



UNIVERSITA' DEGLI STUDI DI PAVIA

**DIPARTIMENTO DI SCIENZE POLITICHE E SOCIALI
CORSO DI LAUREA MAGISTRALE IN GOVERNO E POLITICHE
PUBBLICHE**

**L'IMPATTO DELL'AI ACT SULL'USO
DELL'INTELLIGENZA ARTIFICIALE NELLA
PUBBLICA AMMINISTRAZIONE**

Relatore: Chiar.mo Prof. Alessandro Venturi
Correlatore: Dott. Luca Daffonchio

Tesi di Laurea di
Michela Beccaria
Matricola:558344

ANNO ACCADEMICO 2025/2026

INDICE

Introduzione.....	1
Capitolo 1 – Definizione e caratteristiche dell'intelligenza artificiale.....	7
1.1 Definizione di intelligenza artificiale.....	7
1.2 Evoluzione storica dell'intelligenza artificiale.....	8
1.3 Principali tipologie e applicazioni dell'intelligenza artificiale.....	12
1.4 Opportunità e rischi dell'intelligenza artificiale.....	17
Capitolo 2 – L'intelligenza artificiale nella Pubblica Amministrazione..	23
2.1 La trasformazione digitale della Pubblica Amministrazione.....	23
2.2 L'utilizzo dell'intelligenza artificiale nei servizi pubblici.....	27
2.3 Benefici dell'IA per la PA.....	30
2.4 Criticità e limiti dell'utilizzo dell'IA nella PA.....	33
Capitolo 3 – L'AI Act europeo.....	40
3.1 Origini, approvazione e obiettivi dell'AI Act	40
3.2 La classificazione dei sistemi di IA in base al rischio	46
3.3 Le pratiche di intelligenza artificiale vietate.....	53
3.4 I sistemi di IA ad alto rischio.....	60
3.5 Requisiti e obblighi previsti dall'AI Act.....	68
Capitolo 4 – L'impatto dell'AI Act sulla Pubblica Amministrazione.....	80
4.1 Gli obblighi per le amministrazioni pubbliche.....	80
4.2 Trasparenza e accountability.....	85
4.3 Tutela dei diritti fondamentali dei cittadini.....	90
4.4 Opportunità e sfide per la PA.....	95
4.5 Prospettive future.....	100
Conclusioni.....	105

Bibliografia.....	110
Fonti normative e istituzionali.....	113
Sitografia.....	117

INTRODUZIONE

Negli ultimi anni l'intelligenza artificiale ha assunto un ruolo sempre più rilevante nei processi di trasformazione economica, sociale e istituzionale. La crescente capacità dei sistemi di elaborare grandi quantità di dati, riconoscere regolarità, generare contenuti e supportare determinate attività decisionali ha favorito la loro diffusione in numerosi settori. Accanto alle applicazioni sviluppate in ambito privato, l'intelligenza artificiale sta progressivamente entrando anche nel settore pubblico, diventando uno degli strumenti attraverso i quali le amministrazioni possono proseguire il percorso di digitalizzazione avviato negli ultimi decenni.

Per la Pubblica Amministrazione, l'introduzione di queste tecnologie può offrire opportunità significative. I sistemi di intelligenza artificiale possono contribuire all'automazione di attività ripetitive, all'elaborazione di grandi quantità di informazioni, al supporto delle decisioni e al miglioramento delle modalità con cui vengono erogati i servizi pubblici. Chatbot, sistemi di classificazione, strumenti predittivi e applicazioni generative possono essere utilizzati in ambiti differenti dell'attività amministrativa e affiancare il personale nello svolgimento di alcune funzioni.

L'utilizzo dell'intelligenza artificiale nel settore pubblico presenta però caratteristiche particolari rispetto al suo impiego in altri contesti. Le amministrazioni esercitano funzioni rivolte alla collettività e adottano decisioni che possono incidere direttamente sulla posizione delle persone. L'impiego di sistemi automatizzati può quindi coinvolgere aspetti legati alla trasparenza, all'imparzialità, alla protezione dei dati personali, alla non discriminazione e alla possibilità per il cittadino di comprendere e contestare le decisioni che lo riguardano. Ai possibili benefici derivanti dall'innovazione si affiancano così

rischi che richiedono regole, strumenti di controllo e responsabilità chiaramente individuate.

La rapida diffusione dell'intelligenza artificiale ha progressivamente evidenziato la necessità di costruire un quadro normativo capace di accompagnarne lo sviluppo e l'utilizzo. L'Unione europea ha affrontato questa esigenza attraverso un percorso iniziato diversi anni prima dell'approvazione dell'AI Act e fondato sulla ricerca di un equilibrio tra innovazione tecnologica e tutela delle persone. Il Regolamento (UE) 2024/1689 rappresenta il principale risultato di questo percorso e introduce un sistema comune di regole applicabile allo sviluppo, all'immissione sul mercato e all'utilizzo dei sistemi di intelligenza artificiale nell'Unione europea.

L'AI Act adotta un modello basato sul rischio, nel quale l'intensità della disciplina varia in relazione alla finalità del sistema, al contesto nel quale viene utilizzato e alle possibili conseguenze sulle persone. Alcune pratiche considerate incompatibili con i valori dell'Unione sono vietate, mentre i sistemi classificati come ad alto rischio possono essere utilizzati soltanto nel rispetto di requisiti e obblighi specifici. A queste disposizioni si affiancano obblighi di trasparenza e una disciplina dedicata ai modelli di intelligenza artificiale per finalità generali. Questo quadro assume una particolare importanza per la Pubblica Amministrazione. Numerosi ambiti individuati dal regolamento come particolarmente delicati riguardano infatti attività nelle quali gli enti pubblici svolgono un ruolo diretto. Tra questi rientrano l'istruzione, l'occupazione, l'accesso a prestazioni e servizi essenziali, le attività di contrasto, la gestione della migrazione e l'amministrazione della giustizia. In tali settori l'impiego dell'intelligenza artificiale può produrre conseguenze rilevanti per i cittadini e rende necessario comprendere in che modo le nuove regole europee incidano

concretamente sulle modalità di organizzazione e di azione delle amministrazioni.

Da questa esigenza nasce il tema centrale della presente tesi. L'obiettivo del lavoro è analizzare **l'impatto dell'AI Act sull'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione**, cercando di comprendere in che modo il nuovo quadro europeo modifichi le condizioni nelle quali gli enti pubblici possono adottare e utilizzare tali sistemi. La ricerca non riguarda quindi soltanto il contenuto del regolamento, ma il rapporto tra le disposizioni dell'AI Act e le caratteristiche proprie dell'attività amministrativa.

La domanda che guida il lavoro può essere formulata nel modo seguente. **Qual è l'impatto dell'AI Act sull'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione e in che modo il nuovo quadro europeo modifica le condizioni nelle quali gli enti pubblici possono adottare e utilizzare tali sistemi?**

Per rispondere a questa domanda è stata svolta un'analisi della letteratura scientifica relativa all'intelligenza artificiale e al suo impiego nel settore pubblico, affiancata dallo studio della normativa europea e nazionale e della documentazione prodotta dalle istituzioni competenti. Particolare attenzione è stata dedicata al Regolamento (UE) 2024/1689 e alle successive modifiche intervenute nel 2026, oltre ai documenti della Commissione europea e dell'Agenzia per l'Italia Digitale. L'analisi delle fonti normative e istituzionali è stata integrata con contributi scientifici relativi agli effetti organizzativi, giuridici e amministrativi derivanti dall'utilizzo dell'intelligenza artificiale nel settore pubblico.

Il lavoro è articolato in quattro capitoli, costruiti secondo un percorso che parte dall'inquadramento generale dell'intelligenza artificiale e arriva

progressivamente all'analisi delle conseguenze dell'AI Act sulla Pubblica Amministrazione.

Il primo capitolo è dedicato alla definizione e alle principali caratteristiche dell'intelligenza artificiale. Dopo aver affrontato il problema della definizione del concetto, viene ricostruita la sua evoluzione storica, dalle prime elaborazioni teoriche fino allo sviluppo delle tecniche più recenti. Vengono poi esaminate le principali tipologie e metodologie, tra cui machine learning, deep learning, reti neurali, elaborazione del linguaggio naturale e intelligenza artificiale generativa. Il capitolo si conclude con l'analisi delle principali opportunità offerte da queste tecnologie e dei rischi che possono derivare dal loro utilizzo, con particolare attenzione all'opacità dei sistemi, alle distorsioni algoritmiche, alla protezione dei dati e alla responsabilità.

Il secondo capitolo concentra l'attenzione sulla Pubblica Amministrazione. L'analisi parte dal più ampio processo di trasformazione digitale del settore pubblico e dal ruolo assunto nel tempo da dati, infrastrutture e servizi digitali. Successivamente vengono approfondite le principali modalità di utilizzo dell'intelligenza artificiale nei servizi pubblici e nei processi amministrativi. L'esame riguarda sia le applicazioni rivolte direttamente ai cittadini sia gli strumenti impiegati all'interno delle amministrazioni per supportare attività di analisi, pianificazione e controllo. Dopo aver individuato i principali benefici in termini di efficienza, capacità di elaborazione e qualità dei servizi, vengono esaminate le criticità che possono accompagnare l'adozione dell'IA, tra cui la qualità dei dati, la trasparenza, la spiegabilità, la tutela della riservatezza, la sicurezza informatica, le competenze e la dipendenza dai fornitori esterni.

Il terzo capitolo è dedicato all'AI Act europeo. Viene ricostruito il percorso che ha condotto alla sua approvazione, a partire dalle prime iniziative dell'Unione europea fino all'adozione del Regolamento (UE) 2024/1689. Successivamente

viene analizzata la struttura basata sul rischio che caratterizza la disciplina, distinguendo le pratiche vietate, i sistemi ad alto rischio e le applicazioni soggette a specifici obblighi di trasparenza. Una parte rilevante del capitolo è dedicata ai sistemi ad alto rischio e ai requisiti tecnici, organizzativi e documentali che devono essere rispettati dai soggetti coinvolti nello sviluppo e nell'utilizzo dell'intelligenza artificiale. L'analisi considera anche gli obblighi dei provider e dei deployer, la valutazione di conformità, la registrazione, il monitoraggio e le disposizioni relative ai modelli di intelligenza artificiale per finalità generali.

Il quarto capitolo rappresenta il punto centrale del lavoro e analizza direttamente l'impatto dell'AI Act sulla Pubblica Amministrazione. In primo luogo, vengono esaminati gli obblighi che possono ricadere sugli enti pubblici quando assumono il ruolo di deployer e utilizzano sistemi di intelligenza artificiale nelle proprie attività. L'attenzione si sposta poi sui principi di trasparenza e accountability e sulla necessità che l'intervento dell'IA nei procedimenti rimanga conoscibile e riconducibile a soggetti responsabili. Il capitolo affronta successivamente la tutela dei diritti fondamentali dei cittadini, considerando il rapporto tra AI Act, uguaglianza, non discriminazione, protezione dei dati, buona amministrazione e diritto a una tutela effettiva.

L'ultima parte del capitolo esamina le opportunità e le sfide che l'applicazione del nuovo quadro normativo comporta per le amministrazioni. L'utilizzo dell'intelligenza artificiale dipende infatti non soltanto dalla conformità alle disposizioni europee, ma anche dalla presenza di competenze, risorse e capacità organizzative adeguate. Vengono infine considerate le prospettive future, con particolare attenzione al passaggio dalle sperimentazioni a un utilizzo più stabile dell'IA, alla capacità di valutarne i risultati, all'evoluzione delle competenze e alla necessità di adattare progressivamente le strategie pubbliche ai cambiamenti tecnologici e normativi.

Il percorso seguito consente quindi di osservare l'intelligenza artificiale prima come tecnologia, poi come strumento della trasformazione amministrativa e infine come oggetto di una disciplina europea destinata a incidere direttamente sulle modalità con cui gli enti pubblici possono utilizzarla. L'AI Act non riguarda soltanto il rispetto di nuovi adempimenti, ma contribuisce a definire le condizioni entro le quali l'innovazione può essere integrata nell'attività della Pubblica Amministrazione. Comprendere il suo impatto significa quindi valutare come l'utilizzo dell'intelligenza artificiale possa essere accompagnato da forme di organizzazione, controllo e tutela adeguate alla particolare funzione svolta dagli enti pubblici.

CAPITOLO 1

DEFINIZIONE E CARATTERISTICHE DELL'INTELLIGENZA ARTIFICIALE

1.1 Definizione di intelligenza artificiale

L'intelligenza artificiale (IA) costituisce un ambito di ricerca interdisciplinare sviluppatosi nell'ambito dell'informatica e progressivamente esteso a numerosi altri settori, tra cui matematica, statistica, scienze cognitive, neuroscienze, economia e diritto. Nonostante la crescente diffusione del termine nel linguaggio scientifico e comune, non esiste una definizione universalmente condivisa, poiché il concetto di intelligenza artificiale comprende approcci, metodologie e finalità differenti.¹

Una delle definizioni più ricorrenti descrive l'IA come la capacità delle macchine di svolgere attività che richiederebbero normalmente forme di intelligenza umana, quali il ragionamento, l'apprendimento, la risoluzione di problemi, la comprensione del linguaggio e il riconoscimento di immagini o schemi. Tale formulazione, pur essendo immediata, individua soprattutto l'obiettivo generale dell'intelligenza artificiale e non ne esaurisce la complessità. Una prospettiva più ampia la considera infatti come l'insieme di teorie, metodi, tecnologie e applicazioni finalizzati a simulare, estendere e ampliare alcune capacità riconducibili all'intelligenza umana.²

In questa prospettiva, l'IA non si limita a riprodurre comportamenti umani, ma comprende sistemi capaci di elaborare informazioni, individuare regolarità nei dati, apprendere dall'esperienza e utilizzare i risultati ottenuti per svolgere compiti specifici. Un contributo recente al dibattito definitorio è stato fornito da

¹ L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», *MediaLaws*, n. 3, 2021, pp. 13-28.

² Y. Jiang et al., «Quo vadis artificial intelligence?», *Discover Artificial Intelligence*, vol. 2, art. 4, 2022, pp. 1-19.

Gignac e Szodorai, i quali descrivono l'intelligenza artificiale come la massima capacità di un sistema artificiale di raggiungere con successo un obiettivo nuovo attraverso algoritmi computazionali. La definizione attribuisce particolare rilievo alla capacità del sistema di affrontare situazioni non precedentemente incontrate e distingue i processi artificiali, fondati su algoritmi, dai processi percettivi e cognitivi propri dell'essere umano.³

È inoltre necessario distinguere l'intelligenza artificiale dal *machine learning*, termini frequentemente utilizzati in modo improprio come sinonimi. Il *machine learning*, o apprendimento automatico, costituisce un sottoinsieme dell'IA e comprende tecniche attraverso le quali i sistemi apprendono dai dati e modificano le proprie prestazioni senza che ogni passaggio debba essere programmato anticipatamente. L'intelligenza artificiale rappresenta invece un campo più ampio, che include anche sistemi fondati su regole, conoscenze formalizzate e metodologie non necessariamente basate sull'apprendimento automatico.⁴

L'ampiezza della nozione di intelligenza artificiale deriva quindi dalla varietà delle tecniche impiegate e delle funzioni che i sistemi possono svolgere.

1.2 Evoluzione storica dell'intelligenza artificiale

L'evoluzione dell'intelligenza artificiale non ha seguito un andamento lineare, ma è stata caratterizzata dall'alternarsi di fasi di forte espansione e periodi di rallentamento. Sebbene la nascita ufficiale della disciplina venga generalmente collocata nel 1956, le sue basi teoriche furono poste nei decenni precedenti attraverso gli studi sulla logica, sul calcolo automatico e sul funzionamento dei processi cognitivi.⁵

³ G.E. Gignac, E.T. Szodorai, «Defining intelligence: Bridging the gap between human and artificial perspectives», *Intelligence*, vol. 104, 2024, articolo 101832, pp. 1-16.

⁴ L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 14-15.

⁵ Y. Jiang, X. Li, H. Luo, S. Yin, O. Kaynak, «Quo vadis artificial intelligence?», *Discover Artificial Intelligence*, vol. 2, art. 4, 2022, pp. 3-5; P.P. Groumpos, «A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities, and Threats», *Artificial Intelligence and Applications*, vol. 1, n. 4, 2023, pp. 182-184.

Un primo contributo fondamentale risale al 1936, quando Alan Turing elaborò il modello teorico della macchina universale, destinato a costituire uno dei principali fondamenti dell'informatica moderna. Nel 1943 Warren McCulloch e Walter Pitts proposero un modello matematico ispirato al funzionamento dei neuroni biologici, considerato il primo esempio di rete neurale artificiale. A questo risultato seguì, nel 1949, la formulazione della regola di apprendimento di Donald Hebb, fondata sull'idea che l'apprendimento derivi dal rafforzamento delle connessioni tra neuroni attivati simultaneamente.⁶

Nel 1950 Turing pubblicò il saggio *Computing Machinery and Intelligence*, nel quale sostituì la domanda astratta sulla possibilità che una macchina potesse pensare con un criterio fondato sull'osservazione del suo comportamento. Il cosiddetto test di Turing valuta se, nel corso di una conversazione, una macchina sia in grado di produrre risposte tali da non poter essere agevolmente distinte da quelle di un essere umano. Il test non misura direttamente la coscienza o la comprensione, ma rappresentò uno dei primi tentativi di definire operativamente il comportamento intelligente di una macchina.⁷

La nascita ufficiale dell'intelligenza artificiale viene fatta coincidere con il *Dartmouth Summer Research Project on Artificial Intelligence*, organizzato nel 1956 da John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon. In quella sede venne adottata l'espressione *Artificial Intelligence* e fu formulata l'ipotesi che gli aspetti dell'apprendimento e dell'intelligenza potessero essere descritti con sufficiente precisione da consentirne la simulazione mediante una macchina. L'incontro contribuì a delimitare un nuovo campo di ricerca e a riunire studiosi provenienti da ambiti scientifici differenti.⁸

⁶ Y. Jiang et al., «Quo vadis artificial intelligence?», cit., p. 3.

⁷ A.M. Turing, «Computing Machinery and Intelligence», *Mind*, vol. 59, n. 236, 1950, pp. 433-460; L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», *MediaLaws*, n. 3, 2021, p. 17.

⁸ J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, «A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence», 1955; L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 15-16.

I primi anni della disciplina furono caratterizzati da un notevole ottimismo. Furono realizzati programmi capaci di risolvere problemi logici, dimostrare teoremi, giocare e svolgere attività limitate di elaborazione del linguaggio. Nel 1957 Frank Rosenblatt introdusse il perceptron, un modello di rete neurale capace di modificare i propri parametri sulla base degli esempi ricevuti. Questi risultati alimentarono l'aspettativa che sistemi dotati di capacità comparabili a quelle umane potessero essere sviluppati in tempi relativamente brevi.⁹

Le previsioni iniziali non considerarono adeguatamente la complessità dei problemi affrontati e i limiti delle risorse disponibili. Tra la fine degli anni Sessanta e gli anni Settanta, le difficoltà incontrate nei programmi di traduzione automatica, i limiti dei primi modelli neurali e le valutazioni critiche contenute in rapporti istituzionali determinarono una riduzione degli investimenti. Ebbe così inizio il periodo comunemente definito “primo inverno dell'intelligenza artificiale”, durante il quale diminuirono l'interesse e i finanziamenti destinati al settore.¹⁰

Una nuova fase di sviluppo si aprì negli anni Ottanta con la diffusione dei sistemi esperti. Questi programmi erano progettati per riprodurre, in ambiti circoscritti, le conoscenze e i procedimenti decisionali di specialisti umani attraverso basi di conoscenza e regole del tipo “se-allora”. I sistemi esperti trovarono applicazione in settori quali la medicina, la geologia e la configurazione di apparecchiature informatiche, contribuendo a riaccendere l'interesse scientifico e commerciale nei confronti dell'IA.¹¹

Anche questa fase incontrò limiti significativi. La costruzione e l'aggiornamento delle basi di conoscenza richiedevano un'attività complessa e costosa, mentre i

⁹ Y. Jiang et al., «Quo vadis artificial intelligence?», cit., pp. 3-4; L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 17-18.

¹⁰ Y. Jiang et al., «Quo vadis artificial intelligence?», cit., p. 4; P.P. Groumpos, «A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities, and Threats», cit., pp. 184-185.

¹¹ L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 18-20.

sistemi mostravano una ridotta capacità di adattamento a situazioni non previste. Alla fine degli anni Ottanta il settore attraversò quindi un secondo periodo di contrazione, accompagnato dalla diminuzione degli investimenti e dal ridimensionamento delle aspettative.¹²

A partire dagli anni Novanta l'intelligenza artificiale riprese a svilupparsi grazie all'affermazione di metodologie statistiche e probabilistiche e ai progressi del *machine learning*. L'attenzione si spostò progressivamente dalla codificazione manuale delle conoscenze alla costruzione di sistemi capaci di ricavare regolarità e modelli dai dati. Lo sviluppo di tecniche quali alberi decisionali, macchine a vettori di supporto, metodi di insieme e reti neurali rese possibile affrontare problemi più complessi e applicazioni maggiormente aderenti ai contesti reali.¹³

La crescita più intensa si è verificata nel XXI secolo grazie alla convergenza di tre fattori: la disponibilità di grandi quantità di dati digitali, l'aumento della potenza di calcolo e il perfezionamento degli algoritmi. In questo contesto si è consolidato il *deep learning*, un insieme di tecniche basate su reti neurali articolate in più livelli, capaci di apprendere rappresentazioni progressivamente più complesse dei dati. Tali metodologie hanno prodotto risultati particolarmente significativi nel riconoscimento delle immagini, nell'elaborazione del linguaggio naturale, nella previsione e nella classificazione automatica.¹⁴

L'attuale fase di sviluppo rappresenta quindi l'esito di un percorso nel quale progressi teorici, disponibilità di dati e capacità computazionali si sono rafforzati reciprocamente. La storia dell'intelligenza artificiale mostra inoltre quanto il

¹² L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 19-20; Y. Jiang et al., «Quo vadis artificial intelligence?», cit., p. 4.

¹³ L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 20-21; Y. Jiang et al., «Quo vadis artificial intelligence?», cit., pp. 4-5.

¹⁴ L. Portinale, «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», cit., pp. 21-23; Y. Jiang et al., «Quo vadis artificial intelligence?», cit., pp. 5-8; P.P. Groumpos, «A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities, and Threats», cit., pp. 185-186.

progresso della disciplina sia stato condizionato dalla distanza tra le aspettative formulate e i risultati concretamente ottenuti. Questa evoluzione consente di comprendere meglio tanto l'attuale diffusione dell'IA quanto la necessità di valutarne con attenzione le possibilità e i limiti.

1.3 Principali tipologie e applicazioni dell'intelligenza artificiale

L'intelligenza artificiale non costituisce una tecnologia unitaria, ma comprende approcci, metodologie e sistemi differenti per struttura, modalità di apprendimento e funzione svolta. La distinzione tra le principali tipologie permette di comprendere meglio le capacità effettive delle applicazioni esistenti e di valutare le conseguenze che il loro utilizzo può produrre nei diversi contesti economici, sociali e istituzionali.

Una prima classificazione distingue tra intelligenza artificiale debole (*weak artificial intelligence*) e intelligenza artificiale forte (*strong artificial intelligence*). La prima comprende sistemi progettati per svolgere compiti specifici e circoscritti, come riconoscere immagini, tradurre testi, rispondere a domande o analizzare dati. Queste applicazioni possono raggiungere prestazioni elevate nell'ambito per il quale sono state sviluppate, ma non possiedono una capacità generale di comprensione e non trasferiscono autonomamente le competenze acquisite a contesti completamente differenti.

L'intelligenza artificiale forte indica invece una forma teorica di IA dotata di capacità cognitive generali comparabili a quelle umane, in grado di comprendere situazioni diverse, elaborare conoscenze e adattare il proprio comportamento a problemi non circoscritti a un singolo ambito. Una simile forma di intelligenza non è stata ancora realizzata: i sistemi attualmente utilizzati, compresi quelli generativi più avanzati, restano applicazioni specializzate, sebbene possano

eseguire una pluralità di attività e interagire attraverso modalità particolarmente flessibili.¹⁵

Tra le metodologie più importanti rientra il *machine learning* (ML), o apprendimento automatico. Esso comprende tecniche attraverso le quali un sistema ricava dai dati regolarità utilizzabili per classificare informazioni, formulare previsioni o sostenere decisioni, senza che ogni passaggio debba essere definito anticipatamente mediante istruzioni specifiche. Rispetto ai programmi tradizionali fondati prevalentemente su regole prestabilite, i modelli di apprendimento automatico vengono addestrati mediante esempi e modificano i propri parametri in funzione dei risultati ottenuti.¹⁶

Le principali modalità di apprendimento sono quella supervisionata, quella non supervisionata e l'apprendimento per rinforzo. Nell'apprendimento supervisionato il modello viene addestrato mediante dati associati al risultato atteso e impara a ricostruire la relazione tra gli elementi forniti in ingresso e la corrispondente uscita. Questa tecnica viene utilizzata, ad esempio, nella classificazione di immagini, nel riconoscimento di caratteri e nella previsione di valori.

Nell'apprendimento non supervisionato, invece, i dati non sono accompagnati da etichette o risultati prestabiliti. Il sistema ricerca autonomamente strutture, somiglianze e raggruppamenti presenti nelle informazioni, consentendo di individuare configurazioni che non erano state definite in anticipo. Ne costituiscono esempi la segmentazione di gruppi di utenti e il riconoscimento di anomalie all'interno di grandi insiemi di dati.¹⁷

¹⁵ Y. Jiang, X. Li, H. Luo, S. Yin, O. Kaynak, «Quo vadis artificial intelligence?», *Discover Artificial Intelligence*, vol. 2, art. 4, 2022, pp. 8-9, 13-15.

¹⁶ J. Kufel et al., «What Is Machine Learning, Artificial Neural Networks and Deep Learning? —Examples of Practical Applications in Medicine», *Diagnostics*, vol. 13, n. 15, 2023, articolo 2582, pp. 1-4.

¹⁷ Ivi, pp. 4-5.

L'apprendimento per rinforzo (*reinforcement learning*) si fonda sull'interazione tra un agente e l'ambiente nel quale esso opera. L'agente esegue determinate azioni e riceve segnali positivi o negativi in relazione ai risultati conseguiti, modificando progressivamente la propria strategia per massimizzare la ricompensa complessiva. Questa metodologia trova applicazione nella robotica, nella gestione di sistemi autonomi, nei giochi e in problemi decisionali caratterizzati da una successione di scelte.¹⁸

Una componente rilevante dell'apprendimento automatico è costituita dalle reti neurali artificiali, modelli formati da unità di elaborazione interconnesse e organizzate in livelli. La loro struttura trae ispirazione, in forma molto semplificata, dal funzionamento dei neuroni biologici, ma non riproduce il cervello umano né implica l'esistenza di processi cognitivi assimilabili a quelli delle persone. Durante l'addestramento, le connessioni tra le diverse unità vengono modificate affinché il modello riduca progressivamente la distanza tra il risultato prodotto e quello atteso.¹⁹

Il *deep learning*, o apprendimento profondo, utilizza reti neurali composte da più livelli di elaborazione. Questa architettura consente di ricavare progressivamente caratteristiche complesse a partire dai dati iniziali e si è dimostrata particolarmente efficace nel trattamento di immagini, testi, suoni e altre informazioni non strutturate. La sua diffusione è stata favorita dall'aumento della capacità computazionale, dalla disponibilità di grandi raccolte di dati e dal perfezionamento delle tecniche di addestramento.²⁰

Un ulteriore ambito è rappresentato dal *natural language processing* (NLP), o elaborazione del linguaggio naturale. Esso comprende tecniche dirette ad analizzare, rappresentare e generare il linguaggio utilizzato dalle persone. A

¹⁸ V. Kanade, «What Is Reinforcement Learning? Working, Algorithms, and Uses», *Spiceworks*, 2022.

¹⁹ J. Kufel et al., «What Is Machine Learning, Artificial Neural Networks and Deep Learning? —Examples of Practical Applications in Medicine», cit., pp. 8-11.

²⁰ Ivi, pp. 10-12; Y. Jiang et al., «Quo vadis artificial intelligence?», cit., pp. 4-8.

differenza dei linguaggi di programmazione, il linguaggio naturale presenta ambiguità, variazioni contestuali e sfumature semantiche che rendono particolarmente complessa la sua elaborazione automatica.²¹

Le applicazioni del NLP comprendono la traduzione automatica, la classificazione dei testi, l'analisi del contenuto e del sentimento espresso, la produzione di sintesi, la ricerca di informazioni in archivi documentali, gli assistenti virtuali e i chatbot. Le architetture neurali più recenti hanno migliorato la capacità dei sistemi di collegare parole e frasi al contesto complessivo, pur senza eliminare le difficoltà legate all'ironia, ai significati impliciti e alle specificità linguistiche.²²

Negli ultimi anni ha assunto particolare rilievo l'intelligenza artificiale generativa, costituita da sistemi in grado di produrre nuovi contenuti, come testi, immagini, suoni, video e codice informatico, sulla base delle strutture apprese durante l'addestramento. La generazione non deriva da una creatività o da una comprensione assimilabili a quelle umane, ma dall'elaborazione statistica delle informazioni e dalla costruzione di output coerenti con i modelli individuati nei dati.²³

Tra le principali tecnologie generative rientrano i modelli linguistici di grandi dimensioni (*large language models*, LLM), addestrati su ampie raccolte testuali per prevedere e generare sequenze linguistiche. Tali modelli possono rispondere a domande, redigere o sintetizzare testi, rielaborare documenti e sostenere attività di ricerca e comunicazione. La capacità di svolgere compiti diversi attraverso il linguaggio naturale ne ha favorito la rapida diffusione nelle imprese, nelle istituzioni e tra i cittadini. Questi sistemi non possiedono tuttavia una comprensione intrinseca dei contenuti elaborati e possono produrre informazioni

²¹ C. Negri, «Cos'è il Natural Language Processing (NLP) e come funziona», Osservatorio Artificial Intelligence, Politecnico di Milano.

²² Ivi.

²³ E. Frontoni, «Intelligenza Artificiale Generativa e creatività umana», *FOR*, n. 3, 2023, pp. 15-17.

inesatte o non adeguatamente fondate, rendendo necessaria una verifica umana dei risultati.²⁴

Le applicazioni dell'intelligenza artificiale interessano ormai numerosi settori. In ambito sanitario, i sistemi possono sostenere l'analisi delle immagini cliniche, la diagnosi e la previsione dell'evoluzione di determinate condizioni. Nel settore finanziario vengono utilizzati per individuare frodi, valutare rischi e analizzare operazioni. Nell'industria favoriscono il controllo della produzione, la manutenzione predittiva e l'ottimizzazione delle attività logistiche. Nel campo dei trasporti contribuiscono alla gestione della mobilità e allo sviluppo di funzioni automatizzate.²⁵

Altre applicazioni comprendono gli assistenti virtuali, i sistemi di raccomandazione, l'elaborazione intelligente dei dati, la visione artificiale e le soluzioni fisiche autonome. La classificazione proposta dall'Osservatorio *Artificial Intelligence* del Politecnico di Milano mostra come le diverse tecnologie possano essere distinte in relazione alla finalità concretamente perseguita, mentre l'intelligenza artificiale generativa assume un carattere trasversale e può essere integrata in numerose categorie applicative.²⁶

Anche la Pubblica Amministrazione può impiegare sistemi di IA per elaborare documenti, assistere gli utenti, automatizzare attività ripetitive, analizzare grandi quantità di dati e supportare determinate fasi dei procedimenti. Questi utilizzi non costituiscono però una categoria tecnologica autonoma, poiché possono fondarsi su NLP, modelli predittivi, sistemi di classificazione, chatbot o strumenti generativi. La distinzione tra le diverse tipologie assume quindi rilievo anche sul piano giuridico e organizzativo, dal momento che capacità, rischi e possibilità di

²⁴ Ivi, pp. 15-17; C. Negri, «Cos'è il Natural Language Processing (NLP) e come funziona», cit.

²⁵ C. Sorrentino, «Le applicazioni dell'Intelligenza Artificiale e la loro diffusione», Osservatorio Artificial Intelligence, Politecnico di Milano; J. Kufel et al., «What Is Machine Learning, Artificial Neural Networks and Deep Learning? — Examples of Practical Applications in Medicine», cit., pp. 11-15.

²⁶ C. Sorrentino, «Le applicazioni dell'Intelligenza Artificiale e la loro diffusione», cit.

controllo variano in relazione alla tecnica impiegata e alla funzione concretamente attribuita al sistema.

La varietà delle metodologie e delle applicazioni dimostra il carattere trasversale dell'intelligenza artificiale. La sua diffusione può produrre benefici rilevanti, ma solleva anche questioni connesse all'affidabilità dei risultati, alla protezione dei dati, alla trasparenza e alla responsabilità.

1.4 Opportunità e rischi dell'intelligenza artificiale

La crescente diffusione dell'intelligenza artificiale nei contesti economici, sociali e istituzionali ha alimentato un ampio dibattito sulle opportunità offerte da tali tecnologie e sui rischi connessi al loro impiego. I sistemi di IA possono elaborare grandi quantità di informazioni, individuare regolarità difficilmente riconoscibili attraverso il solo intervento umano e svolgere determinate operazioni con rapidità. Le medesime caratteristiche possono però produrre conseguenze problematiche quando i sistemi operano sulla base di dati inadeguati, risultano poco comprensibili o vengono utilizzati in ambiti nei quali incidono sui diritti e sulle condizioni di vita delle persone.

Una prima opportunità riguarda la capacità di sostenere l'analisi e l'assunzione delle decisioni. I sistemi di apprendimento automatico possono esaminare insiemi estesi di dati, riconoscere anomalie e formulare previsioni utili in settori quali la medicina, la finanza, la produzione industriale e la gestione della mobilità. Il valore di tali strumenti non deriva dalla sostituzione automatica del giudizio umano, ma dalla possibilità di mettere a disposizione informazioni ulteriori, rendere più tempestiva l'individuazione dei problemi e migliorare la conoscenza del contesto nel quale occorre intervenire.

L'automazione può inoltre semplificare lo svolgimento di attività ripetitive, standardizzate o caratterizzate dall'elaborazione di numerose informazioni. In

questi casi l'intelligenza artificiale permette di ridurre i tempi necessari per alcune operazioni e di destinare le competenze umane ad attività che richiedono interpretazione, capacità relazionali, conoscenza del contesto e assunzione di responsabilità. L'effettivo beneficio dipende tuttavia dalle modalità con cui la tecnologia viene integrata nell'organizzazione e dalla permanenza di un controllo umano adeguato.²⁷

L'elaborazione dei dati può contribuire anche al miglioramento e alla personalizzazione di prodotti e servizi. L'analisi delle caratteristiche e delle esigenze degli utenti consente di adattare determinate prestazioni, individuare bisogni emergenti e distribuire le risorse in modo più consapevole. Tale possibilità assume particolare rilievo nei contesti nei quali la tempestività della risposta e la capacità di riconoscere situazioni specifiche incidono sulla qualità del servizio offerto.

Questi vantaggi non consentono però di considerare l'intelligenza artificiale come uno strumento neutrale o infallibile. Il funzionamento di un sistema dipende dalle scelte compiute durante la progettazione, dagli obiettivi assegnati, dalle variabili selezionate e dai dati utilizzati per l'addestramento. Anche un risultato tecnicamente coerente con il modello può quindi produrre effetti ingiusti o inadeguati rispetto al contesto sociale e giuridico nel quale viene impiegato.²⁸

Una prima criticità riguarda l'opacità di alcuni sistemi, in particolare dei modelli fondati su tecniche di apprendimento profondo. La complessità delle elaborazioni può rendere difficile ricostruire il percorso che ha condotto a un determinato risultato. La conoscenza dell'output non è infatti sempre accompagnata dalla comprensione degli elementi che hanno inciso sulla sua produzione. Ciò può

²⁷ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», *Discover Artificial Intelligence*, vol. 4, 2024, pp. 1-18; E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», *CERIDAP*, n. 2, 2023, pp. 66-84.

²⁸ D. Tafani, «L'«etica» come specchio per le allodole. Sistemi di intelligenza artificiale e violazioni dei diritti», *Bollettino telematico di filosofia politica*, 2023, pp. 1-13.

ostacolare l'individuazione degli errori, limitare la possibilità di contestare una decisione e rendere più complessa l'attribuzione delle responsabilità.

Per affrontare questo problema si è sviluppata l'intelligenza artificiale spiegabile (*Explainable Artificial Intelligence*, XAI), che comprende metodi diretti a rendere il comportamento dei sistemi maggiormente intelligibile. Una spiegazione efficace non deve limitarsi a descrivere in termini tecnici il modello, ma deve fornire informazioni comprensibili e pertinenti rispetto alle esigenze del destinatario. Sviluppatori, operatori, decisori pubblici e persone interessate da una decisione possono infatti necessitare di spiegazioni differenti. La spiegabilità assume particolare rilievo quando l'IA viene utilizzata in ambiti nei quali il risultato può incidere sulla salute, sull'accesso al lavoro, al credito, ai servizi o sull'esercizio di diritti fondamentali.²⁹

Un secondo rischio è costituito dalle distorsioni algoritmiche. I sistemi di apprendimento automatico individuano regolarità nei dati disponibili e possono riprodurre o amplificare disuguaglianze presenti nelle informazioni di partenza. La scarsa rappresentatività dei dati, l'utilizzo di variabili indirettamente collegate a caratteristiche protette e la tendenza a ricavare valutazioni individuali da comportamenti osservati in gruppi considerati simili possono determinare trattamenti sfavorevoli nei confronti di determinate persone.

La discriminazione non deriva necessariamente da un'intenzione esplicita del progettista. Può essere incorporata nel modo in cui il problema viene definito, nelle categorie utilizzate, nei dati storici o negli indicatori scelti come sostituti di elementi difficilmente misurabili. L'apparente oggettività del risultato algoritmico può inoltre rendere meno visibili tali distorsioni e attribuire loro un'autorità che non corrisponde alla reale affidabilità del sistema. Per questa ragione, l'impiego dell'IA in processi valutativi richiede verifiche sulla qualità

²⁹ D. Gunning, M. Stefik, J. Choi, T. Miller, S. Stumpf, G.-Z. Yang, «XAI—Explainable Artificial Intelligence», *Science Robotics*, vol. 4, n. 37, 2019, articolo eaay7120, pp. 1-5.

dei dati, controlli periodici sugli effetti prodotti e la possibilità di riesaminare concretamente il risultato.³⁰

La protezione dei dati personali costituisce un'altra questione centrale. Molti sistemi richiedono la raccolta e l'elaborazione di quantità rilevanti di informazioni, talvolta riferite ad aspetti sensibili della vita degli individui. L'integrazione di dati provenienti da fonti diverse può consentire di ricavare informazioni ulteriori rispetto a quelle originariamente fornite e aumentare il rischio di profilazioni invasive, accessi non autorizzati e utilizzi incompatibili con le finalità iniziali.

Il ricorso ai dati deve quindi essere limitato a quanto effettivamente necessario, accompagnato da misure di sicurezza e sottoposto a controlli sull'esattezza e sulla pertinenza delle informazioni. La protezione degli interessati non riguarda soltanto la riservatezza, ma anche la possibilità di comprendere come i dati vengano impiegati e di contestare gli effetti derivanti dal loro trattamento.³¹

L'impiego dell'intelligenza artificiale pone inoltre il problema della responsabilità. Lo sviluppo, la commercializzazione e l'utilizzo di un sistema coinvolgono spesso una pluralità di soggetti, tra cui progettisti, programmatori, fornitori, proprietari dei dati, organizzazioni utilizzatrici e operatori umani. Quando il sistema causa un danno, può risultare complesso individuare quale condotta abbia contribuito all'evento e quale soggetto fosse nella posizione più adeguata a prevenirlo o limitarne le conseguenze.

La complessità tecnica e l'opacità dei processi non devono tuttavia trasformarsi in una riduzione della tutela per la persona danneggiata. La distribuzione delle responsabilità deve riflettere il ruolo effettivamente svolto dai diversi soggetti e la loro capacità di incidere sulla progettazione, sul controllo e sull'impiego del

³⁰ D. Tafani, «L'«etica» come specchietto per le allodole», cit., pp. 3-7; E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 71-76.

³¹ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 71-76.

sistema. L'autonomia operativa dell'IA non comporta infatti l'autonomia giuridica della macchina né elimina la necessità di imputare le conseguenze delle decisioni a soggetti umani o organizzazioni.³²

Ulteriori interrogativi riguardano l'impatto dell'automazione sul lavoro. Alcune mansioni possono essere parzialmente sostituite o profondamente trasformate, soprattutto quando consistono in operazioni ripetitive e standardizzabili. Parallelamente, aumentano la richiesta di competenze digitali e la necessità di figure capaci di progettare, valutare, utilizzare e controllare i sistemi. L'effetto dell'IA non coincide quindi con una semplice riduzione dell'occupazione, ma comporta una redistribuzione dei compiti e una trasformazione delle professionalità.

La transizione richiede investimenti nella formazione e nella riqualificazione, affinché l'innovazione non accresca le disuguaglianze tra lavoratori dotati di competenze adeguate e soggetti maggiormente esposti alla sostituzione o all'esclusione. È inoltre necessario evitare che l'automazione riduca gli spazi di autonomia professionale o induca gli operatori ad affidarsi passivamente ai risultati prodotti dai sistemi.³³

Accanto ai rischi individuali devono essere considerate le conseguenze collettive. Lo sviluppo e il funzionamento dei modelli più complessi richiedono infrastrutture, energia e risorse materiali, con possibili effetti ambientali. La crescente concentrazione di dati, capacità computazionale e competenze nelle mani di pochi soggetti può inoltre determinare forme di dipendenza tecnologica e squilibri di potere. Una valutazione completa dell'intelligenza artificiale deve

³² G. D'Alfonso, «Intelligenza artificiale e responsabilità civile. Prospettive europee», *Revista de Estudios Jurídicos y Criminológicos*, n. 6, 2022, pp. 163-195, in particolare pp. 164-168.

³³ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 71-79; K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit.

quindi considerare non soltanto le prestazioni immediate del sistema, ma anche i costi sociali, organizzativi e ambientali che accompagnano il suo ciclo di vita.³⁴

L'intelligenza artificiale presenta, nel complesso, una duplice dimensione. Può contribuire a migliorare la conoscenza dei fenomeni, rendere più efficienti alcune attività e ampliare le capacità di intervento delle organizzazioni. Le stesse tecnologie possono però produrre opacità, discriminazioni, interferenze nella vita privata, difficoltà nell'attribuzione delle responsabilità e nuove forme di disuguaglianza. Il valore dell'innovazione dipende pertanto dalle finalità perseguite, dalla qualità della progettazione, dalla proporzionalità del suo utilizzo e dalla presenza di garanzie adeguate.

Questa esigenza assume particolare rilievo nel settore pubblico, nel quale l'efficienza non può essere perseguita separatamente dalla trasparenza, dall'imparzialità e dalla tutela dei cittadini. L'intelligenza artificiale deve rimanere uno strumento al servizio dell'interesse generale e non può determinare una riduzione delle garanzie proprie dell'azione amministrativa.³⁵

³⁴ D. Tafani, «L'«etica» come specchietto per le allodole», cit., pp. 1-8.

³⁵ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 66-84.

CAPITOLO 2

L'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE

2.1 La trasformazione digitale della Pubblica Amministrazione

La trasformazione digitale della Pubblica Amministrazione rappresenta uno dei principali processi di innovazione che hanno interessato il settore pubblico negli ultimi decenni. Tale fenomeno non consiste semplicemente nell'introduzione di nuove tecnologie all'interno delle amministrazioni, ma implica una profonda revisione dei modelli organizzativi, dei processi decisionali e delle modalità di erogazione dei servizi pubblici. La digitalizzazione costituisce uno strumento strategico volto a rendere l'azione amministrativa più efficiente, trasparente, accessibile e orientata alle esigenze di cittadini e imprese. L'evoluzione tecnologica della Pubblica Amministrazione può essere rappresentata attraverso una scansione in diverse fasi. Il modello della Pubblica Amministrazione 1.0 corrisponde a un'amministrazione fondata prevalentemente su documenti cartacei, procedure manuali e strumenti tradizionali. La fase successiva, definita Pubblica Amministrazione 2.0, è caratterizzata dall'introduzione delle tecnologie informatiche nei processi interni e dalla progressiva digitalizzazione delle attività amministrative. Con la diffusione di Internet, dei portali istituzionali e dei servizi telematici si afferma il modello della Pubblica Amministrazione 3.0, maggiormente orientato all'interazione digitale con cittadini e imprese. La nozione di Pubblica Amministrazione 4.0 indica, infine, una fase contraddistinta dalla valorizzazione dei dati, dall'interconnessione dei sistemi informativi e dall'impiego di tecnologie avanzate, tra cui l'intelligenza artificiale. Tale classificazione non costituisce una periodizzazione normativa ufficiale, ma uno schema interpretativo utile a descrivere il passaggio da un'amministrazione

prevalentemente analogica a un modello digitale, interconnesso e orientato ai dati.³⁶ La diffusione delle tecnologie digitali ha modificato profondamente il rapporto tra amministrazioni pubbliche, cittadini e imprese. L'impiego di strumenti quali l'identità digitale, la posta elettronica certificata, il domicilio digitale, le firme elettroniche e i sistemi di pagamento informatici ha contribuito all'affermazione della cittadinanza digitale, intesa come l'insieme dei diritti e delle possibilità di accesso ai servizi pubblici mediante strumenti telematici. La digitalizzazione non rappresenta quindi soltanto un cambiamento tecnologico, ma anche una trasformazione culturale finalizzata a semplificare le relazioni tra amministrazione e utenti, garantendo un accesso più rapido ed efficace ai servizi pubblici.³⁷ Nel contesto italiano, il principale riferimento normativo in materia è rappresentato dal Codice dell'Amministrazione Digitale (CAD), introdotto con il Decreto Legislativo n. 82 del 2005 e successivamente aggiornato nel corso degli anni. Il CAD costituisce il fondamento giuridico della digitalizzazione della PA, definendo diritti, strumenti e principi finalizzati alla progressiva innovazione dell'azione amministrativa. Attraverso tale normativa è stato promosso un modello amministrativo basato sulla dematerializzazione dei documenti, sulla gestione digitale dei procedimenti e sull'impiego di strumenti tecnologici finalizzati a migliorare l'efficienza, la trasparenza e la semplificazione dell'azione amministrativa.³⁸ Il quadro normativo promuove l'utilizzo delle tecnologie digitali come modalità ordinaria di organizzazione dell'attività amministrativa e di erogazione dei servizi pubblici. Tale impostazione non si limita alla semplice trasposizione in formato elettronico delle procedure esistenti, ma richiede una revisione complessiva dei processi, finalizzata a semplificare le

³⁶ D.-U. Galetta, J.G. Corvalán, «Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto», *Federalismi.it*, n. 3, 2019, pp. 1-23.

³⁷ Agenzia per l'Italia Digitale, *Guida dei diritti di cittadinanza digitali*.

³⁸ Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'Amministrazione Digitale*; F.F. Pagano, «Pubblica amministrazione e innovazione tecnologica», *Gruppo di Pisa*, n. 3, 2021, pp. 84-112.

attività, migliorare l'accessibilità dei servizi e rendere più efficace il rapporto tra amministrazioni. Parallelamente all'evoluzione normativa, negli ultimi anni sono state elaborate strategie nazionali finalizzate ad accelerare la transizione digitale del settore pubblico. Un ruolo centrale è svolto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione, predisposto dall'Agenzia per l'Italia Digitale (AgID), che individua obiettivi, strumenti e linee di intervento per guidare l'innovazione delle amministrazioni italiane. Il Piano promuove un ecosistema digitale integrato fondato sulla diffusione di piattaforme nazionali, sulla valorizzazione dei dati pubblici, sul rafforzamento delle competenze digitali e sul miglioramento della qualità dei servizi erogati ai cittadini. Un elemento essenziale della transizione digitale è rappresentato dal principio di interoperabilità, ossia dalla capacità dei sistemi informativi delle diverse amministrazioni di comunicare, condividere dati e cooperare in maniera efficace. A tal fine, AgID ha elaborato specifiche Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni, che individuano standard, tecnologie e modalità operative finalizzate al coordinamento informativo e informatico tra enti pubblici. In tale prospettiva assume particolare rilevanza la Piattaforma Digitale Nazionale Dati (PDND), introdotta per favorire lo scambio sicuro e standardizzato delle informazioni tra amministrazioni. La piattaforma costituisce uno strumento centrale per l'attuazione del principio *once only*, secondo cui le amministrazioni dovrebbero evitare di richiedere a cittadini e imprese informazioni già in possesso del settore pubblico.³⁹ La condivisione dei dati attraverso infrastrutture interoperabili può contribuire a semplificare i procedimenti, ridurre gli oneri amministrativi e migliorare la capacità degli enti di cooperare nell'erogazione dei servizi. La valorizzazione del patrimonio informativo pubblico costituisce inoltre uno degli aspetti centrali della

³⁹ Agenzia per l'Italia Digitale, *Linee guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati*, versione 2.0, 19 giugno 2025.

trasformazione digitale. La disponibilità di dati affidabili, aggiornati e interoperabili costituisce il presupposto per un'efficace data governance, intesa come gestione strategica delle informazioni pubbliche orientata al supporto dei processi decisionali, al miglioramento dei servizi e allo sviluppo di soluzioni innovative. Un ulteriore impulso alla modernizzazione della PA è stato fornito dal Piano Nazionale di Ripresa e Resilienza (PNRR). Nell'ambito della Missione 1, Componente 1, il Piano individua la digitalizzazione della Pubblica Amministrazione come una priorità strategica per la modernizzazione del Paese. Gli interventi previsti comprendono il rafforzamento delle infrastrutture digitali, la migrazione al cloud, l'ampliamento dei servizi digitali, il miglioramento dell'interoperabilità tra amministrazioni e il potenziamento della sicurezza informatica.⁴⁰ La migrazione verso infrastrutture cloud rappresenta uno dei pilastri della strategia nazionale di innovazione. L'adozione di soluzioni cloud qualificate può favorire una maggiore affidabilità, scalabilità e continuità operativa dei sistemi informativi pubblici, oltre a consentire una gestione più flessibile delle risorse tecnologiche. Tali benefici dipendono però dalla qualità delle infrastrutture adottate, dall'adeguatezza delle misure di sicurezza e dalla capacità delle amministrazioni di governare correttamente il processo di migrazione. Accanto agli investimenti tecnologici, il PNRR attribuisce rilievo alla semplificazione amministrativa e allo sviluppo delle competenze digitali del personale pubblico. La transizione richiede capacità tecniche, gestionali e organizzative che consentano alle amministrazioni di governare l'innovazione, valutarne gli effetti e integrare le nuove tecnologie nei processi esistenti. In questa prospettiva, AgID ha promosso iniziative dedicate alle competenze di e-leadership, necessarie per orientare il cambiamento e trasformare gli investimenti

⁴⁰ Presidenza del Consiglio dei ministri, *Piano Nazionale di Ripresa e Resilienza*, Missione 1, Componente 1, «Digitalizzazione, innovazione e sicurezza nella PA».

digitali in risultati concreti per cittadini e imprese.⁴¹ La trasformazione digitale della Pubblica Amministrazione costituisce un processo multidimensionale, nel quale si intrecciano profili tecnologici, organizzativi, normativi e culturali. Infrastrutture adeguate, interoperabilità, gestione strategica dei dati, competenze professionali e riprogettazione dei servizi rappresentano condizioni essenziali per lo sviluppo di un'amministrazione capace di operare nella società digitale.

2.2 L'utilizzo dell'intelligenza artificiale nei servizi pubblici

L'intelligenza artificiale sta assumendo un ruolo crescente nei processi di innovazione della Pubblica Amministrazione. La disponibilità di dati pubblici, l'evoluzione delle infrastrutture informatiche e lo sviluppo di strumenti avanzati di elaborazione hanno favorito l'introduzione di sistemi di IA in diversi ambiti dell'azione amministrativa. Il loro impiego comprende l'automazione di operazioni standardizzate, l'assistenza agli utenti, l'analisi delle informazioni e il supporto alle attività di pianificazione e controllo.⁴² L'intelligenza artificiale si inserisce quindi nel più ampio processo di trasformazione digitale del settore pubblico, sviluppato attraverso l'integrazione tra dati, piattaforme e servizi.

Una delle applicazioni più diffuse riguarda l'automazione dei processi amministrativi. Attraverso sistemi di elaborazione automatica delle informazioni, le amministrazioni possono gestire attività ripetitive e standardizzate, quali l'archiviazione documentale, la classificazione delle pratiche, la verifica dei dati e lo smistamento delle richieste degli utenti. Un ulteriore ambito di applicazione è rappresentato dall'assistenza ai cittadini mediante chatbot e assistenti virtuali basati su tecniche di Natural Language Processing. Questi sistemi possono

⁴¹ Agenzia per l'Italia Digitale, *Competenze di E-Leadership per gestire la transizione digitale della PA. Un quadro aggiornato di riferimento per le amministrazioni pubbliche*, luglio 2025.

⁴² E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», *CERIDAP*, n. 2, 2023, pp. 71-78; K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», *Discover Artificial Intelligence*, vol. 4, 2024, articolo 18, pp. 1-18.

rispondere alle domande più frequenti, fornire indicazioni sui procedimenti e guidare gli utenti nella consultazione delle informazioni e nella gestione delle pratiche amministrative. Tali strumenti possono facilitare l'accesso ai servizi digitali e alle informazioni amministrative.⁴³ L'intelligenza artificiale trova inoltre applicazione nell'analisi dei dati e nel supporto alle decisioni pubbliche. Le amministrazioni raccolgono quotidianamente grandi quantità di informazioni provenienti da archivi, banche dati e sistemi informativi. Attraverso tecniche di *machine learning* e analisi predittiva, le informazioni raccolte dalle amministrazioni possono essere elaborate per individuare tendenze, anomalie e possibili scenari evolutivi. Tali strumenti vengono impiegati a supporto delle attività di analisi, pianificazione e valutazione.⁴⁴

In Italia, un esempio significativo è rappresentato dall'INPS, che ha introdotto diverse soluzioni basate sull'intelligenza artificiale nei propri servizi. Nell'ambito del Sistema Informativo per l'Inclusione Sociale e Lavorativa (SIISL), piattaforma istituita presso il Ministero del Lavoro e delle Politiche Sociali e gestita dall'Istituto, l'IA viene utilizzata per favorire l'incontro tra domanda e offerta di lavoro. Il sistema elabora un indice di affinità tra i profili professionali degli utenti e le opportunità lavorative o formative presenti nella piattaforma, supportando l'individuazione delle proposte maggiormente coerenti con le competenze dichiarate. L'esperienza del SIISL costituisce quindi un esempio di applicazione dell'intelligenza artificiale nell'ambito delle politiche attive del lavoro.⁴⁵

⁴³ C. Negri, «Cos'è il Natural Language Processing (NLP) e come funziona», Osservatorio Artificial Intelligence, Politecnico di Milano; E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., p. 77.

