Sommario

1. Ambito di applicazione

1.2 Ambito soggettivo

Le presenti Linee guida per il procurement di Intelligenza Artificiale nella Pubblica Amministrazione (di seguito Linee guida) sono rivolte ai soggetti di cui all'articolo 2, comma 2, del CAD. Tali soggetti sono indicati nel documento con l'acronimo PA.

1.3 Ambito oggettivo

Le presenti Linee guida concernono le modalità di procurement dei sistemi di Intelligenza Artificiale con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo.

Esse si applicano a tutte le componenti di applicazioni e infrastrutture tecnologiche che impiegano tecnologie di Intelligenza Artificiale, sia come componente integrata sia come supporto alle funzionalità principali.

2. Riferimenti e sigle

Si veda il corrispondente paragrafo delle Linee guida sull'adozione di sistemi di Intelligenza Artificiale nella Pubblica Amministrazione

2.1 Note di lettura del documento

Si veda il corrispondente paragrafo delle Linee guida sull'adozione di sistemi di Intelligenza Artificiale nella Pubblica Amministrazione

2.1 Struttura del documento

Considerata la velocità dell'innovazione tecnologica, le Linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante evoluzione digitale. Di qui la scelta di corredare le Linee guida di "Strumenti", ovvero documenti a supporto dell'attività operativa di applicazione delle Linee guida.

L'elenco aggiornato degli Strumenti delle Linee guida IA è disponibile al link: <<da definire in fase di pubblicazione>>.

Gli Strumenti potranno essere periodicamente aggiornati per tener conto dell'evoluzione normativa e tecnologica e delle buone pratiche emergenti.

2.2 Riferimenti normativi

Sono riportati di seguito i principali atti normativi di riferimento per le presenti Linee guida.

[CDFUE] Carta dei diritti fondamentali dell'Unione Europea "2016/C 202/02"

[AI Act] Regolamento europeo (UE) 1689/2024 del 13 giugno 2024 del Parlamento Europeo e del Consiglio, che stabilisce regole armonizzate sull'Intelligenza Artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE)

2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'Intelligenza Artificiale).

[Data Act] Regolamento europeo (UE) 2023/2854 del 13 dicembre 2023 del Parlamento Europeo e del Consiglio, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

[DGA] Regolamento europeo (UE) 2022/868 del 30 maggio 2022 del Parlamento Europeo e del Consiglio, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

[CRA] Regolamento (UE) 2024/2847 del 23 ottobre 2024 del Parlamento europeo e del Consiglio, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (Cyber Resilience Act).

[Reg. UE 2018/1725] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[GDPR] Regolamento (UE) 2016/679 del 27 aprile 2016 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[Reg. UE 2012/1025] Regolamento (UE) n. 2012/1025 del 25 ottobre 2012 del Parlamento europeo e del Consiglio, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.

[Direttiva Open Data] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione).

[NIS 2] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

[CER] Direttiva 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (Critical Entities Resilience).

[Dir. (UE) 2016/680] Direttiva (UE) 2016/680 del 27 aprile 2016 del Parlamento europeo e del Consiglio relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[Dir. Prodotti] Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio.1

[Dlgs. 36/2023] Codice dei contratti pubblici

[L. 132/2025] Legge 23 settembre 2025, n. 132 recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale"

[L. 90/2024] Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici."

[D.L. 135/2018] Decreto-legge 14 dicembre 2018, n. 135 recante "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione", convertito in legge, con modificazioni, dall'art. 1, comma 1 della legge 11 febbraio 2019, n. 12.

[Accessibilità] Legge 9 gennaio 2004, n. 4 e s.m.i. recante "Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici".

[Codice privacy] Decreto legislativo 30 giugno 2003, n. 196 e s.m.i. recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

[CAD] Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale".

[D.Lgs. 36/2006] Decreto legislativo 24 gennaio 2006, n. 36 recante "Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE".

