può essere applicabile su scala regionale e potenzialmente su scala nazionale (si segnala infatti un interesse da parte del

DPCOE/Presidenza CdM in merito allo sviluppo del progetto), contribuendo al riuso delle esperienze maturate.

Automazione a supporto dei controlli desk associati ai bandi e ai procedimenti

Per questo progetto è stata realizzata una sperimentazione tecnico-funzionale finalizzata a valutare la fattibilità dell'automatizzazione dei controlli incrociati tra i dati registrati nel sistema Bandi e Servizi e le informazioni contenute in timesheet e fatture elettroniche.
L'obiettivo della sperimentazione è stato quello di testare il modulo di controllo automatizzato, escludendo, in questa fase, l'integrazione diretta con il sistema BES.
Il nucleo funzionale del modulo è rappresentato dal motore di elaborazione dei timesheet, basato sulla conversione dei documenti PDF in formato strutturato tramite tecniche di riconoscimento ottico dei caratteri (OCR).
Per ottimizzare l'accuratezza del processo di conversione, la sperimentazione ha fatto leva sulla struttura fissa del template dei timesheet, caratterizzato da sezioni predefinite e titoli standardizzati, che facilitano l'estrazione e la mappatura dei dati.
Successivamente alla fase di strutturazione dei contenuti, il sistema esegue una serie di controlli logici e di coerenza sui dati acquisiti, finalizzati a validare la correttezza delle informazioni e a individuare eventuali anomalie o discrepanze.
La sperimentazione ha coinvolto la generazione di timesheet fittizi aderenti alla struttura del template per testare le performance:
• Dei modelli OCR, per valutare la capacità dei modelli di IA di leggere il testo
• Del modulo dei controlli, per valutare l'efficacia del sistema
La sperimentazione costituisce un passo preliminare verso la piena integrazione automatizzata dei processi di monitoraggio e controllo, con potenziali benefici in termini di riduzione del carico manuale, incremento dell'affidabilità dei dati e tracciabilità delle verifiche.

ACTAFARMA

Actafarma è una piattaforma basata su tecnologie di Intelligenza Artificiale progettata per automatizzare i processi di raccolta, classificazione e consultazione della normativa sanitaria regionale, con particolare riferimento agli ambiti farmaceutico, protesico e di assistenza integrativa.
Il sistema integra in modo nativo i flussi informativi EDMA, organizza la documentazione normativa per dominio tematico e consente interrogazioni in linguaggio naturale, garantendo la tracciabilità puntuale delle fonti attraverso un approccio RAG (Retrieval-Augmented Generation).
Gli enti destinatari e utilizzatori principali della piattaforma sono: ATS (Agenzie di Tutela della Salute) ASST (Aziende Socio-Sanitarie Territoriali) DG Welfare (Direzione Generale Welfare).
Gli obiettivi principali del progetto sono: automatizzare la raccolta, la classificazione e l'aggiornamento continuo della normativa sanitaria regionale che risulta particolarmente complessa; Organizzare e arricchire i contenuti mediante processi di normalizzazione e tagging semantico, attribuzione di metadati strutturati, clusterizzazione semantica dei documenti, sintesi automatica dei

contenutiAbilitare una consultazione intelligente attraverso modelli linguistici di grandi dimensioni (LLM) con retrieval controllato e citazioni puntuali delle fonti.
I benefici strategici associati a questo progetto sono:
Decision making accelerato: disponibilità di sintesi automatizzate e ricerca semantica avanzata.
Riduzione del rischio interpretativo: garanzia di trasparenza e verificabilità tramite citazioni automatiche e controllo editoriale.
Scalabilità di dominio: architettura modulare e riusabile per ulteriori ambiti normativi.
Single Source of Truth: realizzazione di un repository unificato, coerente e condiviso, a supporto della governance informativa del sistema sanitario.

Reg4ia

Il progetto Reg4IA – Regioni per l'Intelligenza Artificiale nasce con l'obiettivo di sviluppare un algoritmo basato su modelli predittivi a supporto delle amministrazioni regionali italiane. L'iniziativa mira a realizzare uno strumento in grado di prevedere e prevenire problematiche legate al suolo regionale, con particolare attenzione alle condizioni ambientali estreme e agli aspetti energetici. L'idea di fondo è quella di mettere a disposizione delle regioni un modello replicabile e condiviso, capace di migliorare la capacità di risposta delle istituzioni a fenomeni complessi e di supportare le decisioni strategiche in ambito territoriale.
L'ambito principale di applicazione riguarda la mobilità e l'ambiente, due settori fortemente interconnessi e sensibili alle dinamiche climatiche e infrastrutturali. Dopo una fase di pianificazione e progettazione, il progetto ha recentemente avviato la fase operativa, iniziata da circa tre settimane al momento dell'intervista.
L'utilità attesa del progetto risiede nello sviluppo di un modello predittivo utilizzabile da tutte le regioni italiane, con lo scopo di migliorare le politiche di gestione del territorio e di prevenzione dei rischi ambientali. In prospettiva, il sistema potrebbe diventare un supporto decisionale avanzato per le amministrazioni pubbliche, favorendo una gestione più efficiente e informata delle risorse e delle emergenze.
Alla realizzazione del progetto partecipano diversi partner istituzionali e tecnici, tra cui la Regione Veneto (coinvolta al 50%), ARIA S.p.A., Veneto Innovazione, AgiD, i ministeri competenti, Cineca, CEFRIEL e il Politecnico di Milano. Questa rete di collaborazione interregionale e interistituzionale rappresenta uno degli elementi di forza dell'iniziativa, che punta sulla condivisione di conoscenze e competenze specialistiche.
Attualmente, non è ancora previsto un coinvolgimento diretto dei cittadini, poiché il progetto si concentra nella realizzazione di uno strumento destinato principalmente all'uso interno delle amministrazioni regionali.
Tra le principali criticità previste, viene segnalata la possibilità di incontrare difficoltà nella raccolta e analisi dei dati, trattandosi di un progetto sperimentale che implica la gestione di grandi quantità di informazioni e l'integrazione di fonti eterogenee. Anche l'individuazione di modelli efficaci e la loro calibrazione rappresentano una sfida significativa nella fase operativa.
Infine, l'esperienza di Regione Lombardia evidenzia come, per avviare progetti di intelligenza artificiale nella pubblica amministrazione, sia fondamentale definire con chiarezza gli obiettivi, assicurare la qualità dei dati e costruire solide partnership interistituzionali. L'approccio collaborativo e la

condivisione delle competenze tra enti territoriali emergono come fattori chiave di successo e replicabilità del progetto.

Il Digital twin

Anche Regione Lombardia ha avviato la sperimentazione per il Gemello digitale con l'obiettivo di dotarsi di un avanzato strumento di simulazione, analisi predittiva e supporto decisionale, capace di valutare l'impatto delle politiche pubbliche su uno scenario di medio lungo periodo. I modelli che verranno sviluppati nei prossimi cinque anni riguardano l'ambito turistico, con simulazioni di scenari di crescita qualitativa e quantitativa, sia dal punto di vista territoriale che stagionale; la valutazione dell'impatto delle politiche di sostegno ai cittadini e alle famiglie e le politiche per la qualità dell'aria.
La precondizione, come dimostra l'esperienza dell'Emilia Romagna, è la disponibilità di infrastrutture computazionali ad alte prestazioni e di dati con cui costruire le elaborazioni.
Si tratta di un progetto che dovrebbe soprattutto la fase di programmazione e valutazione ex ante delle politiche regionali, permettendo al decisore politiche si assumere decisioni data driven. Nel progetto di costruzione del gemello digitale sono coinvolti esperti del mondo accademico e delle singole Direzioni generali.

5.3 L'intelligenza artificiale in sanità

L'ambito sanitario è particolarmente ricco di progetti di IA. Lo si evince da un'indagine sull'intelligenza artificiale riguardante il monitoraggio dell'avanzamento delle applicazioni nel settore sanitario (Cappellaro et al, 2024). La raccolta dei dati è avvenuta tramite un'indagine che ha coinvolto le aziende sanitarie pubbliche e private lombarde incluse le agenzie di tutela della salute (ATS) e gli istituti di ricovero e cura a carattere scientifico (IRCCS).
L'indagine ha raccolto complessivamente 46 risposte (tra aziende sanitarie pubbliche e private) rappresentative di oltre il 70% del sistema sanitario regionale.
Dall'indagine sono emerse 56 applicazioni di IA distribuite in 20 organizzazioni adottanti (43% del campione), mentre il 57% delle strutture non aveva ancora implementato alcuna soluzione di IA. Le applicazioni identificate si concentrano principalmente su diagnosi e prognosi.
Il settore radiologico emerge come il più avanzato e consolidato in ambito IA, con circa un terzo delle applicazioni totali e una forte presenza di soluzioni marcate CE. Seguono oncologia e diabetologia, dove prevalgono sistemi predittivi o di supporto decisionale clinico ancora in fase di sviluppo o test. Anche discipline come la cardiologia e la neurologia riabilitativa iniziano a integrare strumenti di IA, soprattutto in centri di ricerca.
L'indagine evidenzia quelle che risultano essere le barriere per l'applicazione di Intelligenza Artificiale nel settore sanitario. La gestione dei dati e privacy viene percepita come la criticità maggiore tra gli sviluppatori poiché necessitano di dataset ampi e interoperabili per addestrare gli algoritmi. L'Interoperabilità dei sistemi informativi è un ostacolo tecnico significativo, in particolare per chi sviluppa internamente soluzioni. La carenza di competenze specialistiche risulta essere problema diffuso, indicato come principale barriera dai non adottanti. La cultura organizzativa e resistenza al cambiamento viene percepita come la barriera dominante tra gli acquirenti di soluzioni commerciali.

L'assenza di modelli di rimborso o incentivi economici è segnalata da tutti i gruppi come elemento inibente l'adozione sostenibile.
Le organizzazioni che già sviluppano IA mostrano preoccupazioni legate ad aspetti tecnici e regolatori, mentre quelle che acquistano soluzioni sono più sensibili a fattori culturali e di fiducia verso la tecnologia. Le strutture non adottanti, invece, evidenziano limiti di risorse umane e finanziarie.
Lo studio conferma che la sfida dell'IA non è tanto tecnologica, bensì organizzativa.
Questi approcci riflettono inevitabilmente scelte strategiche profondamente differenti, in parte influenzate dalla natura istituzionale delle singole aziende, con implicazioni sulle scelte organizzative interne e sulle modalità di relazione con gli altri attori dell'ecosistema. Lo sviluppo autonomo o congiunto richiede una vasta gamma di competenze e risorse ed è tipico degli istituti di ricerca.

Anche grazie agli stimoli offerti dall'indagine condotta sulle strutture sanitarie e nella consapevolezza del possibile impatto dell'IA nel settore sanitario, Regione Lombardia si è dotata di uno strumento il Piano Strategico di Sanità Digitale di Regione Lombardia con cui sta traducendo in pratica una visione chiara: usare la tecnologia per sostenere i professionisti, valorizzare il patrimonio informativo e offrire servizi migliori a cittadini e pazienti. È all'interno di questo Piano che si colloca l'integrazione dell'IA, che ruota attorno a una serie di obiettivi fondamentali: garantire ai professionisti strumenti in grado di supportarli nella definizione di percorsi di cura sempre più efficaci, offrire agli organismi decisori informazioni solide per la programmazione e la governance, mettere a disposizione dei ricercatori basi e strumenti per ampliare studi e ricadute cliniche e semplificare i processi amministrativi attraverso soluzioni innovative.
Va detto che il sistema sociosanitario lombardo ha raggiunto un livello di maturità digitale notevole, grazie agli investimenti già realizzati e in corso - quali la diffusione della Cartella Clinica Elettronica (CCE) Regionale, l'introduzione del Sistema Regionale per la Gestione Digitale del Territorio (SGDT) negli ambiti sociosanitari, il potenziamento del Fascicolo Sanitario Elettronico (FSE), la realizzazione dei Clinical Data Repository (CDR) aziendali - che consentono di disporre di una mole di dati significativa e utilizzabile.
In questo contesto di maturazione digitale, l'Intelligenza Artificiale diventa un pilastro per la modernizzazione della Pubblica Amministrazione, in coerenza con il Piano Triennale 2024–2026 per l'informatica nella PA. Regione Lombardia si colloca in questa traiettoria con un approccio pragmatico: integrare l'Intelligenza Artificiale dove crea valore misurabile, supportando l'efficacia ed efficienza del sistema ma garantendo allo stesso tempo trasparenza e sicurezza.
Il Piano Strategico individua tre macroaree di applicazione prioritaria dell'IA: il supporto alle decisioni cliniche, la valorizzazione dei Big Data provenienti dai CDR aziendali per programmazione, ricerca e presa in carico predittiva, e l'automazione dei processi amministrativi a livello aziendale e regionale. Regione si propone di sperimentare soluzioni e servizi basati sull'Intelligenza Artificiale in ambiti sociosanitari mirati, coinvolgendo attivamente numerosi professionisti per valutarne l'efficacia, l'affidabilità e l'utilità sia nella pratica clinica sia nei processi assistenziali, al fine di giungere a un modello operativo in cui l'Intelligenza Artificiale sia pienamente integrata nei processi, sostenuta da meccanismi di governance e miglioramento continuo, ponendo sempre la persona al centro e mantenendo una logica di servizio pubblico.
All'interno di questo scenario, i Clinical Decision Support Systems rappresentano la prima applicazione strategica dell'Intelligenza Artificiale. Con i CDSS ci si propone di potenziare la capacità degli operatori

sanitari di analizzare i dati, di valutare le alternative disponibili e individuare pattern che potrebbero sfuggire nella pratica quotidiana. Lo strumento si integra nei sistemi già in uso, offrendo suggerimenti, generando segnalazioni, aiutando nella definizione delle priorità e documentando le raccomandazioni fornite. Nel 2024, Regione Lombardia ha avviato una consultazione preliminare di mercato per esplorare le soluzioni CDSS esistenti, in ambiti di interesse preventivamente individuati. I risultati hanno restituito un quadro eterogeneo: alcune soluzioni risultano già ben sviluppate, altre sono ancora in fase di evoluzione, mentre il numero di prodotti certificati come dispositivi medici resta contenuto. Questo contesto ha dunque rafforzato la scelta della Regione di procedere con sperimentazioni mirate, condotte in modo controllato e nel pieno rispetto delle normative etiche e regolatorie, focalizzandosi su problematiche cliniche chiaramente definite.
L'avvio dei progetti CDSS segue una logica incrementale e pragmatica, calata nei contesti d'uso. In ambito imaging, ad esempio, l'IA può aiutare a rendere più rapida la lettura delle immagini, sostenendo il lavoro dei professionisti e semplificando i passaggi organizzativi: l'obiettivo è aumentare l'accuratezza degli esiti e ridurre i tempi di refertazione. Nel contesto dei servizi 116/117, l'utilizzo di strumenti di smart triage e symptom checker può ottimizzare l'instradamento delle chiamate e ridurre i tempi di risposta, offrendo un prezioso supporto agli operatori nella gestione efficace delle telefonate. Nei percorsi di cronicità e di appropriatezza prescrittiva, i CDSS, integrati con la cartella clinica e con gli applicativi dei medici di medicina generale, possono offrire suggerimenti coerenti con Percorso Diagnostico Terapeutico Assistenziale e linee guida, riducendo gli errori e sostenendo l'equità di accesso. In ambito ospedaliero, sistemi di allerta per la sepsi potrebbero aiutare a riconoscere più in fretta quadri clinici complessi e a intervenire tempestivamente, con benefici attesi sugli esiti e sull'uso delle risorse.
Ogni progetto di utilizzo dell'IA viene sottoposto a una valutazione ispirata all'Health Technology Assessment che considera efficacia clinica, impatto organizzativo, sostenibilità economica e accettazione professionale. La sicurezza del paziente resta infatti il perno delle sperimentazioni e in conformità alla normativa europea vengono osservate le tutele etiche e la protezione dei dati personali.
Solo le sperimentazioni che avranno superato il vaglio dell'efficacia e della sostenibilità saranno poi estese all'intero sistema socio sanitario.

5.4 L'intelligenza artificiale in ambito ambientale

Le simulazioni degli scenari emissivi sono importanti per il rispetto della Direttiva sulla qualità dell'Aria. In Arpa Lombardia sono in utilizzo da qualche anno algoritmi di Machine learning che consentono di superare la rigidità dei modelli deterministici, introducendo una capacità predittiva fondata sull'analisi di grandi moli di dati eterogenei [14] Tali strumenti permettono di individuare pattern non immediatamente osservabili con metodi convenzionali, integrare vincoli fisici e conoscenze di dominio preservando la coerenza con le leggi che governano i fenomeni atmosferici, ridurre i tempi di elaborazione degli inventari emissivi ed estendere stime locali a domini spaziali più ampi combinando dati ambientali con indicatori demografici, economici e territoriali.

[14] Marongiu A. Angiolino E (2024) Utilizzo di Tecniche di Intelligenza Artificiale per l'analisi di dei Dati Ambientali

Queste potenzialità si traducono in un impatto significativo sul piano operativo: l'IA non si limita a fornire stime più accurate, ma abilita un approccio dinamico e adattivo, capace di rispondere alla variabilità meteorologica e alle fluttuazioni delle attività antropiche.
Nonostante le potenzialità, l'applicazione dell'IA in questo ambito non è esente da criticità. In primo luogo, la qualità dei dati rappresenta un fattore determinante: dataset incompleti, non standardizzati possono compromettere l'affidabilità dei modelli. Inoltre, la complessità intrinseca di alcuni algoritmi introduce il rischio di opacità ("black box"), riducendo la trasparenza e la spiegabilità dei risultati, un aspetto cruciale per la legittimazione scientifica e istituzionale delle stime prodotte.
Un ulteriore elemento di attenzione riguarda la necessità di preservare i vincoli fisici: l'uso indiscriminato di tecniche di ML, privo di un ancoraggio ai principi della fisica atmosferica, può generare previsioni incoerenti con la realtà fenomenologica. Infine, la trasferibilità dei modelli addestrati in contesti specifici non è scontata e richiede procedure di calibrazione accurata, soprattutto in scenari caratterizzati da condizioni estreme o da assenza di dati empirici, come nel caso degli incendi.

Conclusioni

Il rapporto del Comitato europeo delle Regioni esordiva asserendo che In Europa, la maggior parte dei casi di utilizzazione di sistemi IA da parte di amministrazioni pubbliche si registra a livello nazionale, mentre sono meno diffuse le esperienze a livello locale e regionale. La resistenza degli enti territoriali all'impiego dell'AI è legata ad una molteplicità di cause (incapacità di sviluppare sistemi propri, assenza di personale in genere e di personale qualificato, vincoli normativi di carattere nazionale), e ciò rappresenta un forte limite alla diffusione di questa nuova modalità operativa nell'intero settore pubblico (Gardini, 2025).

In realtà, nell'ultimo anno si è assistito a una diffusione anche tra le pubbliche amministrazioni regionali e locali di sistemi di IA tanto che molte pubbliche amministrazioni sono in procinto di adottare soluzioni tecniche basate sull'IA. Del resto, le applicazioni dell'IA nella pubblica amministrazione sono foriere di potenziali vantaggi: l'aumento dell'efficienza nell'uso delle risorse, il supporto alle decisioni e il miglioramento dei servizi offerti ai cittadini.

A livello italiano, le Regioni si sono mosse fin da subito per adottare soluzioni di IA, smentendo almeno in parte quanto riportato nel rapporto del Comitato europeo delle Regioni. Nel corso del 2024, la Conferenza delle Regioni ha presentato una survey in cui si evidenziava come fosse stata già raggiunta una certa maturità e consapevolezza da parte di alcune amministrazioni regionali nell'adozione di sistemi di IA. Infatti, si contavano già 85 casi d'uso di IA tra le Regioni[15], evidenziando un impegno concreto nell'adozione dell'IA, con progetti in diverse fasi di sviluppo, dalla programmazione all'esercizio. La maggior parte di questi progetti si concentrava sul miglioramento dell'efficienza amministrativa tramite l'automazione dei processi interni e l'implementazione di chatbot/virtual assistant per il supporto agli utenti, sia interni che esterni. Secondo la Conferenza delle Regioni questo dimostrerebbe una chiara visione strategica da parte delle Regioni, che mirano a sfruttare l'IA per ottimizzare la pubblica amministrazione e renderla più efficiente e accessibile ai cittadini. Non mancano anche sperimentazioni innovative in alcuni settori come la sanità, l'ambiente, il turismo e la cybersecurity a dimostrazione della volontà da parte delle amministrazioni regionali di affrontare la sfida di migliorare la qualità dei servizi offerti ai cittadini in diversi ambiti.
Le Regioni insomma non sono state alla finestra e, come dimostrano i casi d'uso di IA adottati in Regione Lombardia, sono un cantiere prodromico alla diffusione su larga scala della IA nella pubblica amministrazione territoriale e locale.