⁴⁴ M.S. Agba, G.E.M. Agba, A.W. Obeten, «Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies», *Journal of Public Administration, Policy and Governance Research*, vol. 1, n. 2, 2023, pp. 4-8; K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 1-7.

⁴⁵ INPS, Messaggio 5 aprile 2024, n. 1358, «SIISL – L'Intelligenza Artificiale a supporto dell'incrocio tra domanda e offerta di lavoro», pp. 1-2.

Un ulteriore ambito di applicazione riguarda le attività di controllo e vigilanza. I sistemi di IA possono essere utilizzati per analizzare flussi informativi, individuare anomalie e segnalare situazioni meritevoli di approfondimento da parte degli uffici competenti. Tali strumenti trovano impiego, ad esempio, nella classificazione delle segnalazioni, nella programmazione dei controlli e nell'individuazione di possibili irregolarità o fenomeni fraudolenti. Il risultato prodotto dal sistema non sostituisce necessariamente la valutazione dell'amministrazione, ma può orientare le successive attività di verifica.⁴⁶

Le applicazioni dell'IA si estendono inoltre a numerosi settori specifici dell'azione pubblica. In ambito sanitario, tali tecnologie possono essere impiegate nell'analisi dei dati clinici, nella gestione dei flussi assistenziali e nel supporto alla diagnostica. Un settore particolarmente rilevante è quello della diagnostica per immagini, nel quale i sistemi di IA elaborano radiografie, tomografie computerizzate e risonanze magnetiche allo scopo di segnalare caratteristiche o anomalie meritevoli di attenzione. Questi strumenti possono assistere i professionisti sanitari nell'interpretazione delle immagini e nella valutazione delle informazioni disponibili, senza sostituire la responsabilità clinica del medico. Ulteriori applicazioni riguardano la stima del rischio, il supporto alla formulazione delle prognosi e l'organizzazione delle risorse sanitarie.⁴⁷

Nel settore della mobilità, l'IA può essere applicata all'elaborazione in tempo reale dei dati provenienti da sensori e infrastrutture digitali, con funzioni di monitoraggio dei flussi di traffico e supporto alla gestione dei trasporti. A livello locale, strumenti analoghi possono essere impiegati nell'analisi dei fenomeni urbani, nella pianificazione territoriale e nella programmazione degli interventi.

⁴⁶ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 73-78; M.S. Agba, G.E.M. Agba, A.W. Obeten, «Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies», cit., pp. 5-6.

⁴⁷ Ministero della Salute, Consiglio Superiore di Sanità, *I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*, 9 novembre 2021, pp. 3-12, in particolare pp. 5-7.

Altre sperimentazioni riguardano le politiche sociali, l'istruzione, la sicurezza e la tutela ambientale, ambiti nei quali l'elaborazione automatizzata delle informazioni può affiancare le attività conoscitive e organizzative delle amministrazioni.⁴⁸

Le applicazioni descritte mostrano come l'intelligenza artificiale possa essere impiegata in ambiti molto diversi dell'azione pubblica, dall'organizzazione interna degli uffici all'erogazione dei servizi, fino alle attività di analisi, controllo e programmazione. La diffusione di tali strumenti non produce però soltanto effetti operativi, ma incide anche sulla qualità dell'azione amministrativa e sul rapporto tra istituzioni e cittadini. I principali benefici derivanti dal loro utilizzo saranno esaminati nel paragrafo successivo.

2.3 Benefici dell'IA per la PA

L'impiego dell'intelligenza artificiale nella Pubblica Amministrazione può generare benefici che riguardano l'efficienza organizzativa, la qualità delle decisioni e l'accessibilità dei servizi. Dopo aver esaminato i principali ambiti applicativi, è quindi necessario valutare in che modo tali strumenti possano incidere concretamente sul funzionamento delle amministrazioni e sul rapporto con cittadini e imprese. Uno dei principali vantaggi riguarda l'efficienza amministrativa. Numerose attività svolte dagli uffici pubblici hanno carattere ripetitivo e standardizzato, come la classificazione dei documenti, lo smistamento delle pratiche, la verifica delle informazioni e la gestione delle richieste più semplici. L'impiego di sistemi automatizzati permette di eseguire tali operazioni con maggiore rapidità e uniformità, alleggerendo il carico di lavoro del personale. I dipendenti possono così concentrarsi su compiti più complessi, nei quali

⁴⁸ L. Floridi, «Artificial Intelligence as a Public Service: Learning from Amsterdam and Helsinki», *Philosophy & Technology*, vol. 33, 2020, pp. 541-546; M.S. Agba, G.E.M. Agba, A.W. Obeten, «Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies», cit., pp. 6-8.

risultano indispensabili capacità interpretative, valutazioni discrezionali e interazione diretta con gli utenti.⁴⁹

La semplificazione dei processi può comportare anche un contenimento dei costi di funzionamento. La riduzione dei tempi di lavorazione, degli errori e delle attività manuali consente di impiegare in modo più razionale le risorse economiche e professionali disponibili. Il risparmio ottenuto non dovrebbe tradursi esclusivamente in una diminuzione della spesa, ma essere destinato al potenziamento delle prestazioni offerte. Il Piano Triennale per l'informatica nella Pubblica Amministrazione collega l'automazione dei compiti ripetitivi al recupero di risorse da utilizzare per servizi di qualità superiore e per lo sviluppo di forme di assistenza proattiva.⁵⁰ Un secondo beneficio deriva dalla capacità dei sistemi di IA di analizzare patrimoni informativi molto estesi. Le amministrazioni dispongono di dati provenienti da archivi, banche dati, piattaforme digitali e procedimenti amministrativi, che possono essere elaborati attraverso tecniche di *machine learning* e analisi predittiva. Ciò consente di riconoscere tendenze, anticipare l'emergere di determinati fenomeni e fornire ai decisori pubblici elementi utili per programmare gli interventi, monitorarne gli effetti e definire con maggiore precisione le priorità.⁵¹ In settori quali la sanità, le politiche sociali, la mobilità e la gestione del territorio, questa capacità può tradursi in una distribuzione più consapevole di risorse, mezzi e personale. L'individuazione tempestiva delle aree maggiormente esposte a criticità permette di indirizzare gli

⁴⁹ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», *Discover Artificial Intelligence*, vol. 4, 2024, articolo 18, pp. 1-18; E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», *CERIDAP*, n. 2, 2023, pp. 71-78.

⁵⁰ Agenzia per l'Italia Digitale, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*, 2026, sezione dedicata all'intelligenza artificiale nella Pubblica Amministrazione.

⁵¹ M.S. Agba, G.E.M. Agba, A.W. Obeten, «Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies», *Journal of Public Administration, Policy and Governance Research*, vol. 1, n. 2, 2023, pp. 4-8; K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 1-18.

interventi verso i contesti nei quali risultano più necessari, riducendo sprechi e ritardi.

I vantaggi dell'intelligenza artificiale riguardano inoltre il rapporto tra amministrazione e utenti. Chatbot e assistenti virtuali possono fornire informazioni anche al di fuori degli orari di apertura degli uffici, accompagnare i cittadini nella compilazione delle domande e aiutarli a individuare il procedimento o il servizio più adatto.⁵² In questo modo si riducono i tempi di attesa, gli accessi agli sportelli e le difficoltà legate alla ricerca delle informazioni. Un ulteriore beneficio consiste nella possibilità di sviluppare servizi maggiormente proattivi. Attraverso l'analisi delle informazioni già disponibili, l'amministrazione può individuare in anticipo condizioni rilevanti per l'accesso a determinate prestazioni e segnalare al cittadino opportunità compatibili con la sua situazione. In questo modo l'erogazione del servizio non dipende esclusivamente dalla capacità dell'utente di conoscere tutte le misure esistenti e di attivarsi autonomamente. Una relazione più semplice e tempestiva con gli uffici può contribuire a migliorare la percezione dell'azione amministrativa. Servizi accessibili, comprensibili e coerenti con le esigenze degli utenti rafforzano la capacità dell'ente di produrre valore pubblico, poiché l'innovazione non si esaurisce nell'ottimizzazione dei processi interni, ma si traduce in risultati concretamente utili per la collettività.⁵³ I benefici descritti dipendono dalle condizioni nelle quali le tecnologie vengono adottate. La qualità dei dati, la presenza di competenze adeguate e la corretta progettazione dei sistemi sono elementi indispensabili affinché l'IA possa sostenere l'azione amministrativa senza generare conseguenze negative. L'innovazione deve quindi

⁵² E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico», cit., pp. 76-78.

⁵³ C. Van Noordt, L. Tangi, «The dynamics of AI capability and its influence on public value creation of AI within public administration», *Government Information Quarterly*, vol. 40, 2023, pp. 1-14.

essere accompagnata da meccanismi di controllo finalizzati ad assicurare trasparenza, imparzialità e tutela dei diritti.

2.4 Criticità e limiti dell'utilizzo dell'IA nella PA

L'impiego dell'intelligenza artificiale nella Pubblica Amministrazione, pur offrendo opportunità rilevanti in termini di efficienza, capacità di analisi e qualità dei servizi, presenta criticità che incidono direttamente sulla legittimità e sull'affidabilità dell'azione amministrativa. L'adozione di sistemi algoritmici non costituisce un processo meramente tecnico, poiché le scelte relative ai dati utilizzati, agli obiettivi assegnati e ai criteri di elaborazione possono produrre effetti concreti sulla posizione dei cittadini. La valutazione dei benefici deve quindi essere accompagnata dall'esame dei rischi connessi alla qualità delle informazioni, alla trasparenza dei procedimenti, alla tutela dei diritti e alla capacità delle amministrazioni di mantenere un controllo effettivo sulle tecnologie impiegate.

Una prima criticità riguarda la qualità dei dati utilizzati per addestrare e alimentare i sistemi di intelligenza artificiale. Le prestazioni di un modello dipendono dalla completezza, dall'attendibilità e dalla rappresentatività delle informazioni sulle quali esso opera. Dati inesatti, incompleti o non aggiornati possono condurre a risultati errati anche quando il funzionamento tecnico del sistema appare corretto.⁵⁴ Problemi analoghi emergono quando le informazioni vengono riutilizzate per finalità diverse da quelle originarie oppure derivano esclusivamente da comportamenti passati, senza considerare l'evoluzione del contesto sociale ed economico.

⁵⁴ N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi*, in «BioLaw Journal – Rivista di BioDiritto», n. 2, 2022, pp. 475-476

Rangone evidenzia come le distorsioni possano dipendere da dati raccolti da soggetti portatori di interessi, da presunzioni non verificate, da informazioni storiche o da tracce lasciate dagli utenti in rete. Un sistema apparentemente preciso durante la fase di sperimentazione può rivelarsi inadeguato una volta applicato a situazioni reali, caratterizzate da una maggiore varietà di casi e circostanze. La raccolta, la selezione e la gestione del patrimonio informativo non rappresentano pertanto attività preliminari di importanza secondaria, ma costituiscono elementi determinanti per la correttezza dell'intero processo amministrativo.

La presenza di dati distorti può generare bias algoritmici, ossia deviazioni sistematiche nei risultati, e produrre trattamenti discriminatori. I sistemi di IA apprendono dalle informazioni ricevute e possono riprodurre, consolidare o amplificare disuguaglianze già presenti nella società. Se un modello viene addestrato su decisioni storicamente influenzate da pregiudizi, i suoi risultati potrebbero conservare le medesime distorsioni, pur assumendo l'apparenza di valutazioni neutrali e oggettive. L'automazione non elimina necessariamente la componente soggettiva, ma può trasferirla nelle variabili selezionate, nei criteri di classificazione e negli obiettivi attribuiti al sistema.⁵⁵

Il rischio assume particolare rilevanza quando l'IA viene impiegata per individuare i soggetti da sottoporre a controllo, distribuire prestazioni sociali, valutare domande o stabilire priorità di intervento. L'utilizzo prevalente di dati storici nel settore della sicurezza urbana, ad esempio, può concentrare l'attenzione su determinate aree o categorie di persone, riproducendo modelli di controllo già esistenti e rendendo meno agevole l'individuazione di fenomeni nuovi. Rangone osserva che tali applicazioni possono rafforzare pregiudizi associati a particolari territori e incidere indirettamente sulle persone che vi

⁵⁵ N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni*, cit., pp. 475-476.

abitano.⁵⁶ La neutralità dell'algoritmo non può dunque essere presunta, ma deve essere verificata mediante controlli periodici sui dati, sui risultati e sugli effetti prodotti nei confronti dei diversi gruppi sociali.

Un ulteriore limite è rappresentato dall'opacità dei sistemi algoritmici. Nei procedimenti amministrativi, la conoscibilità delle norme applicate e degli elementi sui quali si fonda la decisione costituisce una condizione essenziale per consentire al cittadino di comprenderla e, se necessario, contestarla. Quando vengono utilizzati sistemi complessi basati sull'apprendimento automatico, può risultare difficile ricostruire il processo attraverso il quale determinati dati hanno condotto a uno specifico risultato. L'elevata complessità tecnica rischia così di creare una distanza tra il funzionamento del sistema e la possibilità di fornire all'interessato una motivazione accessibile.

Il problema della trasparenza emerge già nella difficoltà di individuare quali amministrazioni utilizzino concretamente strumenti di IA, all'interno di quali procedimenti e per quali finalità. Le informazioni possono essere distribuite tra comunicati, circolari e documenti tecnici di non agevole reperibilità, senza che il cittadino disponga di un quadro chiaro delle tecnologie coinvolte.⁵⁷ In mancanza di una conoscenza preventiva dell'utilizzo di un sistema algoritmico, risulta più complesso chiedere l'accesso agli atti, contestare una decisione o verificare il rispetto delle norme applicabili.

La trasparenza non può essere ridotta alla mera pubblicazione del codice sorgente. Un codice formalmente accessibile potrebbe restare incomprensibile per la maggior parte dei cittadini e persino per molti funzionari. È necessario rendere conoscibili, attraverso un linguaggio adeguato, le finalità del sistema, le categorie di dati trattati, i principali criteri di valutazione e il ruolo svolto dall'IA

⁵⁶ Ivi, pp. 478-479.

⁵⁷ N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni*, cit., p. 482.

nel procedimento.⁵⁸ Rangone propone una trasparenza articolata su più livelli: un'informazione semplificata e comprensibile destinata al pubblico, accompagnata dalla possibilità di ottenere approfondimenti tecnici da parte dei soggetti interessati.

Alla trasparenza si collega il requisito della spiegabilità. L'amministrazione deve essere in grado di illustrare le ragioni che hanno condotto all'adozione di un provvedimento anche quando la decisione è stata supportata da un sistema algoritmico. Non sarebbe sufficiente affermare che un determinato esito è stato prodotto automaticamente. Il funzionario deve poter ricostruire gli elementi rilevanti, valutarne la correttezza e tradurli in una motivazione comprensibile. Il Piano Triennale per l'informatica nella Pubblica Amministrazione richiama espressamente la necessità di garantire trasparenza e interpretabilità dei modelli, al fine di assicurare la responsabilità dell'ente e consentire agli utenti di compiere scelte consapevoli rispetto ai servizi basati sull'IA.⁵⁹

Questa esigenza introduce il tema dell'imputazione della responsabilità. Quando una decisione dannosa o illegittima deriva dall'utilizzo di un sistema di IA, può risultare complesso individuare il soggetto al quale attribuire l'errore. Nel processo possono intervenire l'amministrazione che acquista la tecnologia, il fornitore che la sviluppa, il personale che la utilizza e i soggetti che hanno messo a disposizione i dati. La frammentazione delle attività non può tradursi in una dispersione delle responsabilità. L'amministrazione deve mantenere la capacità di verificare che gli strumenti impiegati siano coerenti con le finalità istituzionali e con i principi che regolano l'azione amministrativa.

La supervisione umana assume, di conseguenza, un ruolo essenziale. Il funzionario non può limitarsi a recepire passivamente l'esito prodotto dal

⁵⁸ N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni*, cit., pp. 482-483.

⁵⁹ AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*, 2026, sezione dedicata all'intelligenza artificiale nella Pubblica Amministrazione.

sistema, soprattutto nei procedimenti che implicano valutazioni discrezionali o incidono su diritti e interessi rilevanti. Il controllo umano deve essere sostanziale e non meramente formale: chi utilizza la tecnologia deve possedere le competenze e le informazioni necessarie per riconoscere un risultato anomalo, richiedere una verifica o discostarsi dalla proposta algoritmica. L'obiettivo non consiste nell'escludere l'automazione, ma nell'impedire che il sistema assuma il ruolo di decisore incontestabile.

Rangone sottolinea la necessità di verificare l'adeguatezza del ricorso all'intelligenza artificiale in luogo di quella umana e di assicurare accessibilità, comprensibilità e non discriminazione.⁶⁰ La decisione automatizzata può risultare particolarmente utile per operazioni seriali, standardizzate e prive di discrezionalità, mentre presenta maggiori difficoltà nei casi che richiedono una valutazione del contesto, il bilanciamento di interessi contrapposti o la considerazione di circostanze eccezionali.

Un'altra area problematica riguarda la protezione dei dati personali. Le amministrazioni gestiscono informazioni particolarmente delicate, relative alla salute, alla situazione economica, alla previdenza, alla posizione lavorativa e alle condizioni familiari dei cittadini. La capacità dell'IA di collegare dati provenienti da fonti differenti può generare conoscenze ulteriori rispetto alle singole informazioni originariamente raccolte, aumentando il rischio di profilazioni invasive o di utilizzi incompatibili con le finalità iniziali.

La tutela della riservatezza richiede che siano selezionati esclusivamente i dati necessari, che le informazioni vengano protette da accessi non autorizzati e che le finalità del trattamento siano definite con precisione. Quando compatibili con le finalità del trattamento, l'anonimizzazione può impedire l'identificazione degli interessati, mentre la pseudonimizzazione può ridurre i rischi connessi al

⁶⁰ N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi*, cit., p. 473.

trattamento separando i dati dalle informazioni necessarie per ricondurli a una persona determinata. Rangone richiama esperienze nelle quali vengono registrati soltanto metadati oppure vengono creati ambienti protetti per evitare la circolazione di dati in chiaro.⁶¹ Il Piano Triennale richiede inoltre elevati standard di sicurezza e il rispetto della disciplina in materia di protezione dei dati personali e sicurezza cibernetica.

Alla protezione delle informazioni si affianca il rischio informatico. I sistemi utilizzati dalla PA possono diventare obiettivo di attacchi diretti a modificare i dati, alterare i risultati, sottrarre informazioni o interrompere l'erogazione dei servizi. La crescente interconnessione tra banche dati e piattaforme amplia le possibilità di utilizzo del patrimonio informativo pubblico, ma aumenta anche la superficie esposta alle minacce. Un malfunzionamento o un attacco possono produrre conseguenze particolarmente gravi quando coinvolgono prestazioni essenziali o procedimenti dai quali dipende l'esercizio di diritti.

L'adozione dell'intelligenza artificiale incontra anche limiti organizzativi ed economici. Lo sviluppo, l'acquisto, l'integrazione e la manutenzione dei sistemi richiedono investimenti adeguati, infrastrutture affidabili e personale dotato di competenze specialistiche. Le amministrazioni con minori disponibilità finanziarie e organizzative possono incontrare difficoltà maggiori, determinando una diffusione disomogenea dell'innovazione tra enti centrali, amministrazioni territoriali e piccoli comuni. L'impiego stabile di tali tecnologie presuppone quindi una chiara capacità organizzativa e un indirizzo politico-amministrativo coerente.⁶²

La carenza di competenze può generare un'eccessiva dipendenza dai fornitori privati. Quando l'amministrazione non dispone delle conoscenze necessarie per

⁶¹ Ivi, p. 477

⁶² M.S. Agba, G.E.M. Agba, A.W. Obeten, *Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies*, in «Journal of Public Administration, Policy and Governance Research», vol. 1, n. 2, 2023, pp. 1-14.

comprendere il funzionamento del sistema acquistato, rischia di perdere il controllo su una parte significativa del procedimento. La tutela del segreto industriale non può impedire all'ente di verificarne l'affidabilità, controllarne i risultati e spiegare le decisioni ai cittadini. Nei contratti e nelle procedure di gara è quindi necessario prevedere condizioni che consentano lo svolgimento di audit, la verifica dei risultati, l'aggiornamento dei sistemi e l'accesso alle informazioni necessarie all'amministrazione.

Un ultimo limite riguarda il divario digitale. L'espansione dei servizi automatizzati può agevolare l'accesso per molti utenti, ma rischia di escludere chi non dispone di strumenti tecnologici, connessione, competenze digitali o adeguate capacità linguistiche e cognitive. La digitalizzazione non può tradursi nella scomparsa di ogni forma di assistenza umana. Nei casi complessi e per le persone che incontrano difficoltà nell'utilizzo dei canali digitali, è necessario mantenere forme adeguate di assistenza e la possibilità di interagire con un operatore. La progettazione dei servizi deve inoltre considerare la semplicità del linguaggio, l'accessibilità degli strumenti e la pluralità delle condizioni personali, evitando che l'innovazione accresca le disuguaglianze nell'accesso alle prestazioni pubbliche. Nel complesso, le criticità dell'intelligenza artificiale nella Pubblica Amministrazione non giustificano un rifiuto generalizzato della tecnologia, ma richiedono un modello di adozione consapevole e proporzionato. L'IA può sostenere l'attività amministrativa soltanto quando i dati sono affidabili, i sistemi risultano comprensibili e verificabili, le responsabilità sono chiaramente individuate e il controllo umano rimane effettivo. La ricerca dell'efficienza deve quindi rimanere compatibile con i principi di legalità e imparzialità e con la tutela dei diritti fondamentali.

CAPITOLO 3

L'AI ACT EUROPEO

3.1 Origini, approvazione e obiettivi dell'AI Act

L'adozione dell'AI Act rappresenta il punto di arrivo di un percorso avviato dall'Unione europea diversi anni prima della presentazione della proposta legislativa. La progressiva diffusione dei sistemi di intelligenza artificiale ha evidenziato la necessità di definire un quadro comune capace di favorire lo sviluppo tecnologico e, nello stesso tempo, di prevenire gli effetti negativi derivanti da utilizzi incompatibili con la sicurezza, i diritti fondamentali e i valori europei. L'intervento dell'Unione non è nato con l'obiettivo di limitare in modo generalizzato l'innovazione, ma dalla ricerca di un equilibrio tra promozione degli investimenti, competitività economica, certezza del diritto e protezione delle persone.

Un primo passaggio rilevante si colloca nel 2018, quando la Commissione europea pubblicò la comunicazione *L'intelligenza artificiale per l'Europa*.⁶³ In tale documento l'IA veniva presentata come una tecnologia strategica per la crescita economica, la ricerca e la modernizzazione dei servizi, rispetto alla quale gli Stati membri avrebbero dovuto coordinare le proprie politiche. Nello stesso periodo fu istituito il Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, incaricato di elaborare indicazioni per uno sviluppo responsabile della tecnologia. Il lavoro del gruppo condusse, nell'aprile 2019, alla pubblicazione degli *Orientamenti etici per un'intelligenza artificiale affidabile*, fondati su una concezione antropocentrica dell'innovazione. Secondo tale impostazione, i sistemi di IA devono rimanere al servizio delle persone,

⁶³ Commissione europea, *L'intelligenza artificiale per l'Europa*, COM (2018) 237 final, Bruxelles, 25 aprile 2018.

rispettarne l'autonomia e operare in condizioni di sicurezza, trasparenza e responsabilità.⁶⁴

Gli orientamenti del 2019 individuarono sette requisiti fondamentali per un'IA affidabile: intervento e sorveglianza umani; robustezza tecnica e sicurezza; riservatezza e governance dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale e ambientale; accountability.⁶⁵ Pur non avendo carattere vincolante, questi principi contribuirono a delineare il modello europeo di regolazione e furono successivamente ripresi nei documenti preparatori e nel regolamento definitivo. L'esperienza mostrò anche i limiti di un approccio esclusivamente etico e volontario: la presenza di linee guida poteva orientare sviluppatori e utilizzatori, ma non era sufficiente a creare obblighi uniformi, meccanismi di controllo e rimedi effettivi.

Un momento decisivo fu la pubblicazione, il 19 febbraio 2020, del *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*⁶⁶. La Commissione vi delineò una strategia articolata intorno a due obiettivi complementari. Il primo consisteva nella costruzione di un “ecosistema di eccellenza”, attraverso investimenti nella ricerca, nelle infrastrutture, nei dati, nelle competenze e nella diffusione dell'IA nel settore privato e nelle amministrazioni pubbliche. Il secondo riguardava la creazione di un “ecosistema di fiducia”, fondato su regole capaci di assicurare che le applicazioni tecnologiche fossero sviluppate e utilizzate nel rispetto della legislazione europea e dei diritti dei cittadini.⁶⁷

⁶⁴ Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, *Orientamenti etici per un'intelligenza artificiale affidabile*, Commissione europea, Bruxelles, 8 aprile 2019.

⁶⁵ Ivi, pp. 16-19. Si vedano anche Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, Bruxelles, 19 febbraio 2020, pp. 10-11.

⁶⁶ Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, Bruxelles, 19 febbraio 2020.

⁶⁷ Ivi, pp. 3-4.

Il Libro bianco riconosceva che l'IA può generare benefici rilevanti nell'assistenza sanitaria, nei trasporti, nell'agricoltura, nella tutela ambientale, nei servizi pubblici e nei processi produttivi. Le stesse caratteristiche che ne determinano le potenzialità possono però produrre rischi connessi all'opacità dei meccanismi decisionali, alla qualità dei dati, alla discriminazione, alla sorveglianza, alla protezione della vita privata e alla difficoltà di individuare le responsabilità. La Commissione rilevava inoltre che le norme europee già esistenti in materia di protezione dei dati, sicurezza dei prodotti, tutela dei consumatori e non discriminazione continuavano ad applicarsi, ma potevano non essere sufficienti ad affrontare tutte le specificità dei sistemi di IA.⁶⁸

Da questa analisi derivò l'idea di un intervento proporzionato, concentrato sugli impieghi maggiormente pericolosi. Il Libro bianco proponeva già un approccio basato sul rischio, secondo il quale l'intensità degli obblighi avrebbe dovuto dipendere dal settore, dalla finalità del sistema e dalla gravità delle conseguenze potenziali. Le applicazioni capaci di incidere significativamente sulla sicurezza o sui diritti delle persone avrebbero dovuto essere soggette a requisiti più rigorosi in materia di dati, documentazione, trasparenza, precisione, robustezza e sorveglianza umana. Questa impostazione divenne il nucleo della successiva proposta legislativa.⁶⁹

A seguito della consultazione pubblica avviata insieme al Libro bianco, il 21 aprile 2021 la Commissione europea presentò la proposta di regolamento COM (2021) 206 final, recante regole armonizzate sull'intelligenza artificiale.⁷⁰ La scelta del regolamento, anziché della direttiva, rispondeva all'esigenza di introdurre una disciplina direttamente applicabile e uniforme in tutti gli Stati

⁶⁸ Ivi, pp. 11-19.