[Codice dei contratti] Decreto legislativo 31 marzo 2023, n.36 e s.m.i recante "Codice dei contratti pubblici in attuazione dell'art. 1 della legge 21 giugno 2022, n.78, recante delega al Governo in materia di contratti pubblici".

[D.lgs 200/2021] Decreto legislativo 8 novembre 2021, n. 200 recante "Attuazione della direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione)".

[D.lgs 82/2022] Decreto legislativo 27 maggio 2022, n. 82 recante "Attuazione della direttiva (UE) 2019/882 (CER) del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi".

[D.Lgs. 134/2024] Decreto legislativo 4 settembre 2024, n. 134. recante "Attuazione della direttiva (UE) 2022/2557 (CER) del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio".

[D.lgs. 138/2024] Decreto legislativo 4 settembre 2024, n. 138 recante "Recepimento della direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148".

[D.P.R. 81/2022] Decreto del Presidente della Repubblica 24 giugno 2022, n. 81. Regolamento recante individuazione degli adempimenti relativi ai piani assorbiti dal piano integrato di attività e organizzazione (PIAO).

[AI_ACT_PROHIB] C(2025) 884 Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

[Piano Triennale] D.P.C.M. 12 gennaio 2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026"

[PT agg. 2025] D.P.C.M. 3 dicembre 2024 recante "Aggiornamento 2025 del Piano triennale 2024-2026"

[PT agg. 2026] D.P.C.M. 9 settembre 2025 recante "Aggiornamento 2026 del Piano triennale 2024-2026

[REG_CLOUD] Regolamento unico per le infrastrutture e i servizi cloud per la PA n. 21007 adottato da ACN il 27 giugno 2024.

[Digital Decade] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01)

[Strategia IA] Strategia Italiana per l'Intelligenza Artificiale 2024-2026.

2.3 Linee guida di riferimento

Di seguito sono elencate le Linee guida emesse da AgID ai sensi dell'art. 71 del CAD e altra documentazione regolamentare, che sono richiamate, anche indirettamente, nel presente documento. Le linee guida AgID sono disponibili tramite il sito istituzionale al seguente indirizzo: https://www.agid.gov.it/it/linee-guida, dove sono pubblicati anche i relativi aggiornamenti in conseguenza dell'evoluzione tecnologica o della necessità di adeguamento alla normativa di riferimento.

[LLGG_IA] Linee guida per l'adozione di sistemi di Intelligenza Artificiale nella Pubblica Amministrazione

[LG_OPENDATA] Linee guida Open Data.

[LG-RIUSO] Linee guida su acquisizione e riuso di software per le Pubbliche Amministrazioni.

[LG_ACCESS] Linee guida sull'accessibilità degli strumenti informatici

[LLGG_DES] Linee guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione

[LG_DOC_INF] Linee guida sulla formazione, gestione e conservazione dei documenti informatici

[LG_PDND_INTER] Linee guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi delle basi dati

[LG_SIC_INTER] Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici

[LG_INTER_TEC] Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni

[ST_eDGUE] Specifiche tecniche per la definizione del DGUE elettronico italiano "eDGUE-IT"

2.4 Definizioni e acronimi

Le definizioni e gli acronimi sono descritti nello strumento A.

3. Come acquisire sistemi di Intelligenza Artificiale

3.1 Principi generali del procurement

I principi descritti nel presente paragrafo non esauriscono il quadro dei principi generali applicabili ai contratti pubblici, come definiti dalla normativa vigente dal Codice dei contratti pubblici e dalla disciplina europea in materia di appalti. Essi rappresentano piuttosto una individuazione mirata dei principi ritenuti maggiormente rilevanti ai fini del procurement dei sistemi di Intelligenza Artificiale con riferimento anche a quanto previsto dalla Legge 132/2025.

Il procurement di sistemi di Intelligenza Artificiale presenta caratteristiche peculiