Le Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione

di Fabrizio D'Alessandri, Consigliere di Stato

(Fonte: https://www.altalex.com/ 06/05/2026)

L'AgID, con la Determinazione n. 43/2026, ha adottato la bozza delle "Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione", previste dal Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, che sono state poste in consultazione pubblica dal 12 marzo all'11 aprile 2026. Le Linee Guida costituiscono uno strumento strategico per progettare nuovi sistemi basati sull'IA, occupandosi delle modalità di sviluppo dei sistemi di intelligenza artificiale, con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo, e riguardano tutte le componenti di applicazioni e infrastrutture tecnologiche che impiegano tecnologie di IA, sia come componente integrata sia come supporto alle funzionalità principali.

Le Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica Amministrazione

L'AgID, con la Determinazione n. 43/2026, ha adottato la "bozza" delle "**Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione**" e delle "Linee Guida per il procurement di IA nella Pubblica Amministrazione", previste dal Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, che sono state poste in consultazione pubblica dal 12 marzo all'11 aprile 2026.

In questa sede ci occupiamo delle "Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione", in quanto l'esame delle altre menzionate Linee Guida, è stato affrontato in un precedente contributo.

Le linee guida in questione sono previste dal Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, di cui al D.P.C.M. 12 gennaio 2024, e vengono emanate seguendo l'iter procedimentale previsto dall'art. 71 del Codice dell'Amministrazione Digitale (CAD) di cui al D.lgs. n. 82/2005. Quest'ultimo prevede che l'AgID, previa consultazione pubblica da svolgersi entro trenta giorni, sentite le amministrazioni competenti, il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, adotta linee guida contenenti regole tecniche e di indirizzo, che divengono efficaci dopo la loro pubblicazione nell'apposita area del sito Internet istituzionale dell'AgID.

In sede di consultazione pubblica, tutti i soggetti interessati, siano essi amministrazioni, operatori economici o professionisti, hanno potuto proporre **modifiche o integrazioni** nell'ottica di migliorare il testo delle linee guida in vista della loro adozione finale.

Le Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione costituiscono uno **strumento strategico per progettare nuovi sistemi basati sull'IA**, si occupano

delle modalità di sviluppo dei sistemi di IA, con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo e riguardano tutte le componenti di applicazioni e infrastrutture tecnologiche che impiegano tecnologie di IA, sia come componente integrata sia come supporto alle funzionalità principali.
In considerazione della rapidità che connota i processi di innovazione tecnologica dell'IA, è stata sentita l'esigenza di assicurare un costante adeguamento rispetto ai mutamenti derivanti dalla continua evoluzione digitale.
Le Linee guida sono state, quindi, corredate da **documenti a supporto dell'attività operativa** di applicazione delle stesse (c.d. "Strumenti"). L'elenco aggiornato degli Strumenti relativi alle Linee guida sull'IA sarà reso disponibile in un apposito link e gli Strumenti potranno essere oggetto di periodici aggiornamenti, al fine di tener conto della costante evoluzione del quadro normativo e tecnologico, nonché delle buone pratiche progressivamente emergenti.
D'altra parte, le soluzioni di IA presentano caratteristiche e problematiche nuove e specifiche, connotate da una marcata integrazione tra software, dati e modelli algoritmici, nonché da un'elevata complessità tecnica e da una rapida evoluzione tecnologica. Tali elementi impongono l'adozione di modalità operative differenti rispetto a quelle tradizionali, richiedendo un approccio consapevole, strutturato e adeguatamente governato da parte dell'Amministrazione.
L'IA non opera mediante "software statici" basati su istruzioni predefinite, ma tramite **sistemi adattivi, data-driven ed evolutivi**, il cui comportamento può modificarsi nel tempo in funzione dei dati utilizzati, delle configurazioni adottate, dei processi di addestramento e aggiornamento, nonché dell'evoluzione complessiva del contesto tecnologico.
La complessità che ne deriva incide direttamente sulle modalità con cui le amministrazioni sono chiamate a sviluppare tali sistemi, imponendo un ripensamento degli approcci tradizionali.
L'impiego dell'IA è, inoltre, suscettibile di incidere in modo diretto e significativo sull'azione della PA, influenzando i procedimenti amministrativi anche nella sua fase "decisionale", mediante lo svolgimento di attività istruttorie e valutative. Esso può, altresì, determinare rilevanti effetti sull'organizzazione del lavoro amministrativo e sul rapporto tra amministrazione e utenti, con un impatto rilevante sui diritti fondamentali e sulle aspettative di cittadini e imprese, nonché sulle modalità di esercizio della funzione pubblica.

Valenza giuridica delle linee guida e quadro normativo generale di riferimento
È importante definire la natura giuridica e gli effetti delle Linee guida, nonché la loro incidenza in termini di validità sull'attività dell'amministrazione in materia di intelligenza artificiale.
In linea di massima, le Linee guida **non hanno natura strictu sensu normativa**, non sono regolamenti, e non sono in linea di massima necessariamente vincolanti, trattandosi di atti amministrativi di carattere generale con funzione di indirizzo, volti a orientare l'azione dell'amministrazione, che, tuttavia, possono incidere sulla legittimità dell'azione amministrativa

ove l'Amministrazione se ne discosti senza adeguata motivazione, dando luogo al vizio di eccesso di potere. Non si tratta, però, di semplici raccomandazioni: le medesime linee guida possono assumere carattere vincolante quando **prevedono regole tecniche**. Si tratta, infatti, di quel "fenomeno" di fonti di disciplina atipiche, anche dette soft law, difficilmente inquadrabili nel quadro delle fonti normative, che ha avuto ampia fortuna, ad esempio, nel previgente codice dei contratti pubblici.

Sulla natura delle Linee Guida emesse da AgID, ai sensi dell'art. 71 CAD, il Consiglio di Stato si è già da tempo pronunciato in sede consultiva nel senso che tali linee guida possono assumere una **valenza erga omnes** e un carattere di vincolatività, ponendosi come "un atto di regolazione seppur di natura tecnica, con la conseguenza che le medesime dovrebbero ritenersi pienamente giustiziabili dinanzi al giudice amministrativo" (Consiglio di Stato, Commissione speciale, parere 10 ottobre 2017, n. 2120, che richiama il precedente parere 1° aprile 2016, n. 855, relativo alle linee guida dettate da ANAC). Tali conclusioni sono state ribadite dal Consiglio di Stato anche in sede giurisdizionale (Cons. Stato, Sez. IV, 8 marzo 2021, n. 1931; Cons. Stato, Sez. IV, 6 marzo 2020, n. 3025). Diversa conclusione si deve raggiungere laddove le linee guida abbiano un contenuto di indirizzo, che l'amministrazione può motivatamente non seguire qualora la situazione concreta lo renda opportuno.

Le Linee guida sull'IA si collocano all'interno di **un'articolata cornice normativa**, riportata nel testo, i cui più rilevanti atti nazionali e unionali sono:

Il Regolamento (UE) 2024/1689 del 13 giugno 2024 (**AI Act**) che stabilisce regole armonizzate sull'intelligenza artificiale e definisce i requisiti per un uso sicuro ed etico dell'IA. Il Regolamento classifica i sistemi di IA in base al livello di rischio, distinguendo tra rischio minimo, limitato e alto, e impone obblighi specifici e requisiti particolarmente stringenti per i sistemi ad alto rischio. Il medesimo regolamento prevede la supervisione umana (human in the loop) ai sensi dell'art. 14, un sistema di gestione dei rischi previsto dall'art. 9 e la trasparenza ai sensi dell'art. 13. Le applicazioni utilizzabili dalle amministrazioni pubbliche, come ad esempio i processi decisionali automatizzati o la gestione di servizi pubblici, possono rientrare tra i sistemi ad alto rischio e le linee guida AgID si muovono quindi in una prospettiva di allineamento con il quadro europeo.

Il Regolamento (UE) 2016/679 del 27 aprile 2016(**Regolamento Generale sulla Protezione dei Dati**), comunemente detto GDPR, che stabilisce norme per la protezione dei dati personali e la privacy delle persone fisiche, nonché il Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)