Questo studio ha documentato come anche a livello europeo, l'ambito più immediato e meno rischioso di utilizzo dell'IA riguarda l'automazione dei processi interni alla Pubblica amministrazione, che può velocizzare le procedure burocratiche, riducendo tempi e costi, con l'eliminazione di attività ripetitive a basso valore aggiunto. L'adozione delle soluzioni basate sull'IA e soprattutto sull'IA di tipo generativo a campi quali l'erogazione di servizi agli utenti (servizi per l'occupazione, servizi sanitari, servizi

[15] Conferenza delle Regioni e delle Province autonome (2024) Esiti della rilevazione 2024 sui casi d'uso regionali di sperimentazione dell'intelligenza artificiale (ia);

assistenziali etc) deve infatti misurarsi con il rispetto della normativa (privacy e tutela dei diritti delle persone), e secondo l'analisi del rischio attorno a cui ruota il regolamento comunitario, porta le pubbliche amministrazioni ad adottare un comportamento prudente.
Non è un caso se nella ricognizione internazionale ristretta ai casi europei non si trovino casi di Intelligenza artificiale applicata ai settori critici, e lo stesso si può dire anche per la ricognizione effettuata a livello nazionale sulle amministrazioni centrali (AGID, 2025). Come evidenziato infatti nel rapporto AGID, emerge che il 95% dei progetti di Intelligenza Artificiale censiti nelle pubbliche amministrazioni non rientra nelle categorie ad alto rischio definite dall'AI Act. Solo una quota marginale riguarda attività che potrebbero comportare forme di profilazione automatica (4%) o avere impatti significativi sui diritti delle persone in ambiti sensibili, come il lavoro o l'istruzione (1%). Il dato confermerebbe una diffusa aderenza al principio di precauzione e una limitata esposizione della PA a scenari regolatori più stringenti.

Ciò vale anche per i casi d'uso dell'IA avviati da Regione Lombardia e dal SIREG. La maggior parte di queste sperimentazioni si concentra sui processi interni alle pubbliche amministrazioni, senza che ciò comporti quindi una valutazione di impatto per i diritti fondamentali. Le sperimentazioni nei settori ad alto rischio richiedono infatti un attento bilanciamento tra innovazione tecnologica, conformità normativa e tutela dei diritti fondamentali (Riccio, 2024). La realizzazione della valutazione di impatto è tra gli obblighi fondamentali per i deployer di sistemi di IA ad alto rischio e va realizzata prima dell'uso del sistema, al fine di individuare potenziali pregiudizi per i diritti fondamentali riconosciuti nell'Unione europea (Carta, 2024; Riccio, 2024). Sarà questo il banco di prova per l'IA generativa per la pubblica amministrazione anche regionale nei prossimi anni, soprattutto per dare gambe alle promettenti sperimentazioni in campo sanitario e del mercato del lavoro.

Il dinamismo delle Regioni è evidente anche sul fronte normativo. Alcune Regioni italiane si sono mosse, nelle more dell'approvazione della legge nazionale, approvando una legge sull'argomento.
È il caso della Regione Toscana, che come evidenziato nel paragrafo dedicato, ha approvato la l.r. 57/2024 Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009 e della Regione Puglia, che ha inserito alcuni riferimenti all'intelligenza artificiale in un testo di legge prevalentemente dedicato all'open innovation[16]. In altre Regioni sono allo studio disegni di legge[17].
Da un certo punto di vista, questo attivismo delle Regioni sul versante normativo, è una riprova di quanto affermato in letteratura. Le Regioni rappresentano «un fondamentale banco di prova per riforme e innovazioni giuridiche che, dopo una prima fase di sperimentazione, vengono successivamente introdotte su scala nazionale», e, pertanto, esse «potrebbero rappresentare la "sandbox normativa" ideale per lo sviluppo di sperimentazioni regolative sulle decisioni algoritmiche» (Gardini, 2025).

[16] LEGGE REGIONALE 14 aprile 2025, n. 4 "Misure di promozione in materia di innovazione aperta e intelligenza artificiale e disposizioni varie".
[17] Anche in Lombardia sono depositati due progetti di legge sull'intelligenza artificiale. In particolare, il PdL 2 *Disposizioni regionali in materia di intelligenza artificiale* e il PdL 3 *Regolamentazione utilizzo dell'intelligenza artificiale*

Le Regioni e le amministrazioni locali nel progressivo adattamento delle soluzioni di IA alla gestione dei servizi e all'efficientamento delle procedure amministrative devono tenere conto dei principi generali contenuti nel Piano triennale per l'informatica nelle Pubbliche amministrazioni che definiscono il perimetro delle indicazioni di policy in questo ambito:

1. Miglioramento dei servizi e riduzione dei costi. Le pubbliche amministrazioni concentrano l'investimento in tecnologie di intelligenza artificiale nell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo. Il conseguente recupero di risorse è destinato al miglioramento della qualità dei servizi anche mediante meccanismi di proattività.
2. Analisi del rischio. Le amministrazioni pubbliche analizzano i rischi associati all'impiego di sistemi di intelligenza artificiale per assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti. Le pubbliche amministrazioni adottano la classificazione dei sistemi di IA secondo le categorie di rischio definite dall'AI Act.
3. Trasparenza, responsabilità e informazione. Le pubbliche amministrazioni pongono particolare attenzione alla trasparenza e alla interpretabilità dei modelli di intelligenza artificiale al fine di garantire la responsabilità e rendere conto delle decisioni adottate con il supporto di tecnologie di intelligenza artificiale. Le amministrazioni pubbliche forniscono informazioni adeguate agli utenti al fine di consentire loro di prendere decisioni informate riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale.
4. Inclusività e accessibilità. Le pubbliche amministrazioni sono consapevoli delle responsabilità e delle implicazioni etiche associate all'uso delle tecnologie di intelligenza artificiale. Le pubbliche amministrazioni assicurano che le tecnologie utilizzate rispettino i principi di equità, trasparenza e non discriminazione.
5. Privacy e sicurezza. Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della privacy per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile. In particolare, le amministrazioni garantiscono la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
6. Formazione e sviluppo delle competenze. Le pubbliche amministrazioni investono nella formazione e nello sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi pubblici.
7. Standardizzazione. Le pubbliche amministrazioni tengono in considerazione, durante le fasi di sviluppo o acquisizione di soluzioni basate sull'intelligenza artificiale, le attività di normazione tecnica in corso a livello internazionale e a livello europeo da CEN e CENELEC con particolare riferimento ai requisiti definiti dall'AI Act.
8. Sostenibilità: Le pubbliche amministrazioni valutano attentamente gli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adottando soluzioni sostenibili dal punto di vista ambientale.
9. Foundation Models (Sistemi IA "ad alto impatto"). Le pubbliche amministrazioni, prima di adottare foundation models "ad alto impatto", si assicurano che essi adottino adeguate misure di trasparenza che chiariscono l'attribuzione delle responsabilità e dei ruoli, in particolare dei fornitori e degli utenti del sistema di IA.

10. Dati. Le pubbliche amministrazioni, che acquistano servizi di intelligenza artificiale tramite API, valutano con attenzione le modalità e le condizioni con le quali il fornitore del servizio gestisce di dati forniti dall'amministrazione con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati e privacy.

È possibile ritrovare alcuni dei principi elencati nel Piano triennale per l'informatica nella Pubblica amministrazione, con una formulazione diversa, nelle raccomandazioni del Rapporto del Comitato europeo delle Regioni, trattandosi di condizioni abilitanti per permettere alle pubbliche amministrazioni di ottemperare ai contenuti dell'AI ACT e della legge 132/2025 e alle Linee guida che dovrebbero essere prossimamente adottate da AGID[18].
È proprio il combinato disposto dell'AI ACT, della legge 132/2025 e delle Linee guida a definire il quadro di regole entro cui si devono muovere le pubbliche amministrazioni nell'adozione di soluzioni di IA.

Qui è sufficiente ricordare come l'approccio di Regione Lombardia abbia seguito i principi enunciati nella normativa per lo sviluppo dei casi d'uso di IA con particolare attenzione agli aspetti collegati alla privacy e alla sicurezza del dato, che rappresentano un possibile freno alle sperimentazioni.
All'interno di ARIA, infatti, nel corso degli ultimi due anni è stato costituito un Gruppo di Lavoro multidisciplinare con la finalità di indirizzare gli aspetti tecnici e di compliance alle normative vigenti oltre che di protezione dei dati e dei sistemi. Dalle soluzioni più sfidanti che sono in fase di realizzazione il GdL ha l'obiettivo di istruire una metodologia standardizzata atta ad indirizzare la compliance a tutte le future soluzioni progettuali basata sull'IA introdotte in ARIA e quindi nel SIREG, facendo fare un salto di scala all'utilizzo dell'IA che oggi risente, come evidenziato dalle ricognizioni sulle pubbliche amministrazioni, di un approccio precauzionale.
Nell'approccio di Regione Lombardia all'intelligenza artificiale, desumibile dai documenti presentati nel gruppo di lavoro interdirezionale sull'intelligenza artificiale, viene sottolineata l'attenzione alla trasparenza e all'interpretabilità dei modelli e viene ribadita la centralità della supervisione umana sulle decisioni finali.

Stando alla Bozza di Linee guida di AGID, le PA devono porre in essere idonee misure di comunicazione. Le PA che adottano sistemi di IA devono implementare misure di trasparenza finalizzate a garantire che gli utenti siano consapevoli del loro utilizzo e dell'impatto che tali sistemi possono avere sui processi decisionali. La trasparenza è un requisito fondamentale per assicurare la fiducia nei confronti delle tecnologie utilizzate, in conformità con i principi di trasparenza e responsabilità amministrativa sanciti dalle normative unionali. Lo scopo è quello di consentire ai cittadini di comprendere i criteri e i parametri su cui si basano le decisioni automatizzate prese dal sistema di IA con un'informazione chiara e semplice.

La supervisione di esperti o di personale qualificato risponde ad una visione antropocentrica dell'IA e al tempo stesso ad uno dei principi del diritto amministrativo, quello della responsabilità degli atti. La

[18] Cfr. Bozza di linee guida per l'adozione di IA nella pubblica amministrazione disponibile per la consultazione sul sito di AGID https://www.agid.gov.it/sites/agid/files/2025-02/Linee_Guida_adozione_IA_nella_PA.pdf

supervisione umana è indispensabile perché, nonostante l'elevato grado di affidabilità raggiunto da alcuni sistemi di IA di tipo generativo, questi possono commettere errori dovuti all'addestramento, al tipo di modelli predittivi. Allo stesso tempo come ribadito da autorevole dottrina, la decisione ultima, resta sotto la piena responsabilità dell'essere umano, come prevede l'art. 4, comma 2, d.lgs. n. 165/2001.
La necessità della supervisione umana, che nella pubblica amministrazione è una condizione necessaria per i procedimenti amministrativi, richiede un forte investimento sulla formazione e lo sviluppo delle competenze dedicate a gestire procedimenti che prevedono l'utilizzo di soluzioni di IA . Come ribadito nelle Linee guida di prossima adozione «la Pubblica amministrazione deve sviluppare competenze specifiche per poter governare e regolamentare l'utilizzo dell'IA, garantendo il rispetto di principi etici, di protezione dei dati personali e di trasparenza. Questo aspetto è fondamentale per promuovere un'adozione responsabile e sostenibile di queste tecnologie, che possano contribuire a migliorare l'equità e l'inclusione nell'erogazione dei servizi pubblici.» Come evidenziato dal rapporto di AGID «una delle principali criticità è la dipendenza da fornitori esterni. Tale scenario solleva interrogativi rispetto alla capacità delle amministrazioni di adeguare i profili professionali interni alle esigenze progettuali, o di formare risorse in linea con gli obiettivi di sviluppo e gestione delle soluzioni IA. Inoltre, si osserva una marcata esternalizzazione delle fasi progettuali, affidate prevalentemente a imprese private, con una partecipazione marginale di università, enti di ricerca ed enti pubblici. Questo modello operativo potrebbe nel tempo limitare l'autonomia delle amministrazioni e ridurre la loro capacità di innovazione interna».

Le indicazioni di policy non possono non tenere conto dei contenuti delle Linee guida e di alcune buone pratiche realizzate a livello regionale.
In particolare, l'amministrazione regionale sulla scorta di quanto realizzato dalla Regione Puglia potrebbe istituire un centro di competenza regionale sull'IA nella pubblica amministrazione. Si tratta di una forma di coordinamento delle azioni sull'IA allargato non solo agli enti del SIREG, come l'attuale Gruppo di lavoro, ma anche al Consiglio regionale e ad altre pubbliche amministrazioni del territorio.
La parte innovativa dell'intervento della Regione Puglia, già previsto nel 2023 e successivamente inserito nella legge regionale, è stata quello di ideare una forma di coordinamento che coinvolgesse le università del territorio, il Consiglio regionale e anche un rappresentante dell'Agenzia per l'Italia Digitale. Riprendendo i contenuti della DGR della Regione Puglia[19], le attività di questo centro di competenza regionale potrebbero essere:
- studio sullo sviluppo delle tecnologie di intelligenza artificiale nel settore della Pubblica Amministrazione;
- monitoraggio delle soluzioni applicative di intelligenza artificiale da adottare, o eventualmente già adottate, all'interno dell'Amministrazione Regionale e degli enti del sistema regionale;
- il supporto al procurement di tecnologie e strumenti basati sull'intelligenza artificiale da implementare in bandi e avvisi per migliorare la performance dei sistemi regionali;

[19] DELIBERAZIONE DELLA GIUNTA REGIONALE 30 ottobre 2023, n. 1488 Istituzione del Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione. Il Centro è uno strumento del Piano triennale per l'Informatica nella Pubblica amministrazione.

- comunicazione e divulgazione, alle strutture regionali e alle altre amministrazioni del territorio, su tutti gli aspetti dell'utilizzo delle tecnologie di intelligenza artificiale;
- adozione di linee di indirizzo per l'utilizzo di soluzioni tecnologiche di intelligenza artificiale in ambito regionale;
- formazione orientata ai dipendenti e alle altre Pubbliche Amministrazioni del territorio per l'utilizzo delle soluzioni tecnologiche di intelligenza artificiale.

Si tratta in alcuni casi di attività già svolte da ARIA o coordinate dal GdL interdirezionale, ma che potrebbero essere utilmente estese alle pubbliche amministrazioni territoriali.

Nell'ottica del rafforzamento delle competenze interne, sulla scorta delle indicazioni fornite nelle Bozze di Linee guida Regione Lombardia potrebbe avviare una mappatura attenta e comprensiva delle figure professionali già presenti nelle PA, con l'obiettivo di identificare chiaramente le responsabilità legate alla governance dell'IA. Questo processo permetterebbe di definire in maniera mirata i piani formativi e di up-skilling, garantendo che il personale disponga delle competenze necessarie per gestire in modo efficace e responsabile i sistemi IA, anche nella fase del procurement.
Infine occorre, all'interno del centro di competenze e sulla scorta di quanto già fatto in ARIA, consolidare metodologie per analizzare la compliance dei casi di utilizzo dell'IA con una valutazione preventiva degli impatti etici e sociali integrata come prassi ordinaria nell'implementazione delle nuove tecnologie. Tale attività dovrebbe evitare le forme di discriminazione e di bias che potrebbero celarsi nelle decisioni algoritmiche.