⁶⁹ Ivi, pp. 19-24.

⁷⁰ Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione*, COM (2021) 206 final, Bruxelles, 21 aprile 2021, pp. 1-8.

membri. Soluzioni nazionali divergenti avrebbero potuto generare ostacoli alla circolazione dei sistemi di IA, aumentare l'incertezza per gli operatori economici e determinare livelli di tutela differenti all'interno dell'Unione.

La proposta si fondava principalmente sull'articolo 114 del Trattato sul funzionamento dell'Unione europea, relativo all'adozione di misure necessarie per il funzionamento del mercato interno. A tale base giuridica si affiancava l'articolo 16 TFUE per le disposizioni riguardanti la protezione delle persone fisiche rispetto al trattamento dei dati personali, con particolare riferimento agli usi dell'identificazione biometrica remota nelle attività di contrasto. Questa duplice base riflette la natura dell'intervento europeo, diretto sia ad armonizzare le condizioni di sviluppo e commercializzazione delle tecnologie sia a proteggere le persone dagli impieghi più invasivi.⁷¹

La Commissione indicò quattro obiettivi specifici. Il primo era assicurare che i sistemi di IA immessi sul mercato o utilizzati nell'Unione fossero sicuri e conformi alla normativa in materia di diritti fondamentali. Il secondo consisteva nel garantire certezza del diritto, così da favorire gli investimenti e l'innovazione. Il terzo riguardava il rafforzamento della governance e dell'applicazione effettiva delle norme già esistenti. Il quarto mirava a sviluppare un mercato unico per applicazioni lecite, sicure e affidabili, evitando la frammentazione normativa tra gli Stati membri.⁷²

La proposta adottava una struttura orizzontale, applicabile a settori differenti, combinata con una disciplina graduata in relazione al rischio. Non tutti i sistemi venivano quindi assoggettati alle medesime prescrizioni. Le pratiche considerate incompatibili con i valori dell'Unione erano destinate al divieto; i sistemi ad alto rischio venivano sottoposti a requisiti obbligatori e procedure di conformità; per alcuni impieghi erano previsti obblighi di trasparenza; le applicazioni meno

⁷¹ Commissione europea, COM (2021) 206 final, cit., pp. 9-12

⁷² Ivi, pp. 5-7.

problematiche rimanevano in larga misura libere, ferma restando l'applicazione delle altre norme europee. La proposta includeva anche misure per sostenere l'innovazione, tra cui gli spazi di sperimentazione normativa e disposizioni dedicate alle piccole e medie imprese.⁷³

La proposta fu poi esaminata dal Parlamento europeo e dal Consiglio secondo la procedura legislativa ordinaria. Nel corso del negoziato, il testo fu ampliato mediante l'introduzione di disposizioni specifiche dedicate ai modelli di IA per finalità generali, non presenti nella proposta originaria nella forma poi adottata. Dopo una lunga fase di negoziato, nella notte tra l'8 e il 9 dicembre 2023 i rappresentanti del Parlamento europeo e del Consiglio raggiunsero un accordo politico provvisorio sul testo. Il Parlamento europeo approvò il regolamento il 13 marzo 2024, mentre il Consiglio adottò formalmente l'atto il 21 maggio dello stesso anno. Il testo definitivo divenne il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, pubblicato nella Gazzetta ufficiale dell'Unione europea il 12 luglio 2024. Il regolamento entrò in vigore il 1° agosto 2024, venti giorni dopo la pubblicazione.⁷⁴

L'applicazione delle disposizioni dell'AI Act è organizzata secondo un calendario graduale, successivamente modificato nel 2026. Dal 2 febbraio 2025 trovano applicazione, tra l'altro, le disposizioni generali, gli obblighi in materia di alfabetizzazione sull'intelligenza artificiale e le pratiche vietate. Dal 2 agosto 2025 sono divenute applicabili ulteriori disposizioni relative, in particolare, alla governance europea e ai modelli di IA per finalità generali. Il 2 agosto 2026 rappresenta una tappa ulteriore dell'attuazione del regolamento, con l'entrata in applicazione di numerose disposizioni generali e degli obblighi di trasparenza

⁷³ Commissione europea, COM (2021) 206 final, cit., pp. 6-8 e 20-25.

⁷⁴ Consiglio dell'Unione europea, *Normativa sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole al mondo in materia di IA*, comunicato stampa, 9 dicembre 2023; Parlamento europeo, *Il Parlamento europeo approva la legge sull'intelligenza artificiale*, 13 marzo 2024; Consiglio dell'Unione europea, *Regolamento sull'intelligenza artificiale: via libera definitivo del Consiglio*, 21 maggio 2024; Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, GUUE L, 12 luglio 2024.

pertinenti. Il Regolamento (UE) 2026/1744 ha tuttavia modificato il calendario relativo ai sistemi di IA ad alto rischio: per i sistemi rientranti nei casi d'uso dell'Allegato III le relative disposizioni troveranno applicazione dal 2 dicembre 2027, mentre per i sistemi ad alto rischio collegati ai prodotti disciplinati dall'Allegato I il termine è fissato al 2 agosto 2028. La scansione temporale non modifica l'entrata in vigore dell'AI Act, ma differisce l'operatività di specifici gruppi di obblighi, consentendo agli operatori e alle amministrazioni di adeguarsi progressivamente al nuovo quadro normativo.⁷⁵

L'articolo 1 del regolamento definisce la finalità complessiva dell'intervento. L'AI Act mira a migliorare il funzionamento del mercato interno attraverso un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale. Tale armonizzazione deve promuovere un'IA antropocentrica e affidabile, assicurando un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali riconosciuti dall'ordinamento dell'Unione. Tra gli interessi tutelati rientrano anche la democrazia, lo Stato di diritto e la protezione dell'ambiente dagli effetti dannosi dei sistemi di IA. A questi obiettivi si aggiunge il sostegno all'innovazione, perseguito evitando che gli obblighi normativi producano restrizioni sproporzionate rispetto ai rischi effettivi.⁷⁶

Il regolamento svolge quindi una duplice funzione. Da una parte stabilisce condizioni comuni per la circolazione e l'utilizzo dei sistemi di IA nel mercato europeo, offrendo agli operatori un quadro di riferimento unitario. Dall'altra introduce garanzie rivolte alle persone e alla collettività, mediante divieti, requisiti, obblighi di trasparenza, meccanismi di sorveglianza e strumenti di controllo. La tutela non viene costruita attraverso un divieto generale della

⁷⁵ Regolamento (UE) 2024/1689, art. 113, come modificato dal Regolamento (UE) 2026/1744; Commissione europea, documentazione aggiornata sull'attuazione dell'AI Act.

⁷⁶ Regolamento (UE) 2024/1689, cit., art. 1, par. 1.

tecnologia, ma mediante una regolazione differenziata, legata alla finalità del sistema, al contesto d'impiego e alla possibile incidenza su interessi giuridicamente rilevanti.

L'approccio europeo assume un rilievo particolare per la Pubblica Amministrazione. Gli enti pubblici possono utilizzare sistemi di IA in settori capaci di incidere sull'accesso a prestazioni, servizi essenziali, opportunità lavorative, istruzione, giustizia e sicurezza. In questi contesti l'esigenza di efficienza deve essere conciliata con legalità, imparzialità, trasparenza, non discriminazione e tutela dei diritti. L'AI Act fornisce il quadro generale entro il quale tali tecnologie possono essere sviluppate, acquistate e impiegate, mentre la disciplina concretamente applicabile dipende dalla categoria di rischio e dal ruolo assunto dai soggetti coinvolti.

3.2 La classificazione dei sistemi di IA in base al rischio

Uno degli elementi centrali dell'AI Act è l'adozione di un modello regolatorio basato sul rischio. Il legislatore europeo non assoggetta tutti i sistemi di intelligenza artificiale alle medesime prescrizioni, ma modula l'intensità degli obblighi in funzione della probabilità e della gravità dei danni che il loro impiego può provocare.⁷⁷ La disciplina è quindi costruita secondo un criterio di proporzionalità: quanto maggiore è il pericolo per la salute, la sicurezza o i diritti fondamentali, tanto più rigorose risultano le condizioni poste allo sviluppo, all'immissione sul mercato e all'utilizzo del sistema. Questa impostazione era già presente nel Libro bianco del 2020, nel quale la Commissione aveva proposto di concentrare gli obblighi più stringenti sulle applicazioni capaci di produrre conseguenze significative. La proposta di regolamento del 2021 trasformò tale

⁷⁷ Regolamento (UE) 2024/1689, considerando 26-27; Commissione europea, COM (2021) 206 final, cit., pp. 6-8.

orientamento in una metodologia normativa più strutturata, fondata sull'individuazione degli usi vietati, dei sistemi ad alto rischio e delle applicazioni soggette a specifici obblighi di trasparenza. Il regolamento definitivo conserva questa impostazione e la integra con disposizioni rivolte ai modelli di IA per finalità generali.

La classificazione non dipende esclusivamente dalle caratteristiche tecniche del sistema.⁷⁸ Assumono rilievo soprattutto la finalità prevista, il contesto nel quale l'IA viene utilizzata, le persone interessate e la natura degli effetti che possono derivarne. Uno stesso strumento tecnologico può quindi essere soggetto a regole differenti a seconda dell'uso concreto. Un sistema impiegato per organizzare documenti interni non presenta necessariamente lo stesso livello di rischio di un'applicazione utilizzata per valutare l'accesso a un servizio essenziale, selezionare candidati a un posto di lavoro o supportare una decisione giudiziaria. Il rischio deriva dall'interazione tra funzionamento del sistema, settore di applicazione e conseguenze prodotte sulle persone.

Nella comunicazione istituzionale pubblicata in occasione dell'entrata in vigore dell'AI Act, la Commissione europea rappresenta l'approccio attraverso quattro livelli: rischio inaccettabile, rischio elevato, rischio specifico per la trasparenza e rischio minimo.⁷⁹ Questa suddivisione consente di comprendere la logica generale del regolamento, ma richiede una precisazione. Il testo normativo non contiene un unico articolo che classifichi formalmente tutti i sistemi mediante quattro categorie rigidamente separate. Esso disciplina le pratiche vietate all'articolo 5, i sistemi ad alto rischio agli articoli 6 e seguenti, determinati obblighi di trasparenza all'articolo 50 e la possibilità di adottare codici di condotta volontari per altri sistemi all'articolo 95. La quadripartizione costituisce

⁷⁸ Regolamento (UE) 2024/1689, considerando 26-27 e art. 6.

⁷⁹ Commissione europea, *Entrata in vigore della legge europea sull'intelligenza artificiale*, 1° agosto 2024.

quindi una rappresentazione sintetica del diverso grado di intervento previsto dal legislatore.

Tabella 1 – Classificazione dei sistemi di IA in base al livello di rischio

Livello di rischio	Disciplina	Esempi generali	Riferimento normativo
Inaccettabile	Divieto di immissione sul mercato, messa in servizio o utilizzo	Social scoring, pratiche manipolative, alcuni usi biometrici	art. 5
Elevato	Requisiti obbligatori, controlli e valutazione di conformità	Occupazione, istruzione, servizi essenziali, giustizia	art. 6, allegati I e III
Specifico per la trasparenza	Obblighi informativi verso gli utenti	Chatbot, deep fake, riconoscimento delle emozioni	art. 50
Minimo o nullo	Nessun obbligo specifico dell’AI Act, salvo altre norme applicabili	Filtri spam, alcuni sistemi di raccomandazione	art. 95; Commissione europea, comunicato del 1° agosto 2024

Fonte: elaborazione dell’autrice sulla base del Regolamento (UE) 2024/1689 e della comunicazione della Commissione europea del 1° agosto 2024.

Il livello più grave è rappresentato dal rischio inaccettabile. Vi rientrano le pratiche considerate incompatibili con i valori dell’Unione e capaci di costituire una minaccia particolarmente seria per i diritti e le libertà delle persone. In tali casi il regolamento non ritiene sufficiente imporre obblighi di controllo, ma vieta l’immissione sul mercato, la messa in servizio o l’utilizzo delle applicazioni interessate. Rientrano in questa logica, nei limiti e secondo le condizioni stabilite dall’articolo 5, le tecniche manipolative o ingannevoli capaci di compromettere consapevolmente la libertà di scelta, lo sfruttamento delle vulnerabilità di determinate persone, alcune forme di valutazione sociale, specifiche applicazioni

di polizia predittiva e taluni impieghi dei sistemi biometrici. L'analisi dettagliata di tali divieti è rinviata al paragrafo successivo.⁸⁰

Il secondo livello riguarda i sistemi ad alto rischio, che costituiscono il nucleo principale della disciplina. Tali applicazioni non sono vietate, poiché possono perseguire finalità lecite e socialmente utili, ma sono sottoposte a requisiti e controlli più rigorosi. L'articolo 6 individua due modalità attraverso le quali un sistema può essere qualificato come ad alto rischio.⁸¹

La prima riguarda i sistemi che costituiscono componenti di sicurezza di un prodotto, oppure sono essi stessi prodotti, disciplinati dalla normativa europea di armonizzazione elencata nell'allegato I. La classificazione richiede anche che il prodotto interessato sia soggetto a una valutazione di conformità da parte di un organismo terzo prima dell'immissione sul mercato o della messa in servizio. In questa categoria possono rientrare, in presenza delle condizioni indicate dal regolamento, sistemi inseriti in dispositivi medici, macchinari, veicoli, attrezzature e altri prodotti sottoposti alla legislazione europea in materia di sicurezza.

La seconda modalità riguarda i sistemi utilizzati negli ambiti espressamente elencati nell'allegato III. Tra questi figurano determinate applicazioni di identificazione e categorizzazione biometrica, gestione delle infrastrutture critiche, istruzione e formazione professionale, occupazione e gestione dei lavoratori, accesso a servizi essenziali pubblici e privati, attività di contrasto, migrazione e controllo delle frontiere, amministrazione della giustizia e processi democratici.⁸² L'inclusione di tali settori deriva dalla particolare capacità dei sistemi impiegati in questi contesti di incidere sulla sicurezza, sulle opportunità delle persone e sull'esercizio dei diritti fondamentali.

⁸⁰ Regolamento (UE) 2024/1689, art. 5.

⁸¹ Regolamento (UE) 2024/1689, art. 6, parr. 1-2, e allegati I e III.

⁸² Regolamento (UE) 2024/1689, allegato III.

La presenza di un sistema nell'allegato III non determina sempre e automaticamente la sua qualificazione come ad alto rischio. L'articolo 6, paragrafo 3, prevede che un'applicazione elencata possa non essere considerata tale quando non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali e non influenza materialmente il risultato del processo decisionale. Questa esclusione può operare quando il sistema svolge un compito procedurale ristretto, migliora il risultato di un'attività umana già completata, individua modelli decisionali o deviazioni senza sostituire la valutazione umana oppure esegue un'attività preparatoria rispetto a una valutazione più ampia. Il fornitore che ritiene applicabile l'esclusione deve documentare la propria valutazione prima dell'immissione sul mercato o della messa in servizio.⁸³

Il regolamento stabilisce però un limite rilevante: i sistemi ricompresi nell'allegato III che effettuano la profilazione di persone fisiche sono sempre considerati ad alto rischio. In tali casi l'elaborazione delle caratteristiche personali e la capacità di formulare valutazioni o previsioni sul comportamento, sulle preferenze o sulle condizioni degli individui giustificano l'applicazione del regime più rigoroso.

La qualificazione come sistema ad alto rischio comporta l'applicazione di requisiti relativi, tra l'altro, alla gestione dei rischi, alla qualità e alla governance dei dati, alla documentazione tecnica, alla registrazione automatica degli eventi, alla trasparenza verso i deployer, alla sorveglianza umana, all'accuratezza, alla robustezza e alla cibersecurity. A tali requisiti si affiancano obblighi differenziati per fornitori, deployer, importatori e distributori. Questi aspetti saranno analizzati nei paragrafi dedicati ai sistemi ad alto rischio e agli obblighi previsti dal regolamento.

⁸³ Regolamento (UE) 2024/1689, art. 6, parr. 3-4.

Il terzo livello comprende le applicazioni caratterizzate da un rischio specifico connesso alla trasparenza. In questi casi il regolamento non vieta il sistema e non lo sottopone necessariamente all'intera disciplina prevista per l'alto rischio, ma richiede che le persone siano informate della presenza o dell'intervento dell'intelligenza artificiale. L'articolo 50 prevede, ad esempio, che i sistemi destinati a interagire direttamente con persone fisiche siano progettati in modo da rendere gli utenti consapevoli di interagire con un sistema di IA, salvo che ciò risulti evidente dal contesto. Obblighi informativi sono previsti anche per i sistemi di riconoscimento delle emozioni e di categorizzazione biometrica, mentre specifiche prescrizioni riguardano i contenuti generati o manipolati artificialmente.⁸⁴

Una particolare attenzione è dedicata ai cosiddetti deep fake, ossia contenuti consistenti in immagini, audio o video generati o manipolati dall'IA che assomigliano a persone, oggetti, luoghi, entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri. In tali situazioni deve essere resa nota la natura artificiale o manipolata del contenuto, secondo condizioni compatibili con il mezzo utilizzato e senza impedire gli usi legittimi connessi alla libertà di espressione, alla creazione artistica, alla satira o ad altre finalità riconosciute dall'ordinamento. La funzione degli obblighi di trasparenza consiste nel permettere alle persone di comprendere la natura dell'interazione o del contenuto e di valutare in modo più consapevole le informazioni ricevute.

Il livello più basso comprende i sistemi considerati a rischio minimo o nullo. La maggior parte delle applicazioni di IA rientra in quest'area e non è soggetta agli obblighi specifici previsti per i sistemi ad alto rischio. Possono costituirne esempi i filtri antispam, alcuni sistemi di raccomandazione e applicazioni destinate a compiti interni privi di conseguenze significative sui diritti o sulla sicurezza.

⁸⁴ Regolamento (UE) 2024/1689, art. 50.

L'assenza di obblighi specifici derivanti dall'AI Act non significa che tali sistemi operino al di fuori di ogni disciplina. Continuano ad applicarsi le norme dell'Unione e degli Stati membri in materia di protezione dei dati personali, tutela dei consumatori, non discriminazione, sicurezza dei prodotti, responsabilità e diritto del lavoro, quando pertinenti.⁸⁵

Per i sistemi non classificati ad alto rischio, l'articolo 95 incoraggia inoltre l'elaborazione di codici di condotta volontari diretti a promuovere l'applicazione di alcuni requisiti propri dell'IA affidabile. Tali strumenti possono riguardare la sostenibilità ambientale, l'alfabetizzazione in materia di IA, l'accessibilità, la partecipazione dei soggetti interessati e la valutazione degli effetti sui diritti fondamentali. Il legislatore affianca così agli obblighi giuridici un sistema di adesione volontaria, finalizzato a diffondere standard di affidabilità anche oltre le applicazioni sottoposte al regime più rigoroso.

La classificazione non ha carattere immutabile. L'articolo 7 attribuisce alla Commissione il potere di modificare l'allegato III mediante atti delegati, aggiungendo o aggiornando casi d'uso quando ricorrono le condizioni stabilite dal regolamento. La valutazione deve considerare la finalità prevista, la misura in cui il sistema è già stato utilizzato, la natura e la quantità dei dati trattati, il grado di autonomia, la possibilità di intervento umano, il numero e la vulnerabilità delle persone interessate, la gravità e la probabilità dei danni e la possibilità di porvi rimedio. Questo meccanismo consente di adeguare il quadro normativo all'evoluzione tecnologica senza modificare ogni volta l'intero regolamento.⁸⁶

Accanto alla classificazione dei sistemi, l'AI Act introduce una disciplina specifica per i modelli di IA per finalità generali. Tali modelli possono essere integrati in una pluralità di applicazioni e non sono collegati, al momento della

⁸⁵ Regolamento (UE) 2024/1689, art. 95; Commissione europea, comunicato del 1° agosto 2024.

⁸⁶ Regolamento (UE) 2024/1689, art. 7.

loro realizzazione, a un'unica finalità d'uso. Per questa ragione non si inseriscono automaticamente in una sola delle categorie descritte. Il regolamento prevede obblighi propri per i loro fornitori e prescrizioni aggiuntive quando il modello presenta un rischio sistemico. Il sistema concreto sviluppato mediante un modello per finalità generali può essere successivamente classificato come vietato, ad alto rischio o soggetto a trasparenza in base alla funzione e al contesto nei quali viene utilizzato.⁸⁷

L'approccio basato sul rischio permette quindi di differenziare la disciplina evitando sia una regolazione uniforme e sproporzionata sia l'assenza di tutele nei contesti più delicati. La classificazione rappresenta il punto di partenza per determinare quali sistemi possano essere utilizzati, quali debbano rispettare requisiti rafforzati e quali siano sottoposti a obblighi informativi.

3.3 Le pratiche di intelligenza artificiale vietate

Il livello più intenso di intervento previsto dall'AI Act riguarda le pratiche di intelligenza artificiale considerate incompatibili con i valori dell'Unione e con la tutela dei diritti fondamentali. Diversamente dai sistemi ad alto rischio, che possono essere immessi sul mercato e utilizzati purché rispettino requisiti e procedure specifiche, le applicazioni comprese nell'articolo 5 sono oggetto di un divieto. Il legislatore ritiene che, in tali ipotesi, il rischio non possa essere adeguatamente contenuto mediante obblighi di trasparenza, sorveglianza umana o valutazioni di conformità, poiché la finalità o le modalità di funzionamento del sistema determinano un livello di pregiudizio ritenuto inaccettabile.⁸⁸

I divieti si applicano all'immissione sul mercato, alla messa in servizio o all'uso delle pratiche espressamente individuate. La disciplina non vieta quindi

⁸⁷ Regolamento (UE) 2024/1689, artt. 51-55.

⁸⁸ Regolamento (UE) 2024/1689, considerando 28-29 e art. 5; Commissione europea, COM (2021) 206 final, cit., sezione 5.2.2.

determinate tecnologie in quanto tali, ma specifici impieghi dell'intelligenza artificiale. Anche in questo ambito assumono rilievo la finalità prevista, il contesto operativo, le persone interessate e gli effetti che il sistema è capace di produrre. La stessa tecnica può rientrare nel divieto soltanto quando ricorrono tutte le condizioni indicate dall'articolo 5, mentre può essere assoggettata a un regime diverso se impiegata per altre finalità.

Una prima categoria riguarda i sistemi che utilizzano tecniche subliminali, operanti al di là della consapevolezza di una persona, oppure tecniche intenzionalmente manipolative o ingannevoli. Il divieto si applica quando tali strumenti hanno lo scopo o l'effetto di alterare materialmente il comportamento di una persona o di un gruppo, compromettendone in modo apprezzabile la capacità di adottare una decisione informata e inducendoli a compiere una scelta che altrimenti non avrebbero effettuato. È inoltre necessario che tale comportamento provochi, o sia ragionevolmente idoneo a provocare, un danno significativo alla persona interessata o a un'altra persona.⁸⁹

La disposizione mira a proteggere l'autonomia decisionale e la libertà di scelta. Non ogni forma di persuasione commerciale o influenza esercitata mediante strumenti digitali è automaticamente vietata. La soglia stabilita dal regolamento richiede una manipolazione capace di compromettere in misura rilevante la capacità decisionale e di determinare un danno significativo. Restano comunque applicabili le altre norme europee e nazionali in materia di tutela dei consumatori, protezione dei dati, pratiche commerciali scorrette e servizi digitali, anche quando non risultino soddisfatte tutte le condizioni necessarie per l'applicazione dell'articolo 5.

Un secondo divieto riguarda i sistemi che sfruttano le vulnerabilità di una persona o di uno specifico gruppo dovute all'età, alla disabilità oppure a una particolare

⁸⁹ Regolamento (UE) 2024/1689, art. 5, par. 1, lett. a), e considerando 29.

situazione sociale o economica. Anche in questo caso l'impiego è vietato quando determina, o è ragionevolmente idoneo a determinare, un'alterazione materiale del comportamento capace di provocare un danno significativo.⁹⁰ La disposizione tutela soggetti che possono trovarsi in una posizione di maggiore esposizione rispetto alle strategie di influenza automatizzata. Tra questi possono rientrare minori, persone con disabilità e individui le cui condizioni economiche o sociali riducano concretamente la possibilità di valutare o contrastare l'azione del sistema.

Il riferimento alla situazione sociale o economica amplia la formulazione inizialmente contenuta nella proposta del 2021, che concentrava maggiormente l'attenzione sull'età e sulla disabilità. La versione definitiva riconosce che la vulnerabilità può derivare anche da condizioni di dipendenza, marginalità o bisogno economico. Il divieto non presuppone però che qualsiasi servizio rivolto a una categoria vulnerabile sia illecito: occorre che il sistema sfrutti quella condizione con l'obiettivo o l'effetto di alterare materialmente il comportamento e che sussista il rischio di un danno significativo.

Una terza pratica vietata è il cosiddetto social scoring. L'articolo 5 impedisce l'utilizzo di sistemi destinati a valutare o classificare persone fisiche o gruppi per un determinato periodo di tempo sulla base del loro comportamento sociale oppure di caratteristiche personali o della personalità, conosciute, inferite o previste. Il divieto opera quando il punteggio ottenuto conduce a un trattamento pregiudizievole o sfavorevole in contesti sociali estranei a quelli nei quali i dati sono stati originariamente generati o raccolti, oppure a un trattamento ingiustificato o sproporzionato rispetto al comportamento osservato o alla sua gravità.⁹¹

⁹⁰ Ivi, art. 5, par. 1, lett. b), e considerando 29.

⁹¹ Ivi, art. 5, par. 1, lett. c), e considerando 31.

L'elemento problematico non consiste nella semplice attribuzione di una valutazione, attività presente in numerosi settori, ma nella costruzione di profili generalizzati capaci di accompagnare la persona in ambiti diversi e di determinare conseguenze sproporzionate. Il rischio è quello di ridurre l'individuo a un punteggio complessivo e di trasferire informazioni raccolte in un determinato contesto all'interno di decisioni prive di un collegamento adeguato con la loro origine. Questa pratica può incidere sulla dignità, sulla non discriminazione e sulla possibilità di essere valutati in relazione alla situazione concreta.

Il divieto assume particolare rilievo per la Pubblica Amministrazione. Gli enti pubblici dispongono di patrimoni informativi estesi e possono collegare dati provenienti da procedimenti, prestazioni e banche dati differenti. L'uso di tali informazioni per attribuire ai cittadini punteggi generali di affidabilità o meritevolezza, destinati a produrre conseguenze in settori non collegati al contesto originario, potrebbe integrare la pratica vietata. Ciò non impedisce alle amministrazioni di effettuare valutazioni previste dalla legge per l'accesso a una specifica prestazione, purché siano fondate su criteri pertinenti, trasparenti e proporzionati alla finalità perseguita.

L'AI Act vieta inoltre determinate forme di valutazione del rischio criminale individuale. Non possono essere utilizzati sistemi di IA per valutare o prevedere la probabilità che una persona fisica commetta un reato quando la valutazione è fondata unicamente sulla profilazione oppure sull'esame dei tratti e delle caratteristiche della personalità.⁹² Il legislatore esclude così che la pericolosità individuale possa essere determinata esclusivamente attraverso inferenze algoritmiche relative al profilo personale.

⁹² Ivi, art. 5, par. 1, lett. d), e considerando 42.

Il divieto non comprende i sistemi utilizzati per sostenere una valutazione umana già basata su fatti oggettivi e verificabili direttamente collegati a un'attività criminosa. La distinzione è rilevante: l'IA non può sostituire l'accertamento concreto mediante una previsione fondata soltanto sulle caratteristiche della persona, ma può eventualmente fornire supporto nell'analisi di elementi fattuali già disponibili. Questa delimitazione mira a evitare forme di polizia predittiva incentrate sull'individuo e incompatibili con la presunzione di innocenza, senza escludere ogni uso dell'analisi automatizzata nelle attività investigative.

Un ulteriore divieto riguarda la creazione o l'ampliamento di banche dati di riconoscimento facciale attraverso l'acquisizione non mirata di immagini facciali da Internet o da filmati di telecamere a circuito chiuso.⁹³ La pratica consiste nella raccolta indiscriminata di grandi quantità di immagini, effettuata senza l'individuazione preventiva delle persone interessate, allo scopo di costruire archivi utilizzabili per il riconoscimento biometrico.

Il divieto risponde ai rischi derivanti dalla sorveglianza di massa e dal trattamento di dati biometrici senza un collegamento sufficientemente determinato con una finalità legittima. La disponibilità pubblica di una fotografia su Internet non comporta che essa possa essere liberamente raccolta e inserita in una banca dati biometrica. La disposizione non vieta in modo generale ogni uso di immagini facciali, ma la loro acquisizione non mirata da Internet o da sistemi di videosorveglianza per costituire o ampliare archivi destinati al riconoscimento.

L'articolo 5 vieta anche l'impiego di sistemi di riconoscimento delle emozioni nei luoghi di lavoro e negli istituti di istruzione. Il divieto riguarda i sistemi che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici.⁹⁴ La scelta del legislatore deriva sia dai dubbi sull'affidabilità scientifica di tali strumenti sia dallo squilibrio di potere che

⁹³ Ivi, art. 5, par. 1, lett. e), e considerando 43.

⁹⁴ Ivi, art. 5, par. 1, lett. f), e considerando 44.

caratterizza i rapporti lavorativi ed educativi. Un dipendente o uno studente potrebbe subire conseguenze sfavorevoli sulla base di inferenze non sufficientemente precise o condizionate da differenze individuali, culturali e contestuali.

Sono esclusi dal divieto i sistemi destinati a essere messi in servizio o utilizzati per motivi medici o di sicurezza. Un'applicazione finalizzata, ad esempio, a rilevare condizioni rilevanti per la tutela della salute o a prevenire situazioni di pericolo può quindi essere ammessa, purché la finalità medica o di sicurezza sia effettiva e siano rispettate le altre disposizioni applicabili. L'eccezione non consente di utilizzare genericamente il riconoscimento delle emozioni per valutare la produttività, l'affidabilità o il rendimento di lavoratori e studenti. Un'altra pratica vietata consiste nella categorizzazione biometrica delle persone al fine di dedurre o inferire la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale.⁹⁵ Si tratta di caratteristiche particolarmente sensibili, la cui inferenza automatizzata può produrre discriminazioni, stigmatizzazione e forme invasive di profilazione.

Il divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come immagini, quando tale attività sia necessaria per classificare i dati, né la categorizzazione di dati biometrici nel settore delle attività di contrasto. Tali esclusioni non rendono automaticamente le operazioni lecite, poiché continuano ad applicarsi le norme in materia di protezione dei dati personali, non discriminazione e rispetto dei diritti fondamentali. La categorizzazione biometrica deve inoltre essere distinta dalla semplice autenticazione o verifica dell'identità, che non consiste nell'inferire caratteristiche sensibili.

⁹⁵ Ivi, art. 5, par. 1, lett. g), e considerando 30.

L'ultima e più articolata previsione riguarda l'identificazione biometrica remota in tempo reale negli spazi accessibili al pubblico per finalità di contrasto. La regola generale è il divieto, giustificato dalla capacità di tali sistemi di identificare a distanza un numero potenzialmente elevato di persone che non partecipano attivamente al processo di riconoscimento. Questo impiego può incidere profondamente sulla vita privata, sulla protezione dei dati, sulla libertà di circolazione, di riunione e di espressione.⁹⁶

Il regolamento ammette però tre gruppi circoscritti di eccezioni. L'utilizzo può essere autorizzato per la ricerca mirata di vittime di sottrazione, tratta o sfruttamento sessuale e per la ricerca di persone scomparse; per prevenire una minaccia specifica, sostanziale e imminente alla vita o all'incolumità fisica delle persone oppure una minaccia reale e attuale, o reale e prevedibile, di un attentato terroristico; infine, per localizzare o identificare una persona sospettata di aver commesso determinati reati indicati nell'allegato II, quando tali reati siano punibili nello Stato membro interessato con una pena detentiva il cui massimo sia di almeno quattro anni.⁹⁷

Le eccezioni non comportano un'autorizzazione generale. L'impiego deve essere necessario e proporzionato, limitato temporalmente, geograficamente e personalmente e destinato esclusivamente a confermare l'identità della persona specificamente ricercata. L'autorità deve considerare la gravità e la probabilità del danno che potrebbe derivare dal mancato utilizzo del sistema, nonché le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate. Sono inoltre richieste una valutazione d'impatto sui diritti fondamentali, la registrazione del sistema nella banca dati dell'Unione e, di regola, una preventiva

⁹⁶ Ivi, art. 5, par. 1, lett. h), e considerando 32-40.

⁹⁷ Ivi, art. 5, par. 1, lett. h), punti i) -iii), e allegato II.

autorizzazione rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente la cui decisione sia vincolante.⁹⁸

In situazioni di urgenza debitamente giustificate, l'utilizzo può iniziare senza previa autorizzazione, ma la richiesta deve essere presentata senza indebito ritardo e comunque entro ventiquattro ore. Qualora l'autorizzazione venga negata, l'uso deve cessare immediatamente e i dati, i risultati e gli output ottenuti devono essere cancellati. Gli Stati membri possono inoltre adottare norme nazionali più restrittive oppure decidere di non consentire affatto tali usi sul proprio territorio.

Le pratiche vietate dall'articolo 5 sono applicabili dal 2 febbraio 2025. La violazione dei divieti è soggetta al livello sanzionatorio più elevato previsto dall'AI Act: possono essere applicate sanzioni amministrative pecuniarie fino a 35 milioni di euro. Qualora l'autore della violazione sia un'impresa, la sanzione può raggiungere, se superiore, il 7% del fatturato mondiale totale annuo dell'esercizio precedente. Nell'applicazione delle sanzioni devono essere considerate la natura, la gravità e la durata della violazione, nonché le circostanze del caso concreto.⁹⁹

L'elenco dell'articolo 5 rappresenta una scelta normativa particolarmente significativa, poiché stabilisce limiti invalicabili all'impiego dell'intelligenza artificiale. La ricerca dell'innovazione e dell'efficienza non può giustificare applicazioni fondate sulla manipolazione dannosa, sullo sfruttamento delle vulnerabilità, sulla valutazione generalizzata delle persone o su forme sproporzionate di sorveglianza biometrica. Al di fuori di queste ipotesi, il regolamento ammette l'utilizzo dei sistemi di IA, sottoponendo quelli capaci di produrre conseguenze rilevanti a un regime rafforzato.

⁹⁸ Ivi, art. 5, parr. 2-5.

⁹⁹ Regolamento (UE) 2024/1689, art. 99, parr. 3 e 7, e art. 113, par. 3, lett. a).

3.4 I sistemi di IA ad alto rischio

I sistemi di intelligenza artificiale ad alto rischio occupano una posizione centrale nell'architettura dell'AI Act. A differenza delle pratiche vietate, il loro sviluppo e utilizzo sono ammessi, poiché possono perseguire finalità lecite e produrre benefici rilevanti. La loro capacità di incidere sulla salute, sulla sicurezza o sui diritti fondamentali giustifica però l'applicazione di una disciplina più rigorosa rispetto a quella prevista per le applicazioni meno problematiche. La qualificazione come sistema ad alto rischio non rappresenta quindi un giudizio di illiceità, ma indica la necessità di sottoporre la tecnologia a garanzie rafforzate durante il suo intero ciclo di vita.¹⁰⁰ Il regolamento adotta una classificazione fondata soprattutto sulla funzione svolta dal sistema e sul contesto nel quale viene impiegato. La complessità tecnica o il grado di autonomia non sono, da soli, sufficienti a determinare l'alto rischio. Diventa decisiva la possibilità che l'output prodotto dall'IA influenzi la sicurezza di un prodotto, l'accesso a opportunità essenziali, la posizione giuridica di una persona o l'esercizio di un diritto fondamentale. L'articolo 6 individua a questo scopo due gruppi principali: i sistemi collegati a prodotti disciplinati dalla normativa europea di armonizzazione e quelli destinati agli ambiti specificamente indicati nell'allegato III.¹⁰¹ Il primo gruppo comprende i sistemi di IA che costituiscono un componente di sicurezza di un prodotto oppure sono essi stessi un prodotto regolato da uno degli atti legislativi elencati nell'allegato I. La classificazione come ad alto rischio richiede che il prodotto sia anche soggetto a una valutazione della conformità da parte di un organismo terzo prima dell'immissione sul mercato o della messa in servizio. Le due condizioni devono quindi ricorrere congiuntamente.¹⁰² La nozione di componente di sicurezza comprende gli

¹⁰⁰ Regolamento (UE) 2024/1689, considerando 46-49 e art. 6.

¹⁰¹ Ivi, art. 6, parr. 1-2, e allegati I e III.

¹⁰² Ivi, art. 6, par. 1, e allegato I.

elementi che svolgono una funzione essenziale per il funzionamento sicuro del prodotto o il cui guasto o malfunzionamento può mettere in pericolo la salute e la sicurezza delle persone o dei beni.¹⁰³ Possono rientrare in questa categoria, a seconda delle caratteristiche e della funzione concretamente svolta, sistemi integrati in macchinari, dispositivi medici, dispositivi medico-diagnostici in vitro, ascensori, giocattoli, apparecchiature radio, mezzi di trasporto e altri prodotti assoggettati alla normativa europea richiamata nell'allegato I. In questi casi l'AI Act si coordina con le regole settoriali già applicabili al prodotto. Il sistema di IA non viene valutato separatamente dal bene nel quale è incorporato quando la sua funzione incide sulla sicurezza complessiva. I requisiti introdotti dal regolamento si integrano pertanto nelle procedure previste dalla normativa europea di armonizzazione, con l'obiettivo di evitare duplicazioni e assicurare che la valutazione consideri sia i rischi tradizionalmente associati al prodotto sia quelli derivanti dalla componente algoritmica. Il secondo gruppo è costituito dai sistemi utilizzati nei settori elencati nell'allegato III. In tali ambiti l'alto rischio deriva dalla capacità dell'applicazione di incidere in modo significativo sulla vita delle persone, sulle loro opportunità o sulla possibilità di esercitare diritti riconosciuti dall'ordinamento. L'allegato non considera indiscriminatamente rischioso ogni impiego dell'IA all'interno di un determinato settore, ma individua precise finalità d'uso. Il primo ambito riguarda la biometria. Sono compresi determinati sistemi destinati all'identificazione biometrica remota, alla categorizzazione biometrica sulla base di attributi o caratteristiche sensibili o protette e al riconoscimento delle emozioni. La qualificazione come ad alto rischio opera soltanto per le applicazioni non già vietate dall'articolo 5. Il regolamento distingue inoltre l'identificazione biometrica dalla verifica dell'identità, utilizzata esclusivamente per accertare che una persona sia

¹⁰³ Ivi, art. 3, punto 14.

effettivamente chi dichiara di essere. Quest'ultima, considerata meno invasiva, non rientra automaticamente nella categoria dell'alto rischio. Il secondo settore comprende le infrastrutture critiche. Sono classificati come ad alto rischio i sistemi utilizzati come componenti di sicurezza nella gestione o nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed energia elettrica. Un errore o un malfunzionamento in tali contesti può mettere in pericolo la vita e l'incolumità delle persone, interrompere servizi essenziali o produrre conseguenze su una parte estesa della popolazione.¹⁰⁴ Un terzo ambito è rappresentato dall'istruzione e dalla formazione professionale. Rientrano nell'alto rischio i sistemi utilizzati per determinare l'accesso o l'ammissione a istituti e percorsi formativi, assegnare le persone a programmi o livelli di istruzione, valutare i risultati dell'apprendimento e orientare il percorso educativo. Sono comprese anche determinate applicazioni impiegate per controllare o individuare comportamenti vietati durante le prove. Questi strumenti possono condizionare le possibilità formative e professionali degli interessati e richiedono quindi una particolare attenzione alla qualità dei dati, alla non discriminazione e alla possibilità di controllo umano. L'allegato III include poi i sistemi utilizzati nell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo. Sono considerati ad alto rischio, tra gli altri, quelli impiegati per pubblicare annunci mirati, selezionare candidature, analizzare curriculum e valutare i candidati. Lo stesso regime riguarda i sistemi che incidono sulle condizioni dei rapporti di lavoro, sulle promozioni, sull'assegnazione dei compiti, sulla cessazione del rapporto oppure sul monitoraggio e sulla valutazione delle prestazioni e del comportamento dei lavoratori. L'uso dell'IA in tali contesti può incidere direttamente sul diritto al lavoro, sulla protezione contro le discriminazioni e

¹⁰⁴ Ivi, allegato III, punti 1-2; considerando 54-55.

sulla riservatezza, in una relazione caratterizzata da un evidente squilibrio tra le parti.¹⁰⁵ Particolarmente rilevante per la Pubblica Amministrazione è la categoria relativa all'accesso a servizi e prestazioni essenziali, pubblici e privati. Sono classificati come ad alto rischio i sistemi impiegati dalle autorità pubbliche, o per loro conto, per valutare l'ammissibilità delle persone a prestazioni e servizi essenziali di assistenza pubblica, compresi quelli utilizzati per concederli, ridurli, revocarli o richiederne la restituzione. Possono rientrare in questa categoria strumenti impiegati nell'ambito della previdenza, dell'assistenza sociale, del sostegno economico e di altre misure dalle quali dipendono condizioni fondamentali di vita. Il ricorso all'IA in questi procedimenti può migliorare la capacità dell'amministrazione di elaborare le domande e verificare i requisiti, ma può anche produrre conseguenze particolarmente gravi se il sistema utilizza dati inesatti, applica criteri distorti o non considera correttamente le circostanze individuali. La qualificazione come ad alto rischio mira quindi a impedire che l'automazione comprometta l'accesso a prestazioni necessarie per la dignità e l'inclusione sociale della persona. Nello stesso settore sono ricompresi i sistemi destinati a valutare l'affidabilità creditizia o stabilire il merito creditizio delle persone fisiche, fatta eccezione per quelli utilizzati esclusivamente per individuare frodi finanziarie. Sono inoltre inclusi i sistemi impiegati nella valutazione del rischio e nella determinazione dei prezzi delle assicurazioni sulla vita e sanitarie. L'allegato considera infine i sistemi destinati a valutare e classificare le chiamate di emergenza o a stabilire la priorità nell'intervento dei servizi di polizia, vigili del fuoco e assistenza medica, compresi quelli utilizzati nei sistemi di triage sanitario d'urgenza. In questi casi l'output dell'IA può influire sulla tempestività e sulla natura dell'assistenza ricevuta.¹⁰⁶ Un altro ambito riguarda le attività di contrasto. Sono considerate ad alto rischio, nei limiti

¹⁰⁵ Ivi, allegato III, punti 3-4; considerando 56-57.

¹⁰⁶ Ivi, allegato III, punto 5; considerando 58.

previsti dall'allegato III e purché il loro utilizzo sia consentito dal diritto applicabile, determinate applicazioni destinate a valutare il rischio che una persona diventi vittima di un reato, a esaminare l'affidabilità degli elementi di prova, a valutare il rischio che una persona commetta o reiteri un reato sulla base di elementi oggettivi già collegati a un'attività criminosa e a effettuare la profilazione nel corso dell'accertamento, dell'indagine o del perseguimento di un reato. Vi rientrano anche gli strumenti assimilabili a poligrafi e quelli destinati a rilevare lo stato emotivo. Le attività di contrasto incidono sulla libertà personale, sulla presunzione di innocenza, sulla vita privata e sull'accesso alla giustizia; per questa ragione l'impiego dell'IA deve rimanere circoscritto e sottoposto a garanzie effettive. L'allegato III comprende inoltre alcuni sistemi utilizzati nella migrazione, nell'asilo e nella gestione delle frontiere. Possono essere classificati come ad alto rischio gli strumenti destinati a valutare rischi per la sicurezza, di immigrazione irregolare o sanitari, esaminare domande di asilo, visto o permesso di soggiorno, verificare l'autenticità dei documenti e assistere l'identificazione delle persone. Anche in questo settore sono richiamati i sistemi assimilabili a poligrafi e quelli destinati a inferire emozioni. L'eventuale errore può incidere sulla possibilità di entrare o permanere nel territorio dell'Unione e sull'accesso alla protezione internazionale, con conseguenze particolarmente rilevanti per persone che possono trovarsi in condizioni di vulnerabilità.¹⁰⁷ L'ultimo ambito riguarda l'amministrazione della giustizia e i processi democratici. Sono ad alto rischio i sistemi destinati a essere utilizzati da un'autorità giudiziaria, o per suo conto, per assisterla nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a un caso concreto. La classificazione riguarda anche strumenti impiegati in forme alternative di risoluzione delle controversie quando producono effetti analoghi. L'IA può sostenere attività documentali e

¹⁰⁷ Ivi, allegato III, punti 6-7; considerando 59-60.

conoscitive, ma non deve compromettere l'indipendenza del giudice, il diritto a un processo equo e la responsabilità umana nella decisione. Sono inoltre ricompresi i sistemi destinati a influenzare l'esito di elezioni o referendum oppure il comportamento di voto delle persone fisiche. Restano esclusi gli strumenti utilizzati per attività puramente amministrative o logistiche che non interagiscono direttamente con gli elettori e non incidono sulle loro scelte. L'inclusione di questo settore riflette la necessità di tutelare la libertà di formazione della volontà politica e il corretto funzionamento dei processi democratici.¹⁰⁸ La particolare rilevanza dell'allegato III per le amministrazioni pubbliche emerge dalla presenza di numerosi ambiti nei quali gli enti possono agire come utilizzatori dei sistemi. Prestazioni sociali, istruzione, servizi di emergenza, attività di contrasto, gestione delle frontiere e amministrazione della giustizia sono settori nei quali l'IA può intervenire in procedimenti capaci di produrre effetti diretti sulla posizione degli individui. La responsabilità dell'amministrazione non viene meno quando il sistema è acquistato da un fornitore esterno o impiegato soltanto come strumento di supporto: l'ente deve comunque assicurare che il suo utilizzo sia compatibile con la finalità istituzionale e con le garanzie previste dall'ordinamento. La presenza di un sistema tra i casi indicati nell'allegato III non comporta sempre l'applicazione automatica del regime dell'alto rischio. L'articolo 6, paragrafo 3, esclude tale qualificazione quando il sistema non presenta un rischio significativo per la salute, la sicurezza o i diritti fondamentali e non influenza materialmente il risultato del processo decisionale. Ciò può avvenire se l'applicazione esegue un compito procedurale ristretto, migliora il risultato di un'attività umana già completata, individua modelli o deviazioni senza sostituire o influenzare una valutazione umana precedentemente svolta oppure compie un'attività meramente preparatoria.

¹⁰⁸ Ivi, allegato III, punto 8; considerando 61-62.

L'eccezione deve essere interpretata restrittivamente e non può essere fondata su una dichiarazione generica del fornitore. Prima dell'immissione sul mercato o della messa in servizio, il soggetto interessato deve documentare la valutazione compiuta ed essere in grado di presentarla alle autorità nazionali competenti. Il sistema deve inoltre essere registrato nella banca dati dell'Unione secondo le modalità previste dal regolamento. La profilazione delle persone fisiche costituisce un limite invalicabile, un sistema ricompreso nell'allegato III che effettua profilazione è sempre considerato ad alto rischio.¹⁰⁹ L'elenco dei sistemi non è immutabile. L'articolo 7 consente alla Commissione di aggiungere o modificare mediante atti delegati i casi d'uso dell'allegato III, purché essi appartengano a uno dei settori già indicati e presentino un rischio equivalente o superiore a quello delle applicazioni già incluse. La valutazione deve considerare, tra gli altri elementi, la finalità prevista, l'ampiezza dell'utilizzo, la natura e la quantità dei dati trattati, il grado di autonomia, la possibilità di intervento umano, il numero e la vulnerabilità delle persone interessate, la probabilità e la gravità del danno e la possibilità di porvi rimedio. La Commissione può anche rimuovere un sistema dall'allegato III quando esso non presenti più rischi significativi e quando la soppressione non riduca il livello generale di protezione garantito dal diritto dell'Unione. Questa possibilità rende la classificazione adattabile all'evoluzione tecnologica e all'esperienza applicativa, evitando che il quadro normativo rimanga legato a una valutazione effettuata in un determinato momento storico.¹¹⁰ La categoria dell'alto rischio rappresenta dunque il principale punto di equilibrio tra innovazione e tutela. Il regolamento non impedisce l'utilizzo dell'IA nei settori più delicati, ma subordina tale possibilità alla presenza di condizioni capaci di ridurre i pericoli e rendere verificabile il funzionamento del sistema. Una volta individuata la natura ad alto rischio

¹⁰⁹ Ivi, art. 6, parr. 3-4, e art. 49, par. 2.

¹¹⁰ Ivi, art. 7.

dell'applicazione, occorre stabilire quali requisiti debba rispettare e quali obblighi ricadano sui soggetti coinvolti nella sua progettazione, distribuzione e utilizzazione.

3.5 Requisiti e obblighi previsti dall'AI Act

La qualificazione di un sistema di intelligenza artificiale come ad alto rischio determina l'applicazione di un insieme coordinato di requisiti tecnici, organizzativi e documentali. L'AI Act non si limita a individuare gli impieghi maggiormente delicati, ma stabilisce le condizioni alle quali tali sistemi possono essere sviluppati, immessi sul mercato, messi in servizio e utilizzati nell'Unione europea. La disciplina segue una logica preventiva: i rischi devono essere individuati e ridotti prima che il sistema produca effetti sulle persone, senza escludere controlli successivi durante il suo funzionamento.

Il regolamento distingue tra i requisiti che devono essere rispettati dal sistema e gli obblighi attribuiti ai soggetti che intervengono nella catena di sviluppo, commercializzazione e utilizzo. Questa separazione consente di distribuire le responsabilità tra fornitori, rappresentanti autorizzati, importatori, distributori e deployer, evitando che il rispetto della normativa dipenda da un unico attore. L'intensità degli adempimenti varia in relazione al ruolo concretamente assunto e alla capacità di incidere sulla sicurezza e sull'affidabilità dell'applicazione.¹¹¹

Il primo requisito riguarda l'istituzione di un sistema di gestione dei rischi. Esso deve accompagnare l'intero ciclo di vita dell'IA ed essere aggiornato in modo continuativo. Il fornitore è tenuto a individuare e analizzare i rischi conosciuti o ragionevolmente prevedibili, valutando sia quelli che possono emergere quando il sistema viene impiegato conformemente alla sua finalità prevista, sia quelli derivanti da usi impropri ragionevolmente prevedibili. Sulla base dei risultati

¹¹¹ Regolamento (UE) 2024/1689, artt. 8, 16 e 26.

devono essere adottate misure adeguate di prevenzione e attenuazione, verificandone l'efficacia mediante prove e controlli. La gestione del rischio non consiste in una valutazione svolta una sola volta prima dell'immissione sul mercato. Le prestazioni del sistema possono mutare in seguito ad aggiornamenti, variazioni dei dati o cambiamenti del contesto operativo. È quindi necessario considerare le informazioni raccolte durante il monitoraggio successivo all'immissione sul mercato e riesaminare le misure adottate quando emergono nuovi pericoli o effetti inattesi. Il regolamento richiede inoltre che il rischio residuo, dopo l'applicazione delle misure di mitigazione, sia ritenuto accettabile alla luce della finalità del sistema e dei benefici attesi.¹¹²

Un secondo requisito riguarda i dati utilizzati per l'addestramento, la convalida e la prova dei sistemi. La qualità degli output dipende in misura significativa dalle caratteristiche delle informazioni elaborate. Per questo motivo l'articolo 10 richiede pratiche adeguate di governance e gestione dei dati, comprendenti la definizione delle scelte progettuali, l'esame della provenienza delle informazioni, la preparazione dei set di dati, l'individuazione di lacune o distorsioni e la valutazione della loro possibile incidenza sui diritti fondamentali.

I dati devono essere pertinenti, sufficientemente rappresentativi e, per quanto possibile, privi di errori e completi rispetto alla finalità prevista. La rappresentatività non implica che ogni insieme di dati debba riprodurre indistintamente l'intera popolazione, ma che esso risulti adeguato alle persone e ai contesti sui quali il sistema sarà utilizzato. Particolare attenzione deve essere dedicata ai possibili bias capaci di determinare effetti discriminatori o di compromettere la sicurezza. La qualità dei dati costituisce quindi una condizione essenziale per l'affidabilità dell'intero sistema e non un semplice adempimento preliminare.

¹¹² Ivi, art. 9.

Il regolamento ammette, entro limiti rigorosi, il trattamento di categorie particolari di dati personali quando esso sia strettamente necessario per individuare e correggere distorsioni. Tale possibilità non elimina l'applicazione della disciplina europea sulla protezione dei dati, ma richiede garanzie specifiche, tra cui limitazioni all'accesso, misure di sicurezza, documentazione delle ragioni del trattamento e cancellazione delle informazioni quando non siano più necessarie.¹¹³

I sistemi ad alto rischio devono inoltre essere accompagnati da una documentazione tecnica predisposta prima della loro immissione sul mercato o messa in servizio e mantenuta aggiornata. Tale documentazione deve consentire alle autorità e agli organismi competenti di verificare la conformità del sistema. Deve quindi descrivere, con un livello di dettaglio adeguato, la finalità prevista, le caratteristiche tecniche, il processo di sviluppo, i dati utilizzati, le procedure di prova, le misure di gestione del rischio, le prestazioni attese e i limiti conosciuti. La documentazione svolge una funzione di tracciabilità e responsabilizzazione. Essa permette di ricostruire le principali scelte progettuali e di valutare se il sistema sia stato sviluppato in conformità alle prescrizioni dell'AI Act. Non deve essere considerata un documento statico: modifiche significative, aggiornamenti o variazioni delle prestazioni devono essere adeguatamente registrati, affinché le informazioni disponibili riflettano il funzionamento effettivo della tecnologia.

A questa esigenza si collega l'obbligo di registrazione automatica degli eventi, comunemente indicata come logging. I sistemi ad alto rischio devono essere progettati in modo da consentire la registrazione delle operazioni rilevanti durante il loro funzionamento. I log permettono di individuare situazioni di rischio, malfunzionamenti, usi non conformi e variazioni delle prestazioni. Essi

¹¹³ Ivi, art. 10, parr. 2-5.

possono inoltre facilitare il monitoraggio successivo all'immissione sul mercato e la ricostruzione delle circostanze nelle quali si è verificato un incidente.

Il regolamento non richiede la conservazione indiscriminata di qualsiasi informazione generata dal sistema. La registrazione deve essere adeguata alla finalità e alla natura dell'applicazione, rispettando le norme sulla protezione dei dati e sulla riservatezza. Nei sistemi particolarmente delicati, come quelli biometrici, i log devono consentire di ricostruire elementi specifici dell'utilizzo, inclusi il periodo di funzionamento e i dati di riferimento impiegati.¹¹⁴

Un ulteriore requisito è rappresentato dalla trasparenza verso il deployer. Il sistema deve essere progettato in modo che il suo funzionamento risulti sufficientemente comprensibile a chi lo utilizza professionalmente. Il fornitore deve accompagnarlo con istruzioni chiare, complete, corrette e accessibili, contenenti le informazioni necessarie per impiegarlo conformemente alla finalità prevista e interpretarne adeguatamente gli output.

Le istruzioni devono indicare, tra l'altro, le caratteristiche e le prestazioni del sistema, i limiti conosciuti, il livello di accuratezza, le circostanze che possono influire sul funzionamento, le misure di sorveglianza umana, le risorse tecniche necessarie e le modalità di manutenzione. Devono inoltre rendere noti i rischi residui e gli usi impropri ragionevolmente prevedibili. La trasparenza richiesta non comporta necessariamente la divulgazione integrale del codice sorgente, ma deve offrire al deployer gli elementi indispensabili per utilizzare il sistema in modo consapevole e controllabile.

La sorveglianza umana costituisce un requisito autonomo e centrale. I sistemi ad alto rischio devono essere progettati affinché persone dotate di competenze, formazione e autorità adeguate possano comprenderne le capacità e i limiti, riconoscere risultati anomali e intervenire quando necessario. Il controllo umano

¹¹⁴ Ivi, artt. 11-12 e allegato IV.

non può ridursi alla presenza formale di un operatore incaricato di confermare automaticamente gli output prodotti dall'IA.

Le misure di sorveglianza devono consentire di evitare un affidamento eccessivo nei confronti del risultato algoritmico, fenomeno noto come automation bias. Chi esercita il controllo deve poter interpretare correttamente l'output, decidere di non utilizzarlo, annullarlo o modificarlo e interrompere il funzionamento del sistema quando emergano rischi. Nei sistemi di identificazione biometrica remota, il regolamento prevede inoltre specifiche verifiche da parte di persone competenti prima che il risultato possa produrre conseguenze.¹¹⁵

Accuratezza, robustezza e ciphersicurezza costituiscono l'ultimo gruppo di requisiti previsto per i sistemi ad alto rischio. Il livello di accuratezza deve essere adeguato alla finalità prevista e dichiarato nelle istruzioni per l'uso. Le prestazioni devono essere mantenute per tutta la durata di funzionamento, tenendo conto dei possibili errori derivanti dall'interazione con l'ambiente, con altri sistemi o con le persone.

La robustezza riguarda la capacità dell'applicazione di resistere a errori, guasti e condizioni impreviste senza generare conseguenze pericolose. Devono essere predisposte misure tecniche e organizzative per prevenire o ridurre i rischi derivanti da anomalie e assicurare un comportamento sufficientemente stabile. Per i sistemi che continuano ad apprendere dopo la messa in servizio, occorre limitare il rischio che output errati vengano utilizzati come nuovi dati di ingresso e producano progressivamente risultati distorti. La ciphersicurezza mira invece a proteggere il sistema da tentativi di alterazione, accessi non autorizzati o manipolazione dei dati e dei modelli. Le misure adottate devono essere proporzionate alle circostanze e considerare forme di attacco specificamente rivolte all'intelligenza artificiale, come la contaminazione dei dati di

¹¹⁵ Ivi, artt. 13-14.

addestramento, la manipolazione degli input o lo sfruttamento delle vulnerabilità del modello. Accuratezza, robustezza e sicurezza informatica concorrono quindi a garantire che il sistema mantenga prestazioni affidabili anche in presenza di condizioni avverse.¹¹⁶

Il rispetto dei requisiti tecnici ricade principalmente sul fornitore, vale a dire sul soggetto che sviluppa un sistema di IA o lo fa sviluppare e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio. Il fornitore deve assicurare la conformità agli articoli 8-15, istituire un sistema di gestione della qualità, predisporre e conservare la documentazione, mantenere i log generati sotto il proprio controllo e sottoporre il sistema alla procedura di valutazione della conformità applicabile.

Prima dell'immissione sul mercato o della messa in servizio, il fornitore deve redigere la dichiarazione UE di conformità, apporre la marcatura CE e adempiere agli obblighi di registrazione. Deve inoltre adottare misure correttive quando ritiene che un sistema non sia conforme, informare i soggetti coinvolti e cooperare con le autorità competenti. Gli adempimenti proseguono dopo la commercializzazione mediante il monitoraggio delle prestazioni e la segnalazione degli incidenti gravi.¹¹⁷

Quando il fornitore è stabilito fuori dall'Unione europea, deve nominare un rappresentante autorizzato nell'Unione prima di rendere disponibile il sistema. Il rappresentante svolge i compiti indicati nel mandato, verifica l'esistenza della documentazione e coopera con le autorità. Tale figura assicura che vi sia un soggetto identificabile all'interno dell'Unione al quale possano essere rivolte richieste e controlli.

Gli importatori devono verificare, prima dell'immissione sul mercato, che il fornitore abbia completato la valutazione della conformità, predisposto la

¹¹⁶ Ivi, art. 15.

¹¹⁷ Ivi, artt. 16-21.

documentazione richiesta, apposto la marcatura CE e nominato, quando necessario, un rappresentante autorizzato. Se ritengono che il sistema non sia conforme o presenti rischi, non possono renderlo disponibile finché la situazione non sia stata regolarizzata. Devono inoltre indicare la propria identità e garantire che le condizioni di conservazione e trasporto non compromettano la conformità. I distributori sono tenuti a controllare la presenza della marcatura CE, della documentazione e delle istruzioni richieste. Anch'essi devono astenersi dal rendere disponibile un sistema che ritengano non conforme e informare il fornitore, l'importatore e le autorità quando emergano rischi. Pur non partecipando direttamente allo sviluppo, importatori e distributori assumono quindi una funzione di verifica all'interno della catena di fornitura.

Il regolamento disciplina anche le ipotesi nelle quali un distributore, un importatore, un deployer o un altro soggetto viene considerato fornitore. Ciò avviene, ad esempio, quando appone il proprio nome o marchio su un sistema ad alto rischio già immesso sul mercato, ne modifica la finalità prevista oppure introduce una modifica sostanziale. In queste circostanze il soggetto assume gli obblighi propri del fornitore, poiché le sue decisioni incidono sull'identità, sulla destinazione o sul funzionamento dell'applicazione.¹¹⁸

Il deployer è la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, salvo gli impieghi effettuati nell'ambito di un'attività personale non professionale. I suoi obblighi sono differenti da quelli del fornitore, perché riguardano il modo concreto in cui il sistema viene inserito nell'organizzazione e utilizzato nei processi decisionali.

Il deployer deve utilizzare il sistema conformemente alle istruzioni e predisporre misure di sorveglianza umana affidate a persone competenti e adeguatamente

¹¹⁸ Ivi, artt. 22-25.

formate. Quando esercita il controllo sui dati di input, deve assicurare che essi siano pertinenti e sufficientemente rappresentativi rispetto alla finalità prevista. È inoltre tenuto a monitorare il funzionamento e a informare il fornitore o il distributore qualora emergano rischi, incidenti o risultati incompatibili con l'uso previsto.

I log generati automaticamente devono essere conservati dal deployer quando si trovano sotto il suo controllo per un periodo adeguato alla finalità prevista e, in ogni caso, per almeno sei mesi, salvo che il diritto dell'Unione o nazionale applicabile disponga diversamente. Se il sistema viene utilizzato sul luogo di lavoro, i rappresentanti dei lavoratori e i dipendenti interessati devono essere informati prima della sua introduzione. I deployer pubblici o i soggetti che forniscono servizi pubblici sono inoltre sottoposti a specifici obblighi di registrazione e trasparenza, che assumono particolare rilievo per le amministrazioni e saranno approfonditi nel capitolo successivo.¹¹⁹

Prima di utilizzare determinati sistemi ad alto rischio, gli organismi di diritto pubblico e i soggetti privati che forniscono servizi pubblici devono effettuare una valutazione d'impatto sui diritti fondamentali. Lo stesso obbligo riguarda alcuni operatori che impiegano sistemi per la valutazione del merito creditizio o per le assicurazioni sulla vita e sanitarie. La valutazione deve descrivere il processo nel quale il sistema sarà utilizzato, la durata e la frequenza dell'impiego, le persone interessate, i rischi specifici e le misure previste per affrontarli.

La valutazione d'impatto deve essere effettuata prima del primo utilizzo e aggiornata quando cambiano gli elementi rilevanti. Essa non sostituisce l'eventuale valutazione d'impatto sulla protezione dei dati prevista dal GDPR, ma può essere coordinata con quest'ultima. La sua funzione è verificare

¹¹⁹ Ivi, art. 26.

preventivamente le conseguenze dell'uso del sistema sui diritti fondamentali e documentare le misure adottate per limitarle.¹²⁰

Prima di essere immessi sul mercato o messi in servizio, i sistemi ad alto rischio devono essere sottoposti a una valutazione della conformità. La procedura serve a verificare il rispetto dei requisiti stabiliti dal regolamento e varia in funzione della categoria del sistema. In alcuni casi può essere svolta dal fornitore mediante un controllo interno; in altri è necessario l'intervento di un organismo notificato indipendente, soprattutto quando il sistema è collegato a prodotti già sottoposti a valutazione da parte di terzi o quando ricorrono le condizioni previste dalla normativa.

Una nuova valutazione è richiesta quando il sistema subisce una modifica sostanziale, ossia un cambiamento non previsto nella valutazione iniziale capace di incidere sulla conformità o sulla finalità prevista. Non ogni aggiornamento comporta automaticamente una nuova procedura: occorre verificare se la modifica alteri in modo rilevante il funzionamento, i rischi o le condizioni nelle quali il sistema era stato originariamente valutato.¹²¹

Per i sistemi ad alto rischio di cui all'articolo 6, paragrafo 2, il fornitore o il rappresentante autorizzato deve effettuare la registrazione nella banca dati dell'Unione prima dell'immissione sul mercato o della messa in servizio. Anche le autorità pubbliche, le istituzioni, gli organi e gli organismi dell'Unione che intendono utilizzare tali sistemi devono registrarsi come deployer e registrare l'impiego del sistema prima di procedere al suo utilizzo. Per determinate applicazioni nei settori del contrasto, della migrazione, dell'asilo e del controllo delle frontiere sono previste sezioni non accessibili al pubblico, al fine di tutelare esigenze di sicurezza e riservatezza.¹²² La registrazione favorisce la trasparenza

¹²⁰ Ivi, art. 27.

¹²¹ Ivi, art. 3, punto 23, e art. 43.

¹²² Ivi, art. 49 e art. 71.

e consente alle autorità di conoscere le applicazioni disponibili e i soggetti responsabili. Per alcune categorie utilizzate dalle autorità di contrasto, nel settore della migrazione o in altri ambiti sensibili sono previste modalità di registrazione non accessibili pubblicamente, al fine di tutelare esigenze di sicurezza e riservatezza. La conformità non esaurisce gli obblighi del fornitore. Dopo l'immissione sul mercato deve essere istituito un sistema di monitoraggio finalizzato a raccogliere e analizzare in modo sistematico le informazioni sulle prestazioni dell'IA durante il suo utilizzo. Il monitoraggio consente di individuare problemi non emersi nelle prove iniziali e di aggiornare la gestione dei rischi, la documentazione e le misure correttive.

Gli incidenti gravi devono essere segnalati alle autorità competenti secondo le modalità e i termini stabiliti dal regolamento. Sono considerati gravi gli eventi che, direttamente o indirettamente, abbiano causato la morte o un grave danno alla salute, una perturbazione grave e irreversibile della gestione o del funzionamento di infrastrutture critiche, la violazione di obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali oppure gravi danni alla proprietà o all'ambiente. Il fornitore deve svolgere le indagini necessarie e collaborare con le autorità senza compromettere l'eventuale valutazione delle cause.¹²³

Accanto alla disciplina dell'alto rischio, l'AI Act prevede obblighi di trasparenza per alcuni sistemi indipendentemente dalla loro classificazione. I sistemi destinati a interagire direttamente con persone fisiche devono rendere riconoscibile la natura artificiale dell'interazione, salvo che ciò sia evidente. I fornitori di sistemi che generano contenuti sintetici devono inoltre assicurare che gli output siano marcati in un formato leggibile da una macchina e identificabili come artificialmente generati o manipolati.

¹²³ Ivi, art. 3, punto 49, e artt. 72-73.

Ulteriori obblighi ricadono sui deployer di sistemi di riconoscimento delle emozioni o categorizzazione biometrica, che devono informare le persone esposte al loro funzionamento. La natura artificiale dei deep fake deve essere dichiarata, mentre per testi generati o manipolati dall'IA e pubblicati allo scopo di informare il pubblico su questioni di interesse generale è richiesta un'apposita indicazione, salvo i casi nei quali il contenuto sia stato sottoposto a revisione umana e una persona fisica o giuridica ne assuma la responsabilità editoriale. Questi obblighi perseguono lo scopo di consentire ai destinatari di valutare consapevolmente l'origine dell'interazione o del contenuto.¹²⁴

Una disciplina distinta riguarda i modelli di IA per finalità generali. Il fornitore deve predisporre e mantenere aggiornata la documentazione tecnica del modello, mettere a disposizione dei fornitori dei sistemi che lo integrano le informazioni necessarie a comprenderne capacità e limiti e adottare una politica diretta al rispetto del diritto d'autore dell'Unione. Deve inoltre pubblicare una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento, secondo il modello predisposto dall'Ufficio per l'IA. Per i fornitori stabiliti in Paesi terzi è prevista la nomina di un rappresentante autorizzato nell'Unione, salvo le eccezioni stabilite dal regolamento. Gli obblighi possono essere precisati mediante codici di buone pratiche e norme armonizzate, che favoriscono l'applicazione uniforme della disciplina senza eliminare la responsabilità del fornitore.

Quando un modello di IA per finalità generali presenta un rischio sistemico, si applicano prescrizioni aggiuntive. Il fornitore deve effettuare valutazioni adeguate, comprese prove avversariali, individuare e attenuare i possibili rischi sistemici a livello dell'Unione, documentare e comunicare gli incidenti gravi e garantire un livello adeguato di cibersecurity. Questi obblighi tengono conto

¹²⁴ Ivi, art. 50.

della capacità dei modelli più potenti di essere integrati in numerosi sistemi e di produrre effetti estesi su settori e utenti differenti.¹²⁵

L'insieme delle disposizioni esaminate mostra che l'AI Act costruisce un sistema di responsabilità distribuita lungo l'intero ciclo di vita dell'intelligenza artificiale. I requisiti tecnici mirano a rendere i sistemi affidabili e controllabili, mentre gli obblighi attribuiti agli operatori assicurano che la conformità venga verificata prima e dopo l'immissione sul mercato. La distinzione dei ruoli non frammenta la responsabilità, ma individua gli adempimenti corrispondenti alla capacità di ciascun soggetto di incidere sul funzionamento e sull'utilizzo della tecnologia.

Per la Pubblica Amministrazione tale disciplina assume un'importanza particolare. Gli enti pubblici possono trovarsi nella posizione di deployer, ma possono anche sviluppare direttamente sistemi, modificarne la finalità o affidarli a soggetti esterni. L'individuazione del ruolo concretamente assunto determina gli obblighi applicabili e incide sulle modalità di organizzazione, controllo e documentazione dell'impiego dell'IA.

¹²⁵ Ivi, artt. 51-55.

CAPITOLO 4

L'IMPATTO DELL'AI ACT SULLA PUBBLICA AMMINISTRAZIONE

4.1 Gli obblighi per le amministrazioni pubbliche

L'applicazione dell'AI Act alla Pubblica Amministrazione determina un cambiamento significativo nelle modalità con cui gli enti pubblici possono introdurre e utilizzare sistemi di intelligenza artificiale. Il regolamento non considera infatti l'amministrazione come un semplice utilizzatore passivo della tecnologia, ma le attribuisce obblighi specifici in relazione al ruolo assunto, alla finalità del sistema e al livello di rischio connesso al suo impiego. Nella maggior parte dei casi, quando utilizza un sistema di IA sviluppato da un soggetto esterno nell'ambito delle proprie attività istituzionali, l'amministrazione assume la qualifica di *deployer*, definita dall'AI Act come il soggetto, compresa un'autorità pubblica, che utilizza un sistema di IA sotto la propria autorità.¹²⁶

La qualificazione come *deployer* comporta innanzitutto la necessità di conoscere con precisione il sistema utilizzato e il contesto nel quale viene inserito. Non è quindi sufficiente acquistare una soluzione tecnologica dichiarata conforme dal fornitore. L'amministrazione deve verificare la finalità concreta per la quale intende utilizzarla, il procedimento nel quale verrà integrata, le persone potenzialmente interessate e la rilevanza degli output prodotti. Questo passaggio è particolarmente importante perché la classificazione del sistema dipende dalla funzione effettivamente svolta. Le linee guida pubblicate in forma di bozza dalla Commissione europea nel maggio 2026 confermano che la finalità prevista costituisce uno degli elementi centrali per stabilire se un sistema debba essere

¹²⁶ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, 13 giugno 2024, art. 3, punto 4 e considerando 13.

considerato ad alto rischio e chiariscono che la presenza di un operatore umano non è, da sola, sufficiente a escludere tale classificazione.¹²⁷

Per la Pubblica Amministrazione ciò implica la necessità di distinguere gli strumenti utilizzati per attività meramente preparatorie o procedurali da quelli che incidono concretamente su valutazioni o decisioni riguardanti le persone. Un sistema impiegato esclusivamente per organizzare documenti, convertire formati o svolgere compiti amministrativi circoscritti presenta un impatto diverso rispetto a un sistema che attribuisce punteggi, ordina candidati, formula raccomandazioni individuali o contribuisce alla decisione sull'accesso a una prestazione pubblica. Le linee guida della Commissione del 2026 precisano che alcune attività strettamente procedurali possono, in determinate condizioni, non comportare la classificazione ad alto rischio; le eccezioni devono essere interpretate restrittivamente, soprattutto quando l'IA è in grado di influenzare in modo sostanziale l'esito di una decisione.¹²⁸

Una volta individuata la natura del sistema, assume particolare rilievo l'articolo 26 dell'AI Act, che disciplina gli obblighi dei *deployer* dei sistemi di IA ad alto rischio. L'amministrazione deve adottare misure tecniche e organizzative adeguate affinché il sistema sia utilizzato conformemente alle istruzioni fornite dal produttore. Ciò richiede una regolamentazione interna dell'impiego dell'IA, con l'individuazione dei soggetti autorizzati all'utilizzo, delle finalità ammesse e delle procedure da seguire in caso di anomalie o risultati inattesi. L'uso della tecnologia deve quindi essere inserito in un processo amministrativo definito, evitando che strumenti destinati a determinate funzioni vengano utilizzati in modo informale o per finalità differenti.¹²⁹

¹²⁷ Commissione europea, *Draft Guidelines on the classification of high-risk AI systems*, 19 maggio 2026, ai sensi dell'art. 6, par. 5, del Regolamento (UE) 2024/1689.

¹²⁸ Commissione europea, *Draft Guidelines on the classification of high-risk AI systems*, 2026, sezione relativa all'art. 6, parr. 2 e 3; DLA Piper, *EU Commission draft guidelines on classification of "high-risk" AI systems: Key points*, 2026

¹²⁹ Regolamento (UE) 2024/1689, art. 26, par. 1.

A questo obbligo si collega la sorveglianza umana. Nei sistemi ad alto rischio il controllo deve essere affidato a persone dotate di competenze, formazione, autorità e sostegno adeguati. Il funzionario incaricato non deve limitarsi a confermare automaticamente il risultato prodotto dal sistema, ma deve essere in grado di comprenderne la funzione, riconoscere eventuali anomalie e, quando necessario, discostarsi dall'output o interrompere l'utilizzo dello strumento. Per un'amministrazione pubblica questo aspetto assume particolare rilevanza nei procedimenti che possono incidere sulla posizione di cittadini, lavoratori o utenti dei servizi pubblici. Il controllo umano diventa quindi parte integrante dell'organizzazione del procedimento e non un adempimento meramente formale.¹³⁰

Il *deployer* deve inoltre monitorare il funzionamento del sistema sulla base delle istruzioni ricevute e intervenire quando ritenga che il suo utilizzo possa determinare un rischio. Quando i dati di input sono sotto il controllo dell'amministrazione, questa deve assicurarsi che siano pertinenti e sufficientemente rappresentativi rispetto alla finalità prevista. Nei casi stabiliti dal regolamento deve inoltre conservare i registri generati automaticamente dal sistema. Tali obblighi rafforzano la necessità di documentare l'intero ciclo di utilizzo dell'IA, in modo da rendere ricostruibili le modalità con cui il sistema è stato impiegato e gli eventuali problemi emersi durante il suo funzionamento.¹³¹

Il regolamento prevede inoltre obblighi specifici quando i sistemi ad alto rischio sono utilizzati da autorità pubbliche. Prima della messa in servizio, nei casi previsti, l'amministrazione deve verificare l'avvenuta registrazione del sistema nella banca dati europea.¹³² Sono inoltre previsti obblighi informativi nei confronti delle persone interessate e dei lavoratori quando il sistema viene

¹³⁰ Regolamento (UE) 2024/1689, art. 26, par. 2.

¹³¹ Regolamento (UE) 2024/1689, art. 26, par. 4 e 5.

¹³² Regolamento (UE) 2024/1689, art. 49, par. 3.

utilizzato in contesti che possono incidere sulla loro posizione. Questi profili saranno approfonditi nel paragrafo dedicato alla trasparenza e all'*accountability*, mentre in questa sede rileva soprattutto il fatto che l'impiego dell'IA non può avvenire in maniera occulta o completamente separata dalle regole che disciplinano l'attività amministrativa.

Un ulteriore adempimento di particolare importanza per il settore pubblico è rappresentato dalla valutazione d'impatto sui diritti fondamentali prevista dall'articolo 27 dell'AI Act. Gli organismi di diritto pubblico e gli altri soggetti indicati dalla disposizione devono, prima di utilizzare determinati sistemi ad alto rischio, valutare le conseguenze che il loro impiego può produrre sulle persone interessate. La valutazione riguarda, tra gli altri elementi, il processo nel quale il sistema sarà utilizzato, la durata e la frequenza dell'impiego, le categorie di persone coinvolte, i rischi di danno e le misure predisposte per limitarli. L'obiettivo è anticipare i possibili effetti negativi prima che il sistema venga inserito stabilmente nell'attività amministrativa, evitando che la valutazione dei rischi intervenga soltanto dopo il verificarsi di un problema.

La valutazione d'impatto sui diritti fondamentali assume una particolare rilevanza quando l'intelligenza artificiale viene utilizzata in settori nei quali l'amministrazione esercita poteri o fornisce prestazioni che possono incidere in modo significativo sulla vita delle persone. Accesso a servizi essenziali, istruzione, gestione del personale, sicurezza, giustizia e altri ambiti sensibili richiedono quindi una maggiore attenzione nella fase precedente all'introduzione del sistema. Questo adempimento non sostituisce le altre valutazioni previste dalla normativa europea, come quella relativa alla protezione dei dati personali quando ne ricorrono i presupposti, ma si inserisce in un quadro più ampio di prevenzione e gestione dei rischi.¹³³

¹³³ Regolamento (UE) 2024/1689, art. 27.

Accanto agli obblighi riferiti ai singoli sistemi, l'AI Act impone anche una responsabilità organizzativa più generale. L'articolo 4 richiede infatti a provider e *deployer* di adottare misure volte a promuovere un'adeguata alfabetizzazione in materia di intelligenza artificiale delle persone coinvolte nell'utilizzo dei sistemi. Il Regolamento (UE) 2026/1744 ha modificato nel 2026 alcuni aspetti di questa disciplina, mantenendo l'obbligo di adottare misure di *AI literacy* ma rendendo più flessibile la formulazione originaria. Resta comunque necessario che le competenze del personale siano adeguate alla funzione svolta, all'esperienza posseduta e al contesto nel quale il sistema viene utilizzato.

Questa esigenza è particolarmente evidente nella Pubblica Amministrazione italiana. Il *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026 – Aggiornamento 2026* dedica specifica attenzione all'intelligenza artificiale e individua nella capacità di analizzare i rischi, nella formazione continua e nello sviluppo di competenze interne elementi essenziali per una corretta adozione di tali tecnologie.¹³⁴ L'analisi del rischio viene descritta come un processo dinamico, che deve essere adattato alle caratteristiche concrete delle applicazioni utilizzate e accompagnato dalla costruzione di una cultura organizzativa fondata sulla consapevolezza e sulla responsabilità.

L'impatto dell'AI Act non riguarda pertanto soltanto il singolo funzionario che utilizza materialmente un sistema, ma coinvolge l'intera organizzazione dell'ente. Le amministrazioni devono essere in grado di mappare gli strumenti utilizzati, chiarirne le finalità, stabilire responsabilità interne, valutare i rischi, formare il personale e predisporre procedure di monitoraggio. La governance dell'intelligenza artificiale diventa così parte della più ampia trasformazione

¹³⁴ Agenzia per l'Italia Digitale, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*, cap. 5, «Dati e Intelligenza Artificiale», e Strumento 5, «Intelligenza Artificiale nella Pubblica Amministrazione»

digitale della PA e richiede un coordinamento tra competenze tecnologiche, amministrative e giuridiche.

Il quadro applicativo deve inoltre essere letto alla luce delle modifiche intervenute nel 2026. Il Regolamento (UE) 2026/1744, adottato l'8 luglio 2026 e attualmente in vigore, ha modificato l'AI Act anche con l'obiettivo di semplificarne l'attuazione e di concedere più tempo agli operatori per prepararsi agli obblighi relativi ai sistemi ad alto rischio. In base al calendario aggiornato, le disposizioni relative ai sistemi ad alto rischio dell'Allegato III si applicheranno, al più tardi, dal **2 dicembre 2027**, mentre per i sistemi collegati ai prodotti disciplinati dall'Allegato I il termine è fissato al **2 agosto 2028**.¹³⁵ Il rinvio non elimina gli obblighi previsti dal regolamento, ma offre alle amministrazioni un periodo ulteriore per predisporre procedure, competenze, sistemi di controllo e strumenti organizzativi adeguati.

Nel complesso, l'AI Act trasforma quindi l'introduzione dell'intelligenza artificiale nella Pubblica Amministrazione da scelta prevalentemente tecnologica a processo regolato di governance. L'amministrazione che utilizza un sistema di IA deve essere in grado di conoscere lo strumento, valutarne la finalità e il livello di rischio, individuare chi ne controlla l'utilizzo, monitorarne il funzionamento e documentare le principali fasi del processo. La conformità non può essere delegata integralmente al fornitore, poiché l'ente pubblico mantiene responsabilità proprie rispetto al modo in cui la tecnologia viene inserita nell'attività amministrativa. È proprio questo passaggio, dalla semplice disponibilità dello strumento alla responsabilità del suo utilizzo, a rappresentare uno degli effetti più rilevanti dell'AI Act sulla Pubblica Amministrazione.

¹³⁵ Regolamento (UE) 2026/1744; cfr. Commissione europea, documentazione aggiornata sull'attuazione dell'AI Act. Le nuove scadenze prevedono il 2 dicembre 2027 per i sistemi ad alto rischio dell'Allegato III e il 2 agosto 2028 per quelli incorporati nei prodotti dell'Allegato I.

4.2 Trasparenza e accountability

L'introduzione dell'intelligenza artificiale nell'attività amministrativa attribuisce alla trasparenza una funzione ancora più rilevante rispetto a quella già svolta nell'azione pubblica. Quando un procedimento è supportato da un sistema di IA, il cittadino deve poter comprendere non soltanto quale amministrazione abbia adottato una determinata decisione, ma anche se e in quale misura la tecnologia abbia contribuito alla sua formazione. La presenza di un sistema algoritmico non può rendere il procedimento poco conoscibile né impedire agli interessati di capire quale peso abbiano avuto le valutazioni automatizzate.

La trasparenza riguarda quindi due aspetti principali. Il primo consiste nella conoscenza dell'utilizzo stesso dell'intelligenza artificiale. Il cittadino deve sapere quando sta interagendo con un sistema automatizzato o quando un sistema di IA interviene in un'attività che lo riguarda. Il secondo riguarda invece la comprensione del ruolo svolto dalla tecnologia all'interno del procedimento. Non è necessario che ogni destinatario conosca nel dettaglio il funzionamento tecnico del modello, ma deve essere possibile capire quali funzioni siano state affidate al sistema, quali elementi abbiano inciso sul risultato e quale margine di valutazione sia rimasto all'amministrazione.

L'articolo 50 dell'AI Act disciplina specifici obblighi di trasparenza per determinati sistemi di IA. Dal 2 agosto 2026 tali obblighi sono diventati applicabili.¹³⁶ Le linee guida pubblicate dalla Commissione europea nel luglio 2026 hanno chiarito ulteriormente l'ambito di applicazione della norma e le modalità con cui provider, deployer e autorità competenti devono assicurare il rispetto degli obblighi previsti.

Per le amministrazioni pubbliche assume particolare importanza il caso dei sistemi destinati a interagire direttamente con persone fisiche. In queste

¹³⁶ Regolamento (UE) 2024/1689, art. 50; Commissione europea, *Guidelines on transparency obligations for providers and deployers of AI systems*, 20 luglio 2026

situazioni, l'interessato deve essere informato del fatto che sta interagendo con un sistema di IA, salvo che ciò risulti già evidente dalle circostanze e dal contesto. Questo può avvenire, ad esempio, quando un ente utilizza chatbot o assistenti virtuali per fornire informazioni, orientare l'utente tra i servizi o supportarlo nella presentazione di una richiesta. Il cittadino non dovrebbe quindi essere indotto a credere di comunicare con un operatore umano quando le risposte sono generate automaticamente.¹³⁷

La trasparenza assume un'importanza ancora maggiore quando il sistema contribuisce alla formazione di una decisione amministrativa. In questi casi deve essere possibile distinguere il ruolo svolto dall'algoritmo da quello attribuito al funzionario competente. Un sistema può limitarsi a ordinare informazioni, segnalare anomalie o proporre una raccomandazione, oppure può incidere in modo più significativo sulla valutazione finale. Comprendere questa differenza è essenziale per evitare che l'intervento dell'intelligenza artificiale renda poco chiaro chi abbia effettivamente contribuito alla decisione.

L'AI Act riconosce inoltre, all'articolo 86, un diritto specifico alla spiegazione in relazione a determinati processi decisionali individuali. La disposizione riguarda le persone interessate da una decisione adottata sulla base dell'output di un sistema di IA ad alto rischio dell'Allegato III, quando tale decisione produca effetti giuridici o incida in modo analogo e significativo sulla persona. In tali casi l'interessato ha diritto a ricevere spiegazioni chiare e significative sul ruolo svolto dal sistema nel processo decisionale e sui principali elementi che hanno inciso sull'esito.¹³⁸

Per la Pubblica Amministrazione questo diritto assume un valore particolare perché si collega direttamente alla necessità di rendere comprensibili le ragioni dell'azione amministrativa. Quando un sistema di IA contribuisce, ad esempio, a

¹³⁷ Regolamento (UE) 2024/1689, art. 50, par. 1.

¹³⁸ Regolamento (UE) 2024/1689, art. 86.

valutare l'accesso a una prestazione, a stabilire una priorità o a classificare una domanda, l'ente non può limitarsi a richiamare in modo generico il risultato algoritmico. Deve essere in grado di spiegare quale funzione abbia svolto il sistema e quali elementi abbiano inciso sulla decisione finale. L'utilizzo dell'IA non elimina quindi la necessità di una motivazione riconducibile all'amministrazione, ma richiede che essa tenga conto anche della componente automatizzata.

La spiegabilità deve essere distinta dalla semplice trasparenza tecnica. La conoscenza del codice sorgente, dei parametri del modello o delle caratteristiche informatiche del sistema può essere utile agli esperti e alle autorità di controllo, ma non garantisce da sola che il cittadino comprenda perché una determinata decisione lo abbia riguardato. La spiegazione deve essere adeguata al destinatario e al contesto. Ciò che conta è la possibilità di comprendere gli elementi essenziali della decisione e di verificare se esistano ragioni per contestarla. La trasparenza diventa quindi una condizione necessaria per l'effettivo esercizio dei diritti.¹³⁹

Alla trasparenza si collega il concetto di *accountability*, inteso come capacità dell'amministrazione di dimostrare e giustificare le scelte compiute nell'utilizzo dell'intelligenza artificiale. L'ente pubblico deve essere in grado di ricostruire chi abbia deciso di adottare il sistema, per quale finalità sia stato impiegato, quale ruolo gli sia stato attribuito nel procedimento e quali soggetti abbiano mantenuto la responsabilità delle valutazioni finali. L'*accountability* richiede quindi che l'uso dell'IA lasci una traccia organizzativa e documentale sufficiente a rendere verificabili le decisioni adottate.

Questa esigenza resta valida anche quando la tecnologia è fornita da un soggetto privato. L'esternalizzazione dello sviluppo o della gestione tecnica non può comportare anche l'esternalizzazione della responsabilità amministrativa. L'ente

¹³⁹ N. Rangone, «Intelligenza artificiale e pubbliche amministrazioni. Affrontare i numerosi rischi per trarne tutti i vantaggi», *BioLaw Journal – Rivista di BioDiritto*, n. 2, 2022, pp. 482-483.

deve conoscere le condizioni essenziali di funzionamento del sistema e deve poter ottenere dal fornitore le informazioni necessarie per utilizzarlo correttamente e rendere conto delle decisioni adottate. La dipendenza da soluzioni proprietarie o da competenze esterne non può quindi impedire all'amministrazione di verificare il funzionamento della tecnologia né di fornire spiegazioni comprensibili agli interessati.

La tracciabilità costituisce uno strumento essenziale per garantire l'accountability. Registrazioni, documentazione e informazioni relative all'utilizzo del sistema permettono di ricostruire le circostanze nelle quali un determinato output è stato prodotto e il modo in cui è stato utilizzato dall'amministrazione. Il loro valore non è soltanto tecnico. Una documentazione adeguata consente di svolgere controlli interni, rispondere alle richieste degli interessati e permettere alle autorità competenti di verificare il rispetto delle regole applicabili.

Trasparenza e accountability hanno anche una funzione preventiva. Sapere che le modalità di utilizzo del sistema devono poter essere ricostruite e giustificate spinge l'amministrazione a definire in anticipo responsabilità, procedure e criteri di utilizzo.¹⁴⁰ La conoscibilità dell'azione pubblica non interviene quindi soltanto dopo l'adozione di una decisione, ma incide anche sul modo in cui l'intelligenza artificiale viene inserita nell'organizzazione amministrativa.

Il rapporto tra trasparenza e responsabilità non significa che tutte le informazioni relative a un sistema debbano essere rese pubbliche senza limiti. Possono esistere esigenze legate alla riservatezza, alla tutela dei dati personali, alla sicurezza e alla protezione di informazioni commerciali. È quindi necessario trovare un equilibrio tra queste esigenze e il diritto del cittadino a comprendere come l'intelligenza artificiale sia stata utilizzata. La tutela del segreto tecnico o

¹⁴⁰ Agenzia per l'Italia Digitale, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*, cap. 5, «Dati e Intelligenza Artificiale»

commerciale non può diventare un ostacolo tale da rendere incomprensibile l'azione dell'amministrazione. Deve essere garantito un livello di conoscibilità sufficiente a comprendere il ruolo dell'IA, verificare la correttezza del procedimento ed esercitare gli strumenti di tutela previsti dall'ordinamento. L'applicazione degli obblighi di trasparenza dal 2 agosto 2026 rappresenta un passaggio importante per le amministrazioni pubbliche. Le linee guida della Commissione europea del luglio 2026 confermano che l'informazione deve essere fornita tenendo conto del contesto concreto e delle caratteristiche del sistema utilizzato, evitando che la trasparenza si riduca a un adempimento puramente formale.

Nel complesso, l'uso dell'intelligenza artificiale modifica il modo in cui la Pubblica Amministrazione deve rendere conto della propria attività, senza cambiare il principio secondo cui le decisioni pubbliche devono rimanere riconducibili a soggetti responsabili e comprensibili per i destinatari. La trasparenza consente di conoscere la presenza e il ruolo dell'IA. La spiegabilità permette di comprendere l'incidenza del sistema sulla singola decisione. L'accountability assicura che l'amministrazione possa giustificare e documentare le proprie scelte. Questi elementi aiutano a evitare che l'automazione crei zone poco comprensibili all'interno dell'azione amministrativa e contribuiscono a mantenere la fiducia dei cittadini nell'utilizzo pubblico dell'intelligenza artificiale.

4.3 Tutela dei diritti fondamentali dei cittadini

L'utilizzo dell'intelligenza artificiale da parte della Pubblica Amministrazione può incidere direttamente sulla posizione dei cittadini, soprattutto quando i sistemi vengono impiegati in settori collegati all'accesso a servizi, prestazioni, istruzione, lavoro, sicurezza o giustizia. Per questo motivo l'AI Act attribuisce

particolare importanza alla tutela dei diritti fondamentali e richiede che lo sviluppo e l'uso dei sistemi di IA avvengano nel rispetto dei valori riconosciuti dall'Unione europea. Il regolamento richiama espressamente un modello di intelligenza artificiale antropocentrica e affidabile, capace di garantire un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea.¹⁴¹

La tutela dei cittadini assume particolare rilievo nei casi in cui l'IA intervenga in decisioni che possono produrre conseguenze significative sulla vita delle persone. La disciplina dei sistemi ad alto rischio è costruita proprio tenendo conto della possibilità che alcune applicazioni incidano sulla salute, sulla sicurezza o sui diritti fondamentali. L'Allegato III comprende diversi ambiti nei quali questa incidenza può risultare particolarmente rilevante, tra cui istruzione, occupazione, accesso a servizi essenziali, attività di contrasto, migrazione e amministrazione della giustizia. La classificazione dipende quindi non solo dalle caratteristiche tecniche del sistema, ma anche dagli effetti che il suo utilizzo può produrre sulle persone.

Uno degli aspetti centrali riguarda il principio di uguaglianza e il divieto di discriminazione. La Carta dei diritti fondamentali stabilisce che tutte le persone sono uguali davanti alla legge e vieta qualsiasi forma di discriminazione fondata, tra gli altri elementi, sul sesso, sull'origine etnica o sociale, sulla religione, sulle opinioni politiche, sulla disabilità, sull'età o sull'orientamento sessuale.¹⁴² L'uso dell'intelligenza artificiale da parte di un'amministrazione deve quindi rispettare questi principi anche quando la valutazione è supportata da strumenti automatizzati.

¹⁴¹ Regolamento (UE) 2024/1689, art. 1.

¹⁴² Carta dei diritti fondamentali dell'Unione europea, artt. 20 e 21.

L'impiego dell'IA nei procedimenti pubblici non elimina le garanzie che devono essere rispettate nell'attività amministrativa.¹⁴³ L'autrice collega in particolare l'utilizzo di questi strumenti alla tutela dell'uguaglianza e alla necessità di evitare trattamenti discriminatori, ricordando che le garanzie proprie del procedimento continuano a trovare applicazione anche quando viene utilizzata una tecnologia automatizzata.

La tutela dell'uguaglianza assume un significato concreto quando un sistema contribuisce alla valutazione di persone che si trovano in condizioni differenti. Una classificazione o una previsione prodotta dall'IA può influenzare l'accesso a una prestazione, a un percorso formativo o a un'opportunità lavorativa. In questi casi l'amministrazione deve evitare che l'utilizzo della tecnologia produca differenze di trattamento incompatibili con i principi riconosciuti dall'ordinamento. Il fatto che un risultato sia prodotto attraverso un sistema automatizzato non gli attribuisce automaticamente carattere neutrale o imparziale.

Un altro diritto direttamente coinvolto riguarda la protezione dei dati personali. L'AI Act non sostituisce la disciplina già prevista dal Regolamento generale sulla protezione dei dati, ma si aggiunge ad essa. Chiarisce che le norme europee in materia di protezione dei dati continuano a trovare applicazione e che il nuovo regolamento opera in modo complementare rispetto al quadro già esistente.

Il GDPR stabilisce specifiche garanzie anche rispetto ai processi decisionali automatizzati. L'articolo 22 riconosce all'interessato il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, quando questa produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona.¹⁴⁴ La

¹⁴³ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», CERIDAP, n. 2, 2023, pp. 66-84.

¹⁴⁴ Regolamento (UE) 2016/679, art. 22.

disposizione prevede alcune eccezioni e richiede, nei casi indicati, misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato. Nel settore pubblico questo quadro impone di considerare con attenzione il rapporto tra utilizzo dell'IA e trattamento dei dati dei cittadini. Le informazioni utilizzate da un sistema possono riguardare aspetti rilevanti della vita della persona e contribuire alla formazione di valutazioni che producono conseguenze concrete. La protezione dei dati rimane quindi parte delle garanzie che accompagnano l'impiego dell'intelligenza artificiale nella Pubblica Amministrazione. La tutela dei cittadini riguarda anche il diritto a una buona amministrazione. L'articolo 41 della Carta dei diritti fondamentali riconosce il diritto di ogni persona a che le questioni che la riguardano siano trattate in modo imparziale, equo ed entro un termine ragionevole.¹⁴⁵ L'introduzione dell'IA nell'attività pubblica deve essere valutata mantenendo un equilibrio tra maggiore efficienza e rispetto delle garanzie. L'impiego delle tecnologie può contribuire al miglioramento dell'azione amministrativa, ma non può comportare una riduzione dei diritti procedurali già riconosciuti ai cittadini.

Questo principio è particolarmente importante quando il procedimento riguarda situazioni che richiedono una valutazione delle circostanze concrete. L'intelligenza artificiale può fornire supporto all'amministrazione, ma l'impiego dello strumento deve rimanere compatibile con l'imparzialità e con l'equità dell'azione amministrativa. L'innovazione tecnologica non modifica quindi il fatto che l'attività dell'amministrazione continui a essere sottoposta alle garanzie previste dall'ordinamento.

La protezione dei diritti non riguarda soltanto la fase nella quale il sistema viene utilizzato, ma comprende anche la possibilità di reagire quando si ritiene che le norme siano state violate. L'articolo 85 dell'AI Act riconosce a qualsiasi persona

¹⁴⁵ Carta dei diritti fondamentali dell'Unione europea, art. 41.

fisica o giuridica che abbia motivo di ritenere che sia avvenuta una violazione del regolamento il diritto di presentare un reclamo alla competente autorità di vigilanza del mercato.¹⁴⁶ Questo strumento opera senza pregiudicare gli altri ricorsi amministrativi o giurisdizionali previsti dall'ordinamento.

A questa garanzia si affianca il diritto a un ricorso effettivo riconosciuto dall'articolo 47 della Carta dei diritti fondamentali dell'Unione europea. La disposizione stabilisce che chi ritiene violati i diritti e le libertà garantiti dal diritto dell'Unione deve poter ricorrere davanti a un giudice.¹⁴⁷ L'utilizzo dell'intelligenza artificiale non sottrae quindi le decisioni pubbliche ai normali strumenti di tutela previsti dall'ordinamento.

L'utilizzo dell'IA deve essere valutato anche in relazione all'effettività della tutela giurisdizionale. La difficoltà di comprendere come si sia giunti a una determinata decisione può infatti incidere sulla capacità del cittadino di far valere i propri diritti. Per questo motivo le garanzie che accompagnano l'impiego dei sistemi di IA devono permettere alle persone interessate di mantenere una posizione effettivamente tutelabile nei confronti dell'amministrazione.

Il quadro delineato dall'AI Act non sostituisce quindi le tutele già previste dal diritto europeo, ma le integra con regole specifiche rivolte ai sistemi di intelligenza artificiale. Il regolamento stesso stabilisce che restano applicabili i diritti e i mezzi di ricorso già riconosciuti dal diritto dell'Unione e che le nuove disposizioni hanno anche la funzione di rafforzarne l'effettività.

Per la Pubblica Amministrazione questo significa che l'impiego dell'intelligenza artificiale deve essere valutato anche in base agli effetti che può produrre sulla posizione dei cittadini. Il rispetto dell'uguaglianza, della non discriminazione, della protezione dei dati, della buona amministrazione e del diritto a una tutela effettiva rimane necessario anche quando una parte dell'attività amministrativa

¹⁴⁶ Regolamento (UE) 2024/1689, art. 85.

¹⁴⁷ Carta dei diritti fondamentali dell'Unione europea, art. 47.

viene svolta con il supporto di sistemi automatizzati. L'AI Act inserisce quindi l'innovazione tecnologica all'interno di un quadro nel quale l'efficienza dell'amministrazione deve continuare a essere accompagnata dalla tutela delle persone e dei diritti riconosciuti dall'ordinamento europeo.

4.4 Opportunità e sfide per la PA

L'entrata in vigore dell'AI Act non elimina le possibilità offerte dall'intelligenza artificiale nel settore pubblico, ma inserisce il suo utilizzo all'interno di un quadro più definito. Per le amministrazioni la questione non riguarda soltanto la possibilità di adottare nuove tecnologie, ma anche la capacità di farlo in modo consapevole e coerente con le proprie finalità istituzionali. L'innovazione può produrre risultati positivi quando viene accompagnata da competenze adeguate, risorse organizzative e una capacità stabile di gestione della tecnologia.

Una prima opportunità riguarda l'integrazione dell'intelligenza artificiale nel più ampio processo di modernizzazione dell'amministrazione. Il valore della tecnologia non dipende dalla sua semplice disponibilità, ma dal modo in cui viene collegata alle esigenze dell'ente e dei cittadini. L'IA può contribuire al miglioramento dei processi interni, dei servizi e delle attività di supporto alle decisioni, purché venga inserita in un percorso di trasformazione graduale e sostenuto da risorse adeguate.¹⁴⁸

L'AI Act può favorire questo processo anche attraverso la presenza di un quadro normativo comune. Regole più definite permettono alle amministrazioni di valutare con maggiore consapevolezza le soluzioni da adottare, distinguendo gli impieghi consentiti da quelli vietati e individuando le condizioni applicabili ai sistemi più delicati. In questo modo la scelta della tecnologia può essere inserita

¹⁴⁸ E.M. Menéndez Sebastián, «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», CERIDAP, n. 2, 2023, pp. 66-84.

in una valutazione più ampia, che considera non soltanto le prestazioni dello strumento, ma anche la sua adeguatezza rispetto alle finalità dell'ente.

L'opportunità più rilevante non consiste quindi nell'automatizzare il maggior numero possibile di attività. L'aspetto centrale è riuscire a utilizzare l'IA nei casi in cui possa contribuire alla produzione di valore pubblico. La capacità di ottenere risultati utili dipende anche dalle risorse organizzative disponibili e dal modo in cui l'amministrazione riesce a combinare tecnologia, conoscenze interne e obiettivi istituzionali. L'adozione di un sistema, da sola, non garantisce un miglioramento dell'attività amministrativa.¹⁴⁹

L'effetto dell'IA nel settore pubblico dipende infatti dalle condizioni che accompagnano la sua introduzione. La tecnologia può sostenere la produttività e contribuire al miglioramento dei servizi, ma deve essere inserita in organizzazioni capaci di comprenderla e utilizzarla in modo adeguato. Per questo motivo l'innovazione non può essere considerata soltanto come un cambiamento tecnico, ma richiede anche un adattamento delle pratiche e delle modalità di lavoro.¹⁵⁰

Una delle principali sfide riguarda proprio le competenze interne. L'adozione dell'IA non può essere affidata esclusivamente agli uffici informatici, perché coinvolge anche attività amministrative, organizzative e gestionali. Diventa quindi necessario favorire una collaborazione tra professionalità differenti, in modo che le decisioni relative all'utilizzo della tecnologia non dipendano soltanto da valutazioni tecniche.

La disponibilità di personale qualificato rappresenta però una difficoltà concreta. Il settore pubblico può incontrare maggiori ostacoli nell'attrarre professionalità specialistiche e nel costruire competenze interne sufficienti. Il problema non

¹⁴⁹ C. van Noordt, L. Tangi, «The dynamics of AI capability and its influence on public value creation of AI within public administration», *Government Information Quarterly*, vol. 40, n. 4, 2023, art. 101860.

¹⁵⁰ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», *Discover Artificial Intelligence*, vol. 4, art. 18, 2024, pp. 1-18.

riguarda soltanto le figure tecniche. Anche il personale che utilizza o gestisce i sistemi deve possedere una conoscenza adeguata delle loro possibilità e dei loro limiti. La formazione diventa quindi parte integrante del processo di innovazione e deve accompagnare l'introduzione della tecnologia.¹⁵¹

Il Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, nell'Aggiornamento 2026, attribuisce particolare rilievo allo sviluppo delle competenze e alla capacità delle amministrazioni di governare i progetti di intelligenza artificiale. Le conoscenze tecnologiche devono essere affiancate da competenze amministrative, organizzative e giuridiche. La gestione dell'IA assume quindi un carattere trasversale e coinvolge più parti dell'organizzazione.¹⁵²

Un'altra sfida riguarda le risorse economiche e tecnologiche. L'introduzione stabile di sistemi di IA può richiedere investimenti in infrastrutture, personale specializzato, aggiornamento dei sistemi e formazione. Infrastrutture non adeguate e disponibilità finanziarie limitate possono rallentare l'adozione delle nuove tecnologie e creare differenze tra amministrazioni con capacità organizzative diverse.¹⁵³

Il rischio è che le opportunità offerte dall'intelligenza artificiale non siano distribuite in modo uniforme. Gli enti che dispongono di maggiori risorse economiche, infrastrutturali e professionali possono trovarsi in una posizione più favorevole rispetto alle amministrazioni di dimensioni ridotte. La diffusione dell'IA richiede quindi anche strumenti che permettano di condividere conoscenze, soluzioni e competenze, evitando che la capacità di innovare dipenda esclusivamente dalle risorse disponibili all'interno del singolo ente.

¹⁵¹ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 5-7.

¹⁵² Agenzia per l'Italia Digitale, Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026, cap. 5, «Dati e Intelligenza Artificiale».

¹⁵³ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 12-13.

Anche l'acquisizione delle tecnologie rappresenta un elemento importante. I processi di procurement pubblico possono essere caratterizzati da tempi e procedure che non sempre si adattano alla rapidità con cui evolvono le tecnologie di intelligenza artificiale. La scelta di un sistema non può quindi essere valutata soltanto al momento dell'acquisto. Occorre considerare anche la possibilità di aggiornarlo, adattarlo alle esigenze dell'amministrazione e mantenerlo nel tempo.¹⁵⁴

A questo aspetto si collega il rapporto con i fornitori privati. Le amministrazioni possono avere bisogno di competenze e soluzioni sviluppate all'esterno, soprattutto quando non dispongono internamente delle professionalità necessarie. La collaborazione con soggetti esterni può favorire l'accesso a tecnologie avanzate, ma richiede che l'ente mantenga una propria capacità di valutazione. L'amministrazione deve essere in grado di comprendere le caratteristiche essenziali dello strumento e verificarne l'adeguatezza rispetto alle proprie esigenze.¹⁵⁵

L'introduzione dell'AI Act rende questa capacità ancora più importante. Gli obblighi previsti dal regolamento richiedono che l'amministrazione conosca le caratteristiche dell'impiego concreto del sistema e sia in grado di governarne l'utilizzo. La presenza di un fornitore esterno non può sostituire completamente le competenze dell'ente. Una tecnologia avanzata può essere realmente utile soltanto quando l'amministrazione possiede conoscenze sufficienti per inserirla correttamente nei propri processi.

Il cambiamento organizzativo rappresenta quindi una delle condizioni principali per sfruttare le opportunità offerte dall'IA. Gli ostacoli all'adozione non sono esclusivamente tecnologici e possono dipendere anche da pratiche, strutture e

¹⁵⁴ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 5 e 8.

¹⁵⁵ N. Rangone, «Intelligenza artificiale e pubbliche amministrazioni. Affrontare i numerosi rischi per trarne tutti i vantaggi», *BioLaw Journal – Rivista di BioDiritto*, n. 2, 2022, pp. 473-488.

modalità di lavoro non adeguate. L'introduzione di nuovi sistemi può modificare la distribuzione dei compiti e il rapporto tra professionalità diverse. Se l'organizzazione non viene adattata, il rischio è quello di introdurre strumenti nuovi all'interno di processi che rimangono invariati.¹⁵⁶

L'intelligenza artificiale non deve quindi essere considerata una soluzione automatica ai problemi già presenti nell'amministrazione. Allo stesso tempo, le difficoltà connesse alla sua introduzione non devono portare a escluderne l'utilizzo quando può offrire un contributo concreto. L'obiettivo consiste nel trovare un equilibrio tra le possibilità offerte dall'innovazione e le condizioni necessarie per un suo utilizzo efficace nel settore pubblico.

L'AI Act può contribuire a rendere questo processo più strutturato. La necessità di conoscere i sistemi utilizzati, sviluppare competenze interne e definire modalità di gestione più consapevoli può favorire un approccio meno occasionale all'adozione dell'intelligenza artificiale. L'innovazione diventa così parte della programmazione dell'ente e richiede decisioni organizzative che precedono e accompagnano l'introduzione della tecnologia.

Le opportunità offerte dall'IA dipendono quindi dalla capacità delle amministrazioni di trasformare gli strumenti tecnologici in risorse effettivamente utili per l'azione pubblica. Questo risultato richiede competenze, infrastrutture, risorse economiche, capacità organizzativa e una gestione adeguata dei rapporti con i fornitori. Il nuovo quadro europeo rende queste condizioni ancora più importanti, perché l'utilizzo dell'intelligenza artificiale richiede una capacità stabile di gestione della tecnologia.