Il D.lgs. 31 marzo 2023, n. 36 (**Codice dei contratti pubblici**) che disciplina l'intero ciclo di vita dei contratti pubblici, con una normativa tendenzialmente esaustiva, e i cui artt. 19 e 30 dettano principi generali applicabili all'utilizzo degli strumenti digitali, compresi i sistemi di intelligenza artificiale, nel ciclo di vita dei contratti pubblici, imponendo requisiti di tracciabilità, trasparenza

algoritmica e accessibilità ai codici sorgente dei sistemi di IA utilizzati nelle procedure di affidamento.
La **legge 23 settembre 2025, n. 132** di **recepimento e integrazione dell'AI Act**, che “promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale” e riconosce AgID e l’Agenzia per la cybersicurezza nazionale quali autorità nazionali competenti per la promozione, vigilanza e sicurezza. In particolare, l’art. 3 detta i principi generali e l’art. 4 i principi in materia di informazione e di riservatezza dei dati personali. L’art. 14, che riguarda l’uso dell'intelligenza artificiale nella pubblica amministrazione, prevede che "1. Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo. 2. L'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale. 3. Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo responsabile dell'intelligenza artificiale e a sviluppare le capacità trasversali degli utilizzatori".

I principi per l’adozione dell’IA nelle Pubbliche Amministrazioni
Una parte molto importante delle linee guida è dedicata all’enunciazione di **una serie di principi generali** che costituiscono il quadro di base per orientare lo sviluppo di sistemi di IA nell’ambito della Pubblica amministrazione.
I principi sono volti ad assicurare il controllo, la sostenibilità, l’interoperabilità e l’autonomia operativa nel corso dell’intero ciclo di vita dei sistemi di IA.
L’IA non deve tradursi in soluzioni “monolitiche” o tecnicamente rigide, ma deve tendere alla **realizzazione di capacità e servizi governabili**.
I sistemi di IA sono qualificati come sistemi complessi e multilivello, da progettare considerando l’intero stack tecnologico, dalle infrastrutture energetiche fino ai servizi applicativi. In tale prospettiva, è richiesto il disaccoppiamento tra i componenti, così da consentire la sostituzione o l’aggiornamento di modelli, infrastrutture e servizi senza impatti sull’intero sistema.
Le Pubbliche Amministrazioni devono inoltre privilegiare architetture agentiche e basate su servizi, coordinate da un orchestratore di servizi di IA capace di gestire in modo flessibile e controllabile modelli, dati e risorse computazionali.
Risulta centrale anche il principio di neutralità hardware, che impone di evitare dipendenze strutturali da specifici acceleratori computazionali o architetture proprietarie.

Devono essere previste delle attività di rollback e fallback per fronteggiare fattori imprevedibili, quali rischi di mercato, carenze di approvvigionamento, ritardi, rincari dei costi e simili evenienze. Lo sviluppo dei sistemi deve, inoltre, garantire la continuità dei servizi, l'efficienza, la sostenibilità e la capacità della Pubblica Amministrazione di gestire, adattare ed evolvere i sistemi nel tempo in regime di autonomia operativa.
Le linee guida indicano due tipologie di principi, in un'ottica unitaria e integrata di sviluppo eprocurement dei sistemi di IA:

a) in **primo luogo**, **declinano le modalità operative per l'attuazione dei venti principi già dettati dalle Linee Guida dell'AgID per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione**, adottate con la determinazione n. 17/2025 del 17 febbraio 2025, mettendo in relazione ciascun principio con le specifiche azioni da adottare nelle diverse fasi di sviluppo e di procurement dei sistemi di IA (paragrafo 2.2). Ciò consente di tradurre i principi generali in requisiti tecnici e contrattuali concreti riferiti al ciclo di vita del sistema;

b. in **secondo luogo**, prendono in esame anche i **principi generali** dettati dall'art. 3 della legge delega in materia di intelligenza artificiale, n.132/2025, calati nell'ambito dell'**intero ciclo di vita dei sistemi di Intelligenza Artificiale**, sia nelle fasi di progettazione e sviluppo dei sistemi di IA, sia in quella di procurement, al fine di garantire un utilizzo responsabile, sicuro e conforme al quadro normativo vigente (paragrafo 2.3).

I principi dalle Linee Guida dell'AgID per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, di cui al punto A
I **venti principi** previsti dalle Linee Guida dell'AgID per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione del 2025 vengono declinati in termini concreti quali requisiti operativi per lo sviluppo e l'acquisto dei sistemi di IA.
In tale ambito assumono preminenza i principi di conformità normativa, secondo logiche di compliance by design; di gestione del rischio, che contempla i rischi di lock-in tecnologico e di perdita di controllo; di protezione dei dati personali; di responsabilità finale della Pubblica Amministrazione; di sorveglianza umana; di trasparenza e documentazione; di sicurezza cibernetica, interoperabilità e continuità del servizio.
Più specificamente, vengono illustrati i principi che seguono.

1**. Conformità normativa**, secondo cui le Pubbliche Amministrazioni devono adottare sistemi di IA nel pieno rispetto della normativa nazionale ed europea, assicurandone il costante aggiornamento rispetto all'evoluzione legislativa. Ne deriva, in fase di sviluppo, una progettazione secondo il criterio del compliance by design. In fase di procurement, i contratti devono prevedere clausole di

adeguamento nel caso di modifiche normative, nonchè soluzioni tecniche che non ostacolino tali adeguamenti.

2. **Rispetto dei valori fondamentali dell'Unione europea**. L'uso dell'IA deve essere coerente con la Carta dei diritti fondamentali dell'UE e con i principi richiamati dall'AI Act. Lo sviluppo deve, infatti, integrare valutazioni d'impatto sui diritti fondamentali e meccanismi di controllo umano, mentre, in fase di procurement, si devono compiere valutazioni preventive d'impatto sui diritti fondamentali ed evitare vincoli tecnologici che limitino la sostituibilità dei componenti in caso di criticità.

3. **Gestione del rischio**, secondo il quale le amministrazioni devono adottare adeguate politiche di risk management. In sede di sviluppo va curata l'analisi del rischio per i profili tecnici, organizzativi e sistemici. Il procurement deve considerare il rischio di lock-in, di discontinuità operativa e di perdita del controllo tecnologico e i contratti devono supportare portabilità, reversibilità e fallback operativo.

4. **Protezione dei dati personali**, ai sensi del quale le Amministrazioni nell'adottare i sistemi di IA garantiscono il rispetto delle norme in materia di protezione dei dati personali, assicurando la qualità e l'integrità dei dati. Lo sviluppo deve favorire il controllo, la portabilità dei dati e la minimizzazione dei trattamenti, mentre in fase di procurement i contratti devono limitare l'uso secondario dei dati, garantendo la titolarità pubblica dei dataset. Devono, altresì, essere contemplati obblighi di restituzione e cancellazione dei dati.

5. **Responsabilità**. Secondo tale principio, le Amministrazioni identificano chiaramente le responsabilità di tutti gli attori coinvolti e rimangono responsabili finali delle decisioni assunte tramite i sistemi di IA. Conseguentemente, la progettazione deve consentire l'attribuzione delle responsabilità umane, così come la possibilità di intervento e supervisione. In sede di procurement, i contratti devono definire chiaramente ruoli, responsabilità, catene decisionali e presidi di controllo.

6. **Accessibilità, inclusività e non discriminazione**, ai sensi del quale le amministrazioni devono assicurare un trattamento equo per tutti i soggetti e gruppi coinvolti nell'adozione dell'IA, prevenendo, sia in fase di progettazione che in quella di procurement, bias ed effetti discriminatori. Inoltre, in fase di procurement si devono evitare soluzioni che ostacolino l'intervento correttivo nell'ipotesi in cui si verifichino discriminazioni.

7. **Trasparenza, spiegabilità e documentazione**, volto ad assicurare trasparenza, comprensibilità e adeguata documentazione dei sistemi di IA. Il funzionamento del sistema di IA deve essere comprensibile in misura adeguata al rischio e al contesto. In sede di procurement si deve assicurare l'accesso continuativo alla documentazione tecnica e funzionale, anche post-contratto, mediante apposite clausole.

8. **Trasparenza e informazione**. Questo principio postula l'informazione agli utenti sull'interazione con sistemi di IA, al fine di renderli edotti delle capacità e dei limiti di questi sistemi (ex art. 50 dell'IA Act). Conseguentemente, i contratti devono contemplare degli obblighi di supporto alla comunicazione istituzionale verso cittadini e imprese.

9. **Qualità dei dati**. Ai sensi dell'art.10 dell'AI Act IA, deve essere garantita una gestione etica, trasparente e conforme dei dati gestiti dai sistemi di IA, assicurando la qualità, l'integrità, la sicurezza e la sostenibilità. I sistemi di IA devono prevedere meccanismi di validazione, controllo e tracciabilità dei dati; i capitolati di gara devono definire requisiti minimi di qualità dei dati, incluse completezza, rappresentatività e aggiornamento.

10. **Accuratezza**. Questo principio impone alle pubbliche amministrazioni di garantire che i sistemi di IA producano risultati affidabili e coerenti con gli obiettivi istituzionali, in conformità con l'art. 15 dell'AI Act. A tal fine, lo sviluppo deve fondarsi su metriche di accuratezza misurabili, documentate e monitorabili nel tempo, calibrate sul contesto applicativo e sul livello di rischio. In sede di procurement, tali esigenze si traducono nell'inclusione nei contratti di SLA e KPI specifici sull'accuratezza, accompagnati da meccanismi di intervento correttivo e da clausole che evitino vincoli contrattuali ostativi all'adeguamento del sistema nel tempo.

11. **Robustezza**. Secondo tale principio, i sistemi di IA devono essere progettati per operare in modo affidabile anche in condizioni avverse o in presenza di guasti, in conformità all'art. 15 dell'AI Act. Ciò implica l'adozione di architetture modulari, resilienti e degradabili, capaci di mantenere livelli di servizio proporzionati anche in condizioni non ottimali. In fase di sviluppo devono essere previsti meccanismi di fallback e, in in fase di procurement, si devono preferire soluzioni componibili e sostituibili che riducano il rischio di lock-in tecnologico, accompagnate da clausole contrattuali che consentano verifiche e, se necessario, la risoluzione del rapporto in caso di inadempimento per difformità rispetto agli standard pattuiti.

12. **Sicurezza cibernetica**. Questo principio impone alle amministrazioni di garantire la sicurezza cibernetica dei sistemi di IA, proteggendoli da compromissioni, alterazioni o usi impropri, a tutela dell'integrità, della disponibilità e della riservatezza dei dati e dei processi, in conformità all'art.

15 dell'AI Act. In sede di sviluppo devono essere tenute presenti tali esigenze dettando criteri di sicurezza end to end, includendo controllo degli accessi modelli, agenti, infrastrutture e pipeline di dati. A livello contrattuale, è necessario prevedere obblighi in materia di sicurezza, gestione degli incidenti e cooperazione con la PA, evitando soluzioni che ostacolino l'adozione autonoma di misure di sicurezza o la migrazione verso ambienti alternativi.

13**. Sorveglianza umana.** In conformità con l'art. 14 dell'AI Act, i sistemi di IA devono consentire una supervisione umana effettiva e di livello adeguato, tale da garantire la verifica, la correzione o la sostituzione delle decisioni automatizzate. In fase di sviluppo, ciò si traduce nella predisposizione di strumenti che consentano interventi tempestivi, mentre in sede di procurement si deve evitare che l'intervento umano risulti solo formale e si deve garantire l'accesso diretto agli strumenti di supervisione, senza dipendere dal fornitore.

14. **Registrazioni (logging).** Questo principio, contemplato dall'art. 12 dell'AI Act, richiede l'adozione di sistemi di registrazione in grado di garantire la tracciabilità delle operazioni svolte dai sistemi di IA. I meccanismi di logging devono essere interoperabili e verificabili mediante audit, e devono consentire la ricostruzione delle decisioni, dei flussi di dati, degli interventi umani e delle interazioni tra gli agenti. In fase di procurement, i contrati devono assicurare l'accesso completo ai dati di log.

15. **Adozione di standard tecnici**. Le pubbliche amministrazioni devono conformarsi alle norme tecniche nazionali, europee e internazionali, al fine di garantire interoperabilità, sicurezza, manutenibilità e conformità normativa dei sistemi di IA. Lo sviluppo deve fondarsi sull'impiego di standard aperti e riconosciuti, idonei a favorire l'interoperabilità, la portabilità e la manutenibilità. Allo stesso modo, il procurement deve privilegiare soluzioni basate su standard aperti e formati interoperabili, nonché evitare l'adozione di soluzioni che ostacolino l'adozione di standard futuri o l'integrazione con ulteriori sistemi.

16. **Efficienza e qualità dei servizi.** Il principio è volto a orientare l'utilizzo dell'IA verso l'incremento dell'efficienza operativa e della qualità dei servizi resi a cittadini e imprese, nonché a favorire l'automazione, la proattività e la semplificazione. I sistemi di IA devono essere progettati in funzione del miglioramento misurabile, con riferimento a tempi, qualità ed efficacia, dei servizi prestati. Conseguentemente in sede di procurement le amministrazioni sono chiamate a considerare le soluzioni proposte in base all'impatto reale sui servizi, evitando di fermarsi al costo o a valutazioni delle prestazioni "solamente" teoriche.