Glossario

Concetti Tecnici e Operativi

- Algoritmo (Algorithm)

In parole semplici e per il contesto di riferimento, è una serie di istruzioni o regole che un computer segue per eseguire un compito o risolvere un problema. I sistemi di IA utilizzano algoritmi complessi per analizzare dati e prendere decisioni.

- Deep Learning (Apprendimento Profondo)

Una tecnica avanzata di Machine Learning che si ispira alla struttura del cervello umano (reti neurali). È particolarmente efficace nel riconoscere schemi complessi in grandi quantità di dati, come immagini, suoni e testi. È la tecnologia alla base di molte delle più recenti innovazioni in ambito IA.

- Digital Twin (Gemello Digitale)

È una replica virtuale, un modello digitale, di un oggetto fisico, di un processo o di un intero sistema (come una città o una regione). Viene costantemente aggiornato con dati reali e permette di fare simulazioni per prevedere come si comporterà la sua controparte reale in diverse situazioni (es. simulare l'impatto di una nuova politica sul traffico).

- IA (Intelligenza Artificiale)

Un campo dell'informatica che mira a creare macchine e software capaci di svolgere compiti che normalmente richiederebbero l'intelligenza umana, come comprendere il linguaggio, riconoscere immagini, risolvere problemi e apprendere dall'esperienza.

- IA Generativa (GenAI)

Un tipo di intelligenza artificiale in grado di creare contenuti nuovi e originali (testi, immagini, musica, codice) partendo da un'istruzione (chiamata prompt). ChatGPT di OpenAI è l'esempio più famoso di IA generativa. Altri esempi sono Gemini di Google, Claude di Anthropic, Grok di X.

- Lock-in (Vincolo Tecnologico)

Situazione in cui un'amministrazione (o un cliente in generale) diventa dipendente da un unico fornitore di tecnologia, perché i costi per passare a un'alternativa sono troppo alti. L'uso di software open-source è una strategia per evitare il lock-in.

- LLM (Large Language Model - Modello Linguistico di Grandi Dimensioni)

Il "motore" che sta dietro a molte IA generative. È un sistema addestrato su enormi quantità di testi per comprendere e generare il linguaggio umano in modo sofisticato e versatile.

- Machine Learning (Apprendimento Automatico)

Una branca dell'IA in cui i computer "imparano" dai dati senza essere esplicitamente programmati. Invece di seguire istruzioni fisse, il sistema analizza esempi per identificare schemi e fare previsioni o prendere decisioni.

- On-premise

Indica che un software o un sistema informatico è installato ed eseguito sui server fisici di proprietà e gestiti direttamente dall'organizzazione (es. un'amministrazione pubblica), invece che su server esterni di un fornitore (in cloud). Questa scelta aumenta il controllo e la sicurezza dei dati.

- Open-source

Si riferisce a un software il cui codice sorgente è "aperto", cioè liberamente accessibile a tutti. Chiunque può vederlo, modificarlo e distribuirlo. Per la PA, adottare soluzioni open-source favorisce la trasparenza, la collaborazione e riduce la dipendenza da un singolo fornitore.

- RAG (Retrieval-Augmented Generation)

Una tecnica di IA generativa che migliora l'affidabilità delle risposte. Invece di generare testo basandosi solo sulla sua conoscenza pregressa, il sistema prima "cerca" le informazioni pertinenti in una base di dati specifica (es. un insieme di leggi) e poi usa quelle informazioni per costruire la risposta. Questo riduce il rischio di errori ("allucinazioni") e permette di citare le fonti.

- Sandbox (Spazio di sperimentazione)

È un ambiente controllato e sicuro dove sviluppatori e amministrazioni possono testare tecnologie innovative, come i sistemi di IA, sotto una supervisione, anche delle autorità in materia. Permette di sperimentare senza rischi per il pubblico e di verificare la conformità alle normative prima di un'adozione su larga scala.

Concetti Normativi e di Policy

- Accountability (Responsabilità/Rendicontazione)

È il principio per cui deve essere sempre chiaro chi è responsabile per le decisioni e le azioni di un sistema di IA, specialmente in caso di errori o danni. Implica la necessità di tracciare i processi e definire ruoli e responsabilità.

- AI Act (Regolamento UE sull'Intelligenza Artificiale)

La legge fondamentale dell'Unione Europea sull'intelligenza artificiale. Il suo scopo è creare regole comuni per tutti gli Stati membri per garantire che i sistemi di IA siano sicuri e rispettino i diritti fondamentali dei cittadini. Introduce un approccio basato su diversi livelli di rischio.

- Approccio basato sul rischio (Risk-based approach)

È il principio cardine dell'AI Act. Invece di applicare le stesse regole a tutti i sistemi di IA, la legge classifica le applicazioni in quattro categorie di rischio (inaccettabile, alto, limitato, minimo) e impone obblighi più severi per quelle che presentano rischi maggiori per la salute, la sicurezza o i diritti delle persone.

- DPIA (Data Protection Impact Assessment - Valutazione d'Impatto sulla Protezione dei Dati)

Un'analisi obbligatoria prevista dal GDPR quando si utilizzano nuove tecnologie che potrebbero presentare un rischio elevato per i diritti e le libertà delle persone. Serve a identificare e mitigare i rischi legati al trattamento dei dati personali.

- FRIA (Fundamental Rights Impact Assessment - Valutazione d'Impatto sui Diritti Fondamentali)

Un'analisi richiesta dall'AI Act per gli enti pubblici che intendono utilizzare sistemi di IA "ad alto rischio". Serve a valutare e mitigare i potenziali impatti negativi che il sistema potrebbe avere sui diritti fondamentali dei cittadini (es. diritto alla non discriminazione, alla privacy, ecc.).

- GDPR (General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati)

È il principale regolamento europeo sulla privacy. Stabilisce le regole su come le organizzazioni, incluse le PA, devono raccogliere, utilizzare e proteggere i dati personali dei cittadini. L'uso dell'IA deve sempre essere conforme al GDPR.

- Gold-plating

Termine usato in ambito normativo per descrivere la pratica di uno Stato membro di aggiungere obblighi o regole più restrittive rispetto a quanto strettamente richiesto da un regolamento europeo. Nel contesto del DDL italiano sull'IA, si riferisce al rischio che l'Italia imponga requisiti più severi di quelli previsti dall'AI Act.

- Spiegabilità (Explainability)

Il principio secondo cui le decisioni prese da un sistema di IA, specialmente quelle complesse, devono poter essere spiegate in un linguaggio comprensibile per un essere umano. È fondamentale per garantire la trasparenza e il diritto dei cittadini a contestare una decisione automatizzata.

- Supervisione umana (Human-in-the-loop)

Principio secondo cui deve sempre esserci un essere umano in grado di supervisionare, controllare e, se necessario, intervenire o correggere le decisioni di un sistema di IA. È un requisito fondamentale, specialmente per i sistemi ad alto rischio.

Attori e Organismi di Governance

- ACN (Agenzia per la Cybersicurezza Nazionale)

È l'autorità nazionale italiana responsabile della cybersicurezza. La legge italiana sull'IA la designa come una delle due "Autorità nazionali per l'IA", con compiti di vigilanza sul mercato e sanzionatori.

- AGID (Agenzia per l'Italia Digitale)

È l'agenzia governativa che promuove la digitalizzazione della PA in Italia. La legge italiana sull'IA la designa come una delle due "Autorità nazionali per l'IA", con compiti di promozione e notifica degli organismi di valutazione.

- Deployer (Utilizzatore)

Termine usato dall'AI Act per indicare la persona o l'organizzazione (come una PA) che utilizza un sistema di IA sotto la propria autorità e responsabilità. L'utilizzatore ha obblighi specifici, come garantire la supervisione umana e, per i sistemi ad alto rischio, effettuare la valutazione d'impatto (FRIA).

- Fornitore (Provider)

Termine usato dall'AI Act per indicare chi sviluppa un sistema di IA e lo immette sul mercato. Il fornitore ha la responsabilità principale di garantire che il sistema sia conforme ai requisiti di legge prima di venderlo o distribuirlo.

- AI Office (Ufficio per l'IA)

Un nuovo organismo istituito all'interno della Commissione Europea. Ha il compito di supervisionare l'applicazione dell'AI Act in tutta l'UE, con un focus particolare sui modelli di IA più avanzati (GPAI).

Bibliografia

AGID. (2023). Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026.
AGID. (2024). Strategia Italiana per l'Intelligenza Artificiale 2024-2026. Agenzia per l'Italia Digitale. https://www.agid.gov.it/
AGID (2025). L'Intelligenza Artificiale nella Pubblica Amministrazione. Rapporto 2025.
Bird & Bird LLP. (2025). European union artificial intelligence act: A guide [Manual]. Bird & Bird LLP.
Burelli, C. (2024). Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità? Quaderni AISDUE - Fascicolo speciale: La nuova disciplina UE sull'intelligenza artificiale, 2, 237 ss.
Burelli, C. (2025). Ancora sul "ddl intelligenza artificiale": il parere circostanziato della Commissione europea ai sensi dell'art. 6, par. 2, comma 2, della direttiva (UE) 2015/1535. Quaderni AISDUE, 1.
Cabrera, L. L., & McGowan, I. (2024). A series on the EU AI act, part 1: An overview. Center for Democracy & Technology (CDT) Europe. https://cdt.org/insights/cdt-europes-submission-on-the-ethical-and-legal-requirements-in-the-european-commissions-ai-act/
Cancela-Outeda, C. (2024). The EU's AI act: A framework for collaborative governance. Internet of Things, 27, 101291. https://doi.org/10.1016/j.iot.2024.101291
Capolupo, N., & Adinolfi, P. (2023). Organizzazioni pubbliche e intelligenza artificiale. Un cambiamento possibile? Prospettive in Organizzazione. https://prospettiveinorganizzazione.assioa.it/organizzazioni-pubbliche-e-intelligenza-artificiale-un-cambiamento-possibile/
Cappai, M. (2024). Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale? federalismi.it - Rivista di diritto pubblico italiano, comparato, europeo, 30, 186–206.
Cappellaro G., Ardito V., Compagni A. Masella C., Olive M., Petracca F., Preti L.M. Sgarbossa C. (2024), RESEARCH BRIEF Survey MUSA: Adozione dell'intelligenza artificiale nella pratica clinica da parte delle aziende sanitarie lombarde
Carey, S. (2025). Regulating Uncertainty: Governing General-Purpose AI Models and Systemic Risk. European Journal of Risk Regulation, 1–17. https://doi.org/10.1017/err.2025.10040
Carta, M. (2024). Il Regolamento UE sull'Intelligenza Artificiale: Alcune questioni aperte. Eurojus.it Rivista, 3.
Cassano, G. (2024). Il D.D.L. italiano in materia di intelligenza artificiale. Revista Amagis Jurídica, 16(2), 111–136.
Conferenza delle Regioni e delle Province Autonome (2024). Esiti della rilevazione 2024 sui casi d'uso regionali di sperimentazione dell'intelligenza Artificiale (IA).
Coppola, F. (2024). Note in prima lettura sulle disposizioni penali del c.d. DDL "Intelligenza Artificiale". Iura & Legal Systems, XI(2), 102–107.
D'Angiolella, R. (2025). Giustizia e intelligenza artificiale tra l'AI ACT e il disegno di legge italiano. Giustizia Insieme. https://www.giustiziainsieme.it/it/diritto-e-innovazione/3581-giustizia-e-intelligenza-artificiale-tra-lai-act-e-il-disegno-di-legge-italiano-rosita-dangiolella
De Donno, M. (2025). Le Regioni e l'Intelligenza Artificiale, *Istituzioni del Federalismo*, 2, pp.253-257.
Di Salvo, P., Napolitano, A., Ferrari, L., Agosti, C., Carrer, L., Monte, D. D., & Turola, M. (2024). I rischi dell'intelligenza artificiale: Analisi e raccomandazioni per l'applicazione del regolamento europeo

sull'intelligenza artificiale (AI Act). Hermes Center for Transparency and Digital Human Rights and The Good Lobby Italia.
European Commission, Joint Research Centre. (2024a). Competencies and governance practices for AI in the public sector. Publications Office. https://data.europa.eu/doi/10.2760/7895569
European Commission, Joint Research Centre. (2024b). What factors influence perceived AI adoption by public managers?: A survey among public managers in seven EU countries. Publications Office. https://data.europa.eu/doi/10.2760/0179285
European Commission, Joint Research Centre. (2024c). GovTech: Influencing factors, common requirements and recommendations (No. JRC136649). Publications Office of the European Union. https://doi.org/10.2760/284903
European Commission. (2019). Ethics guidelines for trustworthy AI. High-Level Expert Group on Artificial Intelligence.
European Commission. (2024a). Public sector tech watch: Adoption of AI, blockchain and other emerging technologies within the european public sector. Publications Office of the European Union. https://doi.org/10.2799/4393
European Commission. (2024b). Public sector tech watch: Mapping innovation in the EU public services. Publications Office of the European Union. https://doi.org/10.2799/4393
European Commission. (2025). Public sector tech watch: Analysis of the generative AI landscape in the european public sector. Publications Office of the European Union. https://doi.org/10.2799/0409819
European Committee of the Regions: Commission for Economic Policy, Fondazione FORMIT, Trilateral Research Limited, Fontana, S., Errico, B. et al., AI and GenAI adoption by local and regional administrations, European Committee of the Regions, 2024, https://data.europa.eu/doi/10.2863/6007868
Falletta, P., & Marsano, A. (2024). Intelligenza artificiale e protezione dei dati personali: Il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR. *Rivista italiana di informatica e diritto*, 6(1), 119–137. https://doi.org/10.32091/RIID0155
Garante per la protezione dei dati personali. (s.d.). ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola. Recuperato 16 ottobre 2025, da https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9874751
Gardini G. (2025). L'uso preparatorio dell'AI come limite agli eccessi regolativi. Per una valutazione "in concreto" dell'intelligenza artificiale applicata all'agire pubblico, *Istituzioni del Federalismo*, 2, pp. 261-299
Gastaldi, L., Petrocelli, M., Rinaldi, L., & Rollin, A. (2024). AI in public settings: Status and next steps (Economic Focus No. 1). Ministry of Economy and Finance, Department of the Treasury. https://www.dt.mef.gov.it/it/analisi_e_programmazione_economico_finanziaria/focus_economici/
GPDP. (2023). Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9938038
Green, A. (2024). Artificial intelligence and the changing demand for skills in the labour market (OECD Artificial Intelligence Papers, No. 14). OECD Publishing.
Guidi, D. M. (2025). Intelligenza artificiale tra intese e collusioni algoritmiche nel diritto dell'Unione europea: Questioni interpretative alla luce del DMA, DSA e AI ACT. Eurojus.it Rivista, 2.

High-Level Expert Group on AI (AI HLEG). (2020). The assessment list for trustworthy artificial intelligence (ALTAI) for self assessment. European Commission.
Mancarella, M. (2023). Intelligenza artificiale e pubblica amministrazione: riflessioni di informatica giuridica. Rivista Elettronica di Diritto, Economia, Management, 4, 251–263.
Mancioppi, F. M. (2024). La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE. Federalismi.it.
Maslej, N., et al. (2025). Artificial Intelligence Index Report 2025. Stanford Institute for Human-Centered Artificial Intelligence, Stanford University.
Menéndez Sebastián, E. M. (2023). L'intelligenza artificiale nel settore pubblico: Sulla perenne ricerca di un equilibro tra efficienza e garanzie. Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche, 2, 66–84.
Morando, M. (2024). Transizione digitale, intelligenza artificiale e le nuove competenze per la pubblica amministrazione [Tesi di laurea magistrale, Università degli Studi di Padova].
Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2024). A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation, 1–25. https://doi.org/10.1017/err.2024.57
OECD & United Nations Educational, Scientific and Cultural Organization. (2024). G7 Toolkit for Artificial Intelligence in the Public Sector. https://doi.org/10.1787/421c1244-en
OECD. (2023). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449.
OECD. (2024). Governing with artificial intelligence: Are governments ready? (OECD Artificial Intelligence Papers, No. 20). OECD Publishing. https://doi.org/10.1787/26324bc2-en
Perlusz, R. (2025). Dalla proposta AS 1146 alla legge 132/2025. MediaLaws - Rivista di diritto dei media. https://www.medialaws.eu/22350-2/
Pietrocarlo E. (2024). La predictive policing nel regolamento europeo sull'intelligenza artificiale. La legislazione penale ISSN: 2421-552X
Presno Linera, M. Á., & Meuwese, A. (2025). Regulating AI from Europe: A joint analysis of the AI Act and the Framework Convention on AI. The Theory and Practice of Legislation, 0(0), 1–20. https://doi.org/10.1080/20508840.2025.2492524
Rangone, N., & Megale, L. (2025). Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making. European Journal of Risk Regulation, 1–16. https://doi.org/10.1017/err.2025.13
Regione Toscana. (2024). Legge Regionale 9 dicembre 2024, n. 57. Norme per l'innovazione digitale, lo sviluppo e la tutela dei diritti di cittadinanza digitale nel territorio regionale. Modifiche alla l.r. 54/2009. Pubblicata nel Bollettino Ufficiale della Regione Toscana n. 50, Parte prima, dell'11 dicembre 2024.
Regione Toscana. (2025a). Indicazioni operative per l'adozione di soluzioni di Intelligenza Artificiale in riferimento all'AI Act in Toscana.
Regione Toscana. (2025b). Allegato I: Considerazioni Tecniche ed Architetturali su Possibili Implementazioni di AI. Allegato a "Indicazioni operative per l'adozione di soluzioni di Intelligenza Artificiale in riferimento all'AI Act in Toscana"
Riccio, G. (2024). Intelligenza artificiale generativa nella pubblica amministrazione: Un framework integrato per comprenderne l'impatto. Governo dell'economia e dell'innovazione, 1, 61–81.
Sousa E Silva, N. (2024). The Artificial Intelligence Act: Critical Overview. SSRN. https://doi.org/10.2139/ssrn.4937150

Stelling, L., Yang, M., Gipiškis, R., Staufer, L., Chin, Z. S., Campos, S., Gil, A., & Chen, M. (2025). Mapping Industry Practices to the EU AI Act's GPAI Code of Practice Safety and Security Measures.
Taeihagh, A. (2025). Governance of Generative AI. Policy and Society, 44(1), 1–22. https://doi.org/10.1093/polsoc/puaf001
Tommasi, D. S. (2023). DIGITAL SERVICES ACT E ARTIFICIAL INTELLIGENCE ACT: TENTATIVI DI FUTURO DA ARMONIZZARE. Persona e Mercato, 2.
UNESCO. (2022). Recommendation on the Ethics of Artificial Intelligence. UNESCO Publishing.
UNESCO. (2024). AI and democracy: Towards democratic governance of AI. United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000388053
Van Noordt, C., Medaglia, R., & Tangi, L. (2025). Policy initiatives for Artificial Intelligence-enabled government: An analysis of national strategies in Europe. Public Policy and Administration, 40(2), 215–253. https://doi.org/10.1177/09520767231198411
Van Pinxteren, D. (2024). The AI act: Key impacts for the public sector. Digital Government Society. https://www.digit-government.org/policy-briefs/ai-act-public-sector

Sitografia

AP-HP. (2025). L'AP-HP signe un partenariat avec Gleamer pour développer une solution d'intelligence artificielle. Recuperato il 17 ottobre 2025, da https://www.aphp.fr/actualites/lap-hp-signe-un-partenariat-avec-gleamer-pour-developper-une-solution-dintelligence
AIRA. (2025). Aliança per una Intel·ligència Artificial Responsable a Catalunya. Recuperato il 17 ottobre 2025, da https://airacat.eu/
Baden-Württemberg. (2025). KI-Assistenz F13 wird zur Open-Source-Software. Recuperato il 17 ottobre 2025, da https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/ki-assistenz-f13-wird-zur-open-source-software
CIDAI. (2025). Centre of Innovation for Data tech and Artificial Intelligence. Recuperato il 17 ottobre 2025, da https://cidai.eu/
Consiglio Regionale della Toscana. (2025). Servizi Digitali. Recuperato il 17 ottobre 2025, da https://www.consiglio.regione.toscana.it/default?nome=servizi_digitali
CORDIS. (2025). Mobile Ecosystem for GLucose and InSulin Support Automation (MELISSA). Commissione Europea. Recuperato il 17 ottobre 2025, da https://cordis.europa.eu/project/id/101057730
F13. (2025). F13: Der KI-Assistent für den öffentlichen Sektor. Recuperato il 17 ottobre 2025, da https://f13-os.de/
Juncà, D. (2024). L'estratègia d'intel·ligència artificial de Catalunya (CATALONIA.AI). Generalitat de Catalunya. Recuperato il 17 ottobre 2025, da https://www.gencat.cat/eapc/epum/N22/pdf/EPuM22Junca.pdf
KI-Reallabor. (2025). ROUTINE: Real-World Data Lab. Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg. Recuperato il 17 ottobre 2025, da https://ki-reallabor-bw.de/

OEIAC. (2025). Observatory of Ethics in Artificial Intelligence of Catalonia. Recuperato il 17 ottobre 2025, da https://oeiac.cat/en/
Xunta de Galicia. (2025a). Lei 2/2025, do 2 de abril, para o desenvolvemento e o impulso da intelixencia artificial de Galicia. Boletín Oficial del Estado. Recuperato il 17 ottobre 2025, da https://www.boe.es/buscar/doc.php?id=DOG-g-2025-90074
Xunta de Galicia. (2025b). Estratexia Galega de Intelixencia Artificial. Recuperato il 17 ottobre 2025, da https://www.xunta.gal/intelixencia-artificial

Progetto grafico e stampa CENTROSTAMPA - Consiglio regionale della Lombardia