Opportunità e sfide risultano quindi strettamente collegate. Le stesse tecnologie che possono sostenere l'innovazione amministrativa richiedono investimenti e cambiamenti che non tutte le amministrazioni sono immediatamente in grado di

¹⁵⁶ K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 7-8.

affrontare. Il successo dell'adozione dell'IA dipende quindi non soltanto dall'evoluzione delle applicazioni disponibili, ma anche dalla capacità del settore pubblico di sviluppare competenze, risorse e strutture organizzative adeguate al loro utilizzo.¹⁵⁷

4.5 Prospettive future

L'evoluzione dell'intelligenza artificiale nella Pubblica Amministrazione nei prossimi anni sarà legata non soltanto alla diffusione di nuove tecnologie, ma soprattutto alla capacità degli enti pubblici di trasformare le sperimentazioni già avviate in applicazioni stabili e integrate nelle attività amministrative. L'impiego dell'IA nel settore pubblico si trova infatti ancora in una fase caratterizzata da livelli differenti di maturità e da numerosi progetti circoscritti a iniziative pilota. Il passaggio verso un utilizzo più ampio richiede quindi di comprendere quali applicazioni producano risultati effettivamente utili e possano essere mantenute nel tempo.¹⁵⁸

Uno degli aspetti più rilevanti riguarda proprio la capacità di valutare gli effetti dei progetti. La difficoltà di disporre di strumenti adeguati a misurare l'impatto delle applicazioni rappresenta uno degli ostacoli alla loro diffusione su scala più ampia. La sperimentazione non può quindi essere considerata un risultato sufficiente. Sarà sempre più importante verificare se l'introduzione dell'intelligenza artificiale produca benefici concreti rispetto alle finalità perseguite dall'amministrazione e se tali benefici giustifichino le risorse necessarie per sviluppare e mantenere i sistemi.¹⁵⁹

¹⁵⁷ C. van Noordt, L. Tangi, «The dynamics of AI capability and its influence on public value creation of AI within public administration», cit., art. 101860; K. Alhosani, S.M. Alhashmi, «Opportunities, challenges, and benefits of AI innovation in government services: a review», cit., pp. 15-16.

¹⁵⁸ OECD, *Governing with Artificial Intelligence. The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris, 2025.

¹⁵⁹ Ivi.

La prospettiva futura sarà quindi caratterizzata da un passaggio dalla semplice introduzione della tecnologia alla valutazione della sua effettiva utilità. L'innovazione non potrà essere misurata soltanto attraverso il numero di applicazioni adottate, ma dovrà essere collegata ai risultati ottenuti nell'attività amministrativa e nella qualità dei servizi. Questo orientamento assume particolare importanza nel settore pubblico, nel quale l'adozione di una tecnologia deve essere ricondotta agli obiettivi istituzionali dell'ente e al valore che essa può produrre per cittadini e amministrazioni.

La disponibilità e la qualità dei dati continueranno a rappresentare un altro elemento centrale. I sistemi di intelligenza artificiale richiedono informazioni adeguate alle finalità per le quali vengono utilizzati e l'accesso a dati di qualità costituisce ancora una difficoltà comune nelle amministrazioni pubbliche. A questo problema si aggiunge la necessità di favorire forme appropriate di condivisione delle informazioni e di migliorare le infrastrutture digitali già esistenti. Lo sviluppo futuro dell'IA nella PA resterà quindi strettamente collegato alla più generale evoluzione della gestione dei dati pubblici e dei sistemi informativi.¹⁶⁰

Anche le differenze esistenti tra amministrazioni potranno incidere sulla velocità e sulle modalità di diffusione dell'intelligenza artificiale. La capacità di adottare queste tecnologie non è infatti uniforme e può essere condizionata dalla disponibilità di risorse, dalla maturità digitale dell'ente e dalle competenze presenti al suo interno. La costruzione di indirizzi comuni e la condivisione delle esperienze possono contribuire a evitare che l'innovazione proceda in modo eccessivamente frammentato, soprattutto nei confronti degli enti che dispongono di capacità organizzative più limitate.¹⁶¹

¹⁶⁰ Ivi; Agenzia per l'Italia Digitale, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*.

¹⁶¹ Agenzia per l'Italia Digitale, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*.

Nel contesto italiano, AgID svolge un ruolo rilevante nel definire indicazioni e strumenti destinati ad accompagnare le amministrazioni nell'utilizzo dell'intelligenza artificiale. Il Piano triennale per l'informatica nella Pubblica Amministrazione e le iniziative dedicate all'IA collocano queste tecnologie all'interno del più ampio processo di trasformazione digitale del settore pubblico. Le attività rivolte all'adozione, allo sviluppo e al procurement dei sistemi contribuiscono alla progressiva costruzione di un quadro operativo comune, destinato a orientare le scelte delle amministrazioni nelle diverse fasi di introduzione della tecnologia.¹⁶²

Lo sviluppo dell'intelligenza artificiale richiederà inoltre un aggiornamento continuo delle competenze. Le carenze professionali rappresentano ancora uno degli ostacoli alla diffusione dell'IA nel settore pubblico e non possono essere affrontate attraverso interventi formativi limitati alla fase iniziale dell'adozione. La rapidità con cui evolvono le tecnologie rende necessario un processo di aggiornamento progressivo, capace di accompagnare i cambiamenti degli strumenti e delle modalità con cui essi vengono utilizzati nelle attività amministrative.¹⁶³

Questa evoluzione potrà incidere anche sul ruolo del personale pubblico. L'intelligenza artificiale può supportare o automatizzare alcune attività, ma la sua diffusione rende allo stesso tempo necessarie competenze capaci di valutare i risultati, controllare l'utilizzo dei sistemi e inserirli correttamente nei processi dell'amministrazione. Il rapporto tra tecnologia e lavoro pubblico appare quindi destinato a svilupparsi attraverso una trasformazione delle funzioni e delle professionalità, più che attraverso una semplice sostituzione dell'intervento umano.

¹⁶² Agenzia per l'Italia Digitale, *Intelligenza artificiale*; Id., *Linee guida su IA nella PA. Consultazione pubblica su sviluppo e procurement*, 2026.

¹⁶³ OECD, *Governing with Artificial Intelligence*, cit.

Un ulteriore elemento riguarda la difficoltà di prevedere in modo completo l'evoluzione futura dell'intelligenza artificiale. La rapidità dello sviluppo tecnologico rende poco realistico definire strategie rigide e immutabili. Le amministrazioni dovranno essere in grado di adattare progressivamente le proprie scelte, osservando l'evoluzione delle tecnologie, valutando i risultati delle applicazioni già introdotte e modificando le modalità di utilizzo quando necessario. L'OECD individua proprio nella capacità di adottare strategie agili e adattive uno degli elementi necessari per affrontare le future trasformazioni dell'IA nel settore pubblico.¹⁶⁴

La necessità di adattamento riguarda anche il quadro regolatorio. L'AI Act costituisce ormai il riferimento comune dell'Unione europea per lo sviluppo e l'utilizzo dell'intelligenza artificiale, ma la sua concreta attuazione continuerà a essere accompagnata da orientamenti, linee guida e ulteriori strumenti applicativi. Le amministrazioni dovranno quindi confrontarsi con un quadro normativo destinato a precisarsi progressivamente attraverso l'esperienza e gli interventi delle istituzioni competenti.

Le modifiche introdotte nel 2026 confermano il carattere progressivo di questo processo. Il Regolamento (UE) 2026/1744 ha modificato alcune disposizioni dell'AI Act anche con l'obiettivo di semplificarne l'attuazione e ha ridefinito parte del calendario applicativo relativo ai sistemi ad alto rischio.¹⁶⁵ Per le amministrazioni il periodo precedente alla piena applicazione delle disposizioni interessate rappresenta quindi una fase nella quale consolidare le modalità di utilizzo dell'intelligenza artificiale e prepararsi all'integrazione stabile delle nuove regole.

Le prospettive future dipenderanno, nel complesso, dalla capacità di far evolvere insieme innovazione tecnologica e capacità amministrativa. La diffusione dell'IA

¹⁶⁴ Ivi.

¹⁶⁵ Regolamento (UE) 2024/1689, come modificato dal Regolamento (UE) 2026/1744.

non può essere considerata come un processo esclusivamente tecnico, perché richiede dati adeguati, competenze aggiornate, strumenti di valutazione e modalità organizzative capaci di adattarsi nel tempo. Il passaggio dalla sperimentazione a un utilizzo più stabile sarà possibile soltanto quando le amministrazioni saranno in grado di selezionare le applicazioni realmente utili e di integrarle in modo coerente nelle proprie attività.

L'intelligenza artificiale potrà quindi assumere un ruolo sempre più significativo nella trasformazione digitale della Pubblica Amministrazione, ma la sua diffusione non dovrà essere valutata sulla base della sola presenza della tecnologia. La prospettiva dei prossimi anni sarà quella di costruire un utilizzo più maturo, nel quale l'innovazione venga accompagnata dalla capacità di valutarne i risultati, adattarsi ai cambiamenti e mantenere l'impiego dell'IA coerente con le finalità proprie dell'azione pubblica.

CONCLUSIONI

Il presente lavoro ha analizzato l'impatto dell'AI Act sull'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione, partendo dall'evoluzione della tecnologia e dal suo progressivo ingresso nel settore pubblico per arrivare alle conseguenze derivanti dall'introduzione del nuovo quadro normativo europeo.

L'analisi svolta ha mostrato come l'intelligenza artificiale non rappresenti soltanto una nuova tecnologia a disposizione delle amministrazioni, ma uno strumento capace di incidere sulle modalità di organizzazione dell'attività pubblica, sull'erogazione dei servizi e sul rapporto con i cittadini. La possibilità di automatizzare alcune operazioni, elaborare grandi quantità di informazioni e supportare determinate attività decisionali può contribuire a rendere più efficienti alcuni processi e a migliorare la capacità delle amministrazioni di rispondere alle esigenze degli utenti. Allo stesso tempo, l'impiego dell'IA introduce criticità che riguardano la qualità dei dati, la trasparenza, la spiegabilità dei risultati, la protezione delle informazioni personali, la discriminazione e l'individuazione delle responsabilità.

Proprio la presenza di queste opportunità e di questi rischi consente di comprendere la rilevanza dell'intervento normativo europeo. L'AI Act nasce infatti dalla necessità di evitare sia un utilizzo privo di regole sia un approccio che ostacoli indiscriminatamente l'innovazione. Il modello costruito dall'Unione europea si fonda sulla differenziazione degli obblighi in relazione al rischio e consente di sottoporre gli impieghi più delicati a garanzie maggiori, vietando le pratiche considerate incompatibili con i valori dell'Unione e lasciando maggiore libertà alle applicazioni che presentano conseguenze meno rilevanti.

Rispetto alla domanda posta alla base della ricerca, è quindi possibile affermare che **l'AI Act modifica in modo significativo le condizioni nelle quali la**

Pubblica Amministrazione può adottare e utilizzare sistemi di intelligenza artificiale. Il regolamento non impedisce alle amministrazioni di ricorrere a queste tecnologie, ma richiede che la loro introduzione sia accompagnata da una valutazione più consapevole della finalità del sistema, del livello di rischio e degli effetti che il suo utilizzo può produrre sulle persone.

Uno degli effetti principali riguarda il ruolo assunto dall'amministrazione quando utilizza sistemi sviluppati da soggetti esterni. La qualifica di deployer comporta obblighi propri e impedisce all'ente di considerare la conformità normativa come una responsabilità esclusiva del fornitore. L'amministrazione deve conoscere il sistema utilizzato, rispettarne le condizioni d'uso, assicurare una sorveglianza umana adeguata, monitorarne il funzionamento e conservare le informazioni necessarie a ricostruirne l'impiego. Nei casi previsti deve inoltre valutare preventivamente l'impatto sui diritti fondamentali. L'adozione dell'intelligenza artificiale diventa quindi un processo che coinvolge non soltanto la scelta della tecnologia, ma anche l'organizzazione interna dell'ente.

L'analisi ha evidenziato anche il ruolo centrale della trasparenza. L'introduzione di sistemi automatizzati non può rendere meno conoscibile l'attività amministrativa. Il cittadino deve poter sapere quando interagisce con un sistema di IA e, nei casi in cui la tecnologia contribuisca alla formazione di una decisione che lo riguarda, deve poter comprendere quale ruolo essa abbia svolto. La spiegabilità assume così una funzione strettamente collegata alla possibilità di contestare il risultato e di esercitare concretamente i propri diritti.

A questo profilo si collega l'accountability. L'amministrazione deve poter dimostrare come e perché abbia utilizzato un determinato sistema e deve mantenere la responsabilità delle decisioni adottate. La presenza dell'intelligenza artificiale non elimina infatti la necessità che l'azione pubblica rimanga riconducibile a soggetti responsabili. Anche quando lo sviluppo tecnico viene

affidato all'esterno, l'ente continua a essere responsabile delle modalità con cui la tecnologia viene inserita nei propri procedimenti e utilizzata nei confronti dei cittadini.

Un ulteriore risultato riguarda la tutela dei diritti fondamentali. L'AI Act non sostituisce le garanzie già previste dall'ordinamento europeo, ma si inserisce accanto ad esse. Uguaglianza, non discriminazione, protezione dei dati personali, buona amministrazione e diritto a una tutela effettiva continuano quindi a trovare applicazione anche quando l'attività amministrativa è supportata dall'intelligenza artificiale. L'innovazione non consente di ridurre le garanzie riconosciute ai cittadini e l'automazione non attribuisce automaticamente neutralità o correttezza alle decisioni prodotte.

Da questo punto di vista emerge uno degli aspetti più importanti del rapporto tra AI Act e Pubblica Amministrazione. L'efficienza non può essere considerata separatamente dalla tutela delle persone. L'impiego dell'intelligenza artificiale può migliorare alcune attività pubbliche, ma il beneficio prodotto deve essere valutato insieme agli effetti che la tecnologia può determinare sui destinatari dell'azione amministrativa. L'obiettivo non è quindi utilizzare l'IA nel maggior numero possibile di procedimenti, ma individuare gli ambiti nei quali il suo impiego risulti realmente utile e compatibile con le finalità dell'ente e con i principi dell'ordinamento.

L'AI Act produce inoltre conseguenze che vanno oltre il rispetto formale degli obblighi previsti dal regolamento. L'adozione dell'intelligenza artificiale richiede capacità organizzative, competenze e risorse adeguate. Le amministrazioni devono essere in grado di valutare le tecnologie acquistate, collaborare con i fornitori senza perdere il controllo delle proprie attività e formare il personale chiamato a utilizzare o supervisionare i sistemi. La presenza di regole comuni può quindi favorire una maggiore strutturazione dei processi di

adozione, ma la qualità dell'utilizzo continuerà a dipendere dalla capacità concreta dei singoli enti di governare l'innovazione.

Questa esigenza assume particolare rilievo considerando le differenze esistenti tra le amministrazioni. Enti con disponibilità economiche, infrastrutture e competenze differenti possono incontrare difficoltà diverse nell'introduzione dell'IA. Lo sviluppo di indicazioni comuni, strumenti condivisi e forme di collaborazione può contribuire a evitare che la trasformazione digitale produca un divario ulteriore tra amministrazioni dotate di maggiori capacità e realtà che dispongono di risorse più limitate.

Il quadro analizzato non può inoltre essere considerato definitivo. L'intelligenza artificiale continua a evolversi rapidamente e anche l'attuazione dell'AI Act seguirà un percorso progressivo. Le modifiche intervenute nel 2026 e la futura applicazione delle disposizioni relative ai sistemi ad alto rischio mostrano come il processo di adeguamento sia ancora in corso. Nei prossimi anni sarà quindi necessario valutare non soltanto il rispetto formale delle nuove regole, ma anche il modo in cui esse verranno concretamente applicate dalle amministrazioni e la loro capacità di incidere sulla qualità dell'utilizzo dell'IA.

La prospettiva futura appare legata soprattutto al passaggio da una fase caratterizzata da sperimentazioni e progetti circoscritti a un utilizzo più stabile e consapevole. Perché ciò avvenga, non sarà sufficiente aumentare il numero delle applicazioni. Sarà necessario verificare quali sistemi producano risultati effettivamente utili, quali possano essere integrati stabilmente nei processi amministrativi e quali richiedano invece maggiori cautele o non risultino adeguati alle finalità perseguite.

Alla luce dell'analisi svolta, l'AI Act può quindi essere considerato non come un ostacolo all'impiego dell'intelligenza artificiale nella Pubblica Amministrazione, ma come un elemento che modifica il modo in cui l'innovazione deve essere

progettata, valutata e governata. Il regolamento sposta l'attenzione dalla semplice disponibilità della tecnologia alla responsabilità del suo utilizzo e richiede che l'adozione dell'IA avvenga all'interno di un quadro nel quale efficienza, trasparenza, controllo e tutela dei diritti siano considerati congiuntamente.

La risposta alla domanda di ricerca non consiste quindi nell'affermare che l'AI Act riduca o favorisca in modo assoluto l'utilizzo dell'intelligenza artificiale nella Pubblica Amministrazione. Il suo impatto consiste soprattutto nel **rendere tale utilizzo maggiormente regolato, consapevole e responsabile**. Le amministrazioni continuano a poter sfruttare le opportunità offerte dalla tecnologia, ma sono chiamate a farlo dimostrando di saperne conoscere i limiti, governare i rischi e mantenere il controllo sulle conseguenze prodotte.

L'intelligenza artificiale può così diventare una componente sempre più rilevante della trasformazione digitale della Pubblica Amministrazione, purché rimanga uno strumento al servizio delle finalità pubbliche. La sfida non sarà sostituire l'amministrazione con la tecnologia, ma costruire un modello nel quale l'innovazione possa sostenere l'attività degli enti senza indebolire i principi e le garanzie che caratterizzano l'azione pubblica. In questo equilibrio tra possibilità tecnologiche e responsabilità istituzionale si colloca il principale impatto dell'AI Act sulla Pubblica Amministrazione.

BIBLIOGRAFIA

Agba, M.S., Agba, G.E.M., Obeten, A.W. (2023), «Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies», *Journal of Public Administration, Policy and Governance Research*, vol. 1, n. 2, pp. 1-14. Disponibile da: https://www.researchgate.net/publication/371853291_Artificial_Intelligence_and_Public_Management_and_Governance_in_Developed_and_Developing_Market_Economies

Alhosani, K., Alhashmi, S.M. (2024), «Opportunities, challenges, and benefits of AI innovation in government services: a review», *Discover Artificial Intelligence*, vol. 4, art. 18, pp. 1-18. Disponibile da: <https://doi.org/10.1007/s44163-024-00111-w>

Bontempi, V. (a cura di) (2022), *Lo stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, RomaTrepress. Disponibile da: <https://romatrepress.uniroma3.it/wp-content/uploads/2022/04/lost-vabo.pdf>

D'Alfonso, G. (2022), «Intelligenza artificiale e responsabilità civile. Prospettive europee», *Revista de Estudios Jurídicos y Criminológicos*, n. 6, pp. 163-195. Disponibile da: <https://revistas.uca.es/index.php/rejucrim/article/view/9735/10404>

Floridi, L. (2020), «Artificial Intelligence as a Public Service: Learning from Amsterdam and Helsinki», *Philosophy & Technology*, vol. 33, pp. 541-546.

Frontoni, E. (2023), «Intelligenza Artificiale Generativa e creatività umana», *FOR*, n. 3, pp. 15-17. Disponibile da: <https://journals.francoangeli.it/index.php/for/article/view/17072/2638>

Galetta, D.-U., Corvalán, J.G. (2019), «Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto», *Federalismi.it*, n. 3, pp. 1-23.

Gignac, G.E., Szodorai, E.T. (2024), «Defining intelligence: Bridging the gap between human and artificial perspectives», *Intelligence*, vol. 104, art. 101832, pp. 1-16. Disponibile da: <https://doi.org/10.1016/j.intell.2024.101832>

Groumpos, P.P. (2023), «A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities, and Threats», *Artificial Intelligence and Applications*, vol. 1, n. 4, pp. 181-197. Disponibile da: <https://ojs.bonviewpress.com/index.php/AIA/article/view/689/580>

Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S., Yang, G.-Z. (2019), «XAI—Explainable Artificial Intelligence», *Science Robotics*, vol. 4, n. 37, art. eaay7120. Disponibile da: https://openaccess.city.ac.uk/id/eprint/23405/8/aay7120_article_nearly%20final.pdf

Jiang, Y., Li, X., Luo, H., Yin, S., Kaynak, O. (2022), «Quo vadis artificial intelligence?», *Discover Artificial Intelligence*, vol. 2, art. 4, pp. 1-19. Disponibile da: <https://doi.org/10.1007/s44163-022-00022-8>

Kufel, J. et al. (2023), «What Is Machine Learning, Artificial Neural Networks and Deep Learning? —Examples of Practical Applications in Medicine», *Diagnostics*, vol. 13, n. 15, art. 2582. Disponibile da: <https://doi.org/10.3390/diagnostics13152582>

McCarthy, J., Minsky, M.L., Rochester, N., Shannon, C.E. (1955), «A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence». Disponibile da: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>

Menéndez Sebastián, E.M. (2023), «L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie», *CERIDAP*, n. 2, pp. 66-84. Disponibile da: https://ceridap.eu/pdf/estratti/Estratto-10.13130_2723-9195_2023-2-19.pdf

Pagano, F.F. (2021), «Pubblica amministrazione e innovazione tecnologica», *Gruppo di Pisa*, n. 3, pp. 84-112. Disponibile

da: https://gruppodipisa.it/images/convegni/2021_Convegno_Genova/Fabio_Francesco_Pagano_-_Pubblica_Ammministrazione_e_innovazione_tecnologica.pdf

Portinale, L. (2021), «L'Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori», *MediaLaws*, n. 3, pp. 13-28. <https://www.medialaws.eu/wp-content/uploads/2022/01/3-21-Portinale.pdf>

Rangone, N. (2022), «Intelligenza artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi», *BioLaw Journal – Rivista di BioDiritto*, n. 2, pp. 473-488. Disponibile da: <https://teseo.unitn.it/biolaw/it/article/view/2350/2295>

Tafari, D. (2023), «L'“etica” come specchietto per le allodole. Sistemi di intelligenza artificiale e violazioni dei diritti», *Bollettino telematico di filosofia politica*, pp. 1-13. Disponibile da: <https://commentbfp.sp.unipi.it/letica-come-specchietto-per-le-allodole/>

Turing, A.M. (1950), «Computing Machinery and Intelligence», *Mind*, vol. LIX, n. 236, pp. 433-460. Disponibile da: <https://doi.org/10.1093/mind/LIX.236.433>

FONTI NORMATIVE E ISTITUZIONALI

Agenzia per l'Italia Digitale (AgID), *Competenze di E-Leadership per gestire la transizione digitale della PA. Un quadro aggiornato di riferimento per le amministrazioni pubbliche*, luglio 2025. Disponibile da: https://www.agid.gov.it/sites/agid/files/2025-10/Rapporto_competenze_e-leadership.pdf

Agenzia per l'Italia Digitale (AgID), *Guida dei diritti di cittadinanza digitali*. Disponibile da: https://www.agid.gov.it/sites/agid/files/2024-07/Guida_dei_diritti_di_cittadinanza_digitale.pdf

Agenzia per l'Italia Digitale (AgID), *Intelligenza artificiale*, sezione istituzionale dedicata all'intelligenza artificiale.

Agenzia per l'Italia Digitale (AgID), *Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati*, versione 2.0, 19 giugno 2025. Disponibile da: https://www.agid.gov.it/sites/agid/files/2025-06/Linee_guida_Infrastruttura_Interoperabilit _PDND_v2_maggio_2025.pdf

Agenzia per l'Italia Digitale (AgID), *Linee Guida sull'interoperabilit  tecnica delle Pubbliche Amministrazioni*, versione 1.2, 29 novembre 2023. Disponibile da: https://www.agid.gov.it/sites/agid/files/2024-05/linee_guida_interoperabilit_tecnica_pa.pdf

Agenzia per l'Italia Digitale (AgID), *Linee guida su IA nella PA. Consultazione pubblica su sviluppo e procurement*, 2026.

Agenzia per l'Italia Digitale (AgID) (2026), *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026. Aggiornamento 2026*, in particolare cap. 5, «Dati e Intelligenza Artificiale», e Strumento 5, «Intelligenza Artificiale nella Pubblica Amministrazione». Disponibile da: <https://www.agid.gov.it/it/agenzia/piano-triennale>

Carta dei diritti fondamentali dell'Unione europea, in particolare artt. 20, 21, 41 e 47. Disponibile da: https://eur-lex.europa.eu/eli/treaty/char_2016/oj/ita

Commissione europea (2018), *L'intelligenza artificiale per l'Europa*, COM (2018) 237 final, Bruxelles, 25 aprile 2018. Disponibile da: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52018DC0237>

Commissione europea (2020), *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, Bruxelles, 19 febbraio 2020. Disponibile da: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0065>

Commissione europea (2021), *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione*, COM (2021) 206 final, Bruxelles, 21 aprile 2021. Disponibile da: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52021PC0206>

Commissione europea (2024), *Entrata in vigore della legge europea sull'intelligenza artificiale*, comunicazione istituzionale, 1° agosto 2024. Disponibile da: https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_it

Commissione europea (2026), *Draft Guidelines on the classification of high-risk AI systems*, 19 maggio 2026.

Commissione europea (2026), *Guidelines on transparency obligations for providers and deployers of AI systems*, 20 luglio 2026. Disponibile da: <https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems>

Commissione europea, documentazione istituzionale aggiornata sull'attuazione dell'AI Act.

Consiglio dell'Unione europea (2023), *Normativa sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole al mondo in materia di IA*, comunicato stampa, 9 dicembre 2023.

Consiglio dell'Unione europea (2024), *Regolamento sull'intelligenza artificiale: via libera definitivo del Consiglio*, comunicato stampa, 21 maggio 2024.

Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'Amministrazione Digitale (CAD)*.

Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale (2019), *Orientamenti etici per un'intelligenza artificiale affidabile*, Commissione europea, Bruxelles, 8 aprile 2019.

INPS (2024), Messaggio 5 aprile 2024, n. 1358, «SIISL – L'Intelligenza Artificiale a supporto dell'incrocio tra domanda e offerta di lavoro».

Ministero della Salute, Consiglio Superiore di Sanità (2021), *I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*, 9 novembre 2021.

OECD (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris.

Parlamento europeo (2024), *Il Parlamento europeo approva la legge sull'intelligenza artificiale*, comunicato stampa, 13 marzo 2024.

Parlamento europeo e Consiglio dell'Unione europea (2016), *Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento*

dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati – GDPR).

Parlamento europeo e Consiglio dell'Unione europea (2024), *Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale*, Gazzetta ufficiale dell'Unione europea, 12 luglio 2024. Disponibile da: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it>

Parlamento europeo e Consiglio dell'Unione europea (2026), *Regolamento (UE) 2026/1744 dell'8 luglio 2026 che modifica i regolamenti (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (Digital Omnibus on AI)*, Gazzetta ufficiale dell'Unione europea, 24 luglio 2026.

Presidenza del Consiglio dei ministri, *Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 1, Componente 1: Digitalizzazione, innovazione e sicurezza nella PA*. Disponibile da: <https://www.governo.it/it/approfondimento/digitalizzazione-innovazione-competitivita-e-cultura/16701>

SITOGRAFIA

DLA Piper (2026), *EU Commission draft guidelines on classification of “high-risk” AI systems: Key points*.

Kanade, V. (2022), *What Is Reinforcement Learning? Working, Algorithms, and Uses*, Spiceworks. Disponibile da: <https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-reinforcement-learning/>

Negri, C., «Cos'è il Natural Language Processing (NLP) e come funziona», Osservatorio Artificial Intelligence, Politecnico di Milano. Disponibile da: <https://www.osservatori.net/blog/artificial-intelligence/natural-language-processing-nlp-come-funziona-lelaborazione-del-linguaggio-naturale/>

Sorrentino, C., «Le applicazioni dell'Intelligenza Artificiale e la loro diffusione», Osservatorio Artificial Intelligence, Politecnico di Milano. Disponibile da: https://blog.osservatori.net/it_it/applicazioni-intelligenza-artificiale