17. **Innovazione e miglioramento continuo.** Le amministrazioni devono adottare un approccio dinamico, aperto all'innovazione e al miglioramento continuo, e collaborativo nei confronti dell'adozione dell'IA, fondato su ecosistemi aperti, sul riuso e sull'integrazione tra soggetti pubblici e privati. In tale contesto assume rilievo anche il ricorso a componenti open source e open weights. Lo sviluppo deve favorire modularità, riusabilità e integrazione in contesti multi-fornitore e il procurement deve incentivare soluzioni aperte e riutilizzabili, valorizzandone l'impatto in termini di trasparenza, autonomia operativa e sostenibilità economica. Sono da favorire forme di cooperazione tra amministrazioni, anche attraverso modelli consortili o reti stabili.

18. **Sostenibilità ambientale.** Le amministrazioni devono adottare sistemi di IA secondo criteri di sostenibilità, considerando l'efficienza energetica e la riduzione dell'impatto ambientale. La progettazione dei sistemi deve tener conto del consumo energetico e delle risorse computazionali, privilegiando modelli proporzionati alle effettive esigenze. In sede di procurement, le gare debbono considerare criteri di sostenibilità ambientale riferiti all'intero stack tecnologico e devono essere valorizzate soluzioni capaci di dimostrare, in modo misurabile, la riduzione dell'impatto ambientale nel tempo.

19. **Formazione e sviluppo delle competenze.** E' necessario accompagnare l'adozione dell'IA con un adeguato investimento sul capitale umano, rivolto sia alle competenze interne all'amministrazione, che a cittadini e imprese, nell'ottica di garantire un utilizzo consapevole, inclusivo e responsabile delle tecnologie di IA. Lo sviluppo dei sistemi deve essere accompagnato da un trasferimento di competenze verso il personale pubblico e i sistemi devono inoltre essere progettati in modo da risultare pienamente governabili dal personale interno. In sede contrattuale devono essere previsti obblighi di formazione e affiancamento operativo, evitando soluzioni che creino dipendenze da competenze non trasferibili.

20. **Rafforzamento dell'organizzazione e delle infrastrutture.** Viene imposto alle amministrazioni di ottimizzare gli assetti organizzativi e le infrastrutture tecnologiche per sostenere la trasformazione digitale, anche mediante forme di aggregazione e condivisione tra enti. In fase di sviluppo, i sistemi devono essere progettati secondo architetture a servizi, con separazione dei componenti e orchestrazione sotto il controllo della PA, consentendo modelli di gestione sia centralizzati sia federati. In sede di procurement, devono essere privilegiate soluzioni che rafforzino la resilienza e l'autonomia operativa e dell'amministrazione, favorendo il riuso, la condivisione e l'interoperabilità tra più amministrazioni, anche attraverso strumenti di aggregazione, quali accordi quadro o modelli consortili.

I principi generali dettati dall'art. 3 della legge delega in materia di intelligenza artificiale, n.132/2025, di cui al punto B

Le linee guida, come indicato, declinano in termini operativi i principi generali dettati dall'**art. 3** della **Legge n. 132/2025** nelle fasi di progettazione e sviluppo, nonché in sede di procurement dei sistemi di IA, nell'ottica di un utilizzo responsabile, sicuro e conforme alla normativa vigente. In linea di massima un primo leitmotiv nell'adozione dell'IA riguarda la tutela dei diritti fondamentali, la non discriminazione, la trasparenza e la proporzionalità, nel senso che nella progettazione di tali sistemi si devono valutare gli impatti sui diritti e, nei casi rilevanti, mediante strumenti quali DPIA e FRIA. Un secondo criterio guida concerne la necessità di assicurare la qualità e l'affidabilità dei dati e dei processi, mediante una data governance, controlli strutturati e la tracciabilità delle attività di addestramento, validazione e testing. Ulteriore criterio centrale riguarda la centralità dell'azione umana, con la necessità di una supervisione significativa e la possibilità di intervento, nonchè adeguati meccanismi che garantiscano la spiegabilità e misure di prevenzione del danno. Viene, inoltre, assicurata la tutela del metodo democratico e della sovranità istituzionale, imponendo cautele contro manipolazioni informative, interferenze nei processi pubblici e usi distorti delle tecnologie intelligenti. Si impongono, inoltre, le esigenze di coerenza con il diritto unionale, ed in primis con l'AI Act, di implementazione della cybersicurezza e della resilienza by design e by default lungo l'intero ciclo di vita del sistema, nonché dell'accessibilità universale e dell'inclusione delle persone con disabilità. In sostanza, i principi dettati dalla **legge n. 132/2025** "disegnano" l'IA come uno strumento funzionale al perseguimento di interessi pubblici, in piena conformità ai valori costituzionali e al diritto unionale, a salvaguardia delle garanzie giuridiche dei singoli.

Più specificamente, vengono illustrati i **sette gruppi di principi** che seguono.

1. **Tutela dei diritti fondamentali, trasparenza, proporzionalità e non discriminazione.** Questo principio impone che l'impiego dell'IA avvenga nel pieno rispetto dei diritti e delle libertà fondamentali, evitando trattamenti discriminatori, e garantendo un livello di trasparenza e proporzionalità adeguato al contesto d'uso. In questa prospettiva, la progettazione deve prevedere sin dall'origine una valutazione degli impatti sui diritti fondamentali, anche mediante strumenti preventivi quali DPIA e FRIA nei casi di sistemi ad alto rischio. Il criterio di proporzionalità funge da parametro di idoneità tra gli obiettivi perseguiti e le misure tecnologiche adottate.

2. **Qualità, correttezza, attendibilità e trasparenza dei dati e dei processi.** I dati e i processi utilizzati nei sistemi di IA devono essere adeguati, verificabili e trasparenti, secondo il principio di proporzionalità rispetto al settore di utilizzo. L'affidabilità dei sistemi di IA dipende dalla qualità dei dati e dalla verificabilità dei processi decisionali automatizzati. Ne deriva l'obbligo di adottare

processi strutturati di data governance e controlli di qualità dei dataset, nonché di utilizzare meccanismi di tracciabilità delle fasi di addestramento, validazione e testing.

3. **Centralità dell'uomo, spiegabilità e prevenzione del danno.** Il principio riafferma la necessaria centralità del decisore umano nei processi decisionali di IA. I sistemi di IA devono quindi consentire forme di supervisione e intervento umano significativo. Devono, inoltre, essere adottate funzionalità di spiegabilità adeguate al livello di rischio, nonché misure preventive per evitare danni fisici, materiali o immateriali.

4. **Tutela del metodo democratico, istituzionale e della sovranità.** Questo principio riguarda una prospettiva ordinamentale dell'utilizzo dell'IA, salvaguardando il metodo democratico, l'autonomia delle istituzioni e la sovranità dello Stato da interferenze illecite nei processi pubblici. In tal senso, viene imposto l'obbligo di prevenire usi impropri che possano alterare processi decisionali pubblici o politici, di implementare misure di sicurezza contro abusi e manipolazioni informative e di garantire l'integrità, la tracciabilità e la provenienza di modelli e dati.

5. **Coerenza con il quadro normativo europeo (AI Act).** La ratio di questo principio poggia sulla necessità di porre in coordinamento, e non contrapposizione, le previsioni della **Legge n. 132/2025** con l'AI Act europeo, evitando di introdurre un regime parallelo, che imponga ulteriori obblighi non previsti a livello unionale. Infatti, i sistemi di IA devono essere sviluppati in conformità ai requisiti applicabili dell'AI Act.

6. **Cybersicurezza e resilienza lungo il ciclo di vita.** Secondo questo principio, la cybersicurezza costituisce un presupposto essenziale per lo sviluppo e l'utilizzo legittimo dell'IA nella PA. Le misure di sicurezza devono essere integrate sin dalla progettazione ("security by design") e impostate come configurazione predefinita ("by default"), secondo un approccio basato sul rischio. I sistemi devono essere resilienti rispetto ad attacchi informatici e manipolazioni. In tal senso devono essere effettuati test di sicurezza nel corso dell'intero ciclo di vita del sistema di IA.
7. **Accessibilità universale e inclusione.** Quest'ultimo principio si pone sulla dimensione "sociale" dell'utilizzo dell'IA, imponendo che i sistemi di IA siano fruibili in modo universale e non generino discriminazioni. Le interfacce devono essere progettate secondo requisiti di accessibilità e devono essere sottoposte a test di usabilità inclusiva, con particolare riguardo alle persone con disabilità.

Classificazione delle famiglie di sistemi di IA
Una parte rilevante delle linee guida è riservata alla **classificazione delle famiglie di sistemi di IA** maggiormente diffuse.

Si distinguono diverse famiglie di sistemi di IA, procedendo dal generale al particolare, distinte per livello tecnologico, che partono dalla categoria generale del sistema di IA, definito dall'AI ACT come "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali". In sostanza, un sistema di IA è rappresentabile quale insieme delle tecnologie capaci di svolgere compiti che simulano capacità cognitive tipicamente umane, quali l'apprendimento, il ragionamento e l'adattamento, e tali sistemi spaziano da quelli **statistici e data-driven**, più prevedibili e con minore autonomia decisionale, fino ai sistemi più complessi come **machine learning, reti neurali, deep learning e IA generativa**. In linea di generale, questi sistemi si differenziano anche per il livello di complessità tecnologica che comporta un aumento dei rischi applicativi e delle esigenze di controllo e di una governance rafforzata, nonché una maggiore "opacità" operativa.
In particolare si distinguono le seguenti famiglie:
- L'**IA statistica (data-driven)** si fonda sull'elaborazione di grandi quantità di dati mediante algoritmi complessi finalizzati a individuare correlazioni, classificazioni o previsioni. Diversamente dai sistemi deterministici basati su regole predefinite, tali modelli apprendono dai dati attraverso l'uso di modelli matematici.
- Il **machine learning** costituisce una specificazione dell'IA statistica basata su algoritmi statistici e matematici (ad esempio algoritmi di regressione, alberi decisionali o altri modelli supervisionati), capaci di apprendere pattern ricorrenti presenti nei dati strutturati. Nei modelli parametrici l'apprendimento avviene tramite l'ottimizzazione dei pesi associati alle variabili; nei modelli non parametrici, invece, l'apprendimento avviene mediante la selezione progressiva di regole e soglie che massimizzano la capacità predittiva.
- Le **reti neurali** rappresentano modelli computazionali ispirati al funzionamento dei neuroni. Le informazioni vengono trattate da nodi interconnessi organizzati in rete in grado di apprendere le rappresentazioni complesse dei dati. Il tratto distintivo rispetto agli algoritmi di machine learning consiste nella capacità di elaborare dati non strutturati — quali immagini, audio e testo — estraendo automaticamente le caratteristiche rilevanti e identificando autonomamente i pattern senza che questi debbano essere preventivamente definiti in modo esplicito.
- Il **deep learning** costituisce l'evoluzione più avanzata delle reti neurali ed è caratterizzato da architetture multilivello in grado di apprendere le strutture gerarchiche dei dati. In tali sistemi ogni livello della rete elabora l'output del precedente, consentendo al sistema di riconoscere strutture sempre più sofisticate nei dati (pattern complessi e non lineari). La profondità delle reti, rappresentata dal numero di livelli o strati, distingue i modelli di deep learning dalla famiglia di reti neurali "tradizionale" meno complessa.

- Infine, l'**IA generativa** rappresenta una delle evoluzioni più recenti e diffuse ed è basata su modelli fondazionali in grado di generare contenuti originali (testo, immagini, codice, audio o video) a partire da dati di addestramento su larga scala e opera prevalentemente tramite modelli di grandi dimensioni e architetture avanzate, spesso erogate come servizio. Ne costituiscono un esempio i Large Language Model (LLM) che sono modelli addestrati su enormi quantità di dati non strutturati mediante tecniche di self-supervised learning, che consentono al sistema di costruire rappresentazioni latenti complesse, tratte dai dati grezzi elaborati, e di produrre output coerenti con il contesto e rilevanti nel contenuto.

La successiva parte delle Linee Guida si presenta come maggiormente tecnica e introduce alcuni elementi innovativi quali: i livelli tecnologici dello stack IA, i livelli di autonomia dei sistemi, un'architettura logica di riferimento e l'uso delle personas nella PA. Peraltro, un'attenzione particolare è rivolta al ruolo dei dati nello sviluppo dei sistemi di IA e al ciclo di vita di questi sistemi.

Bozza di Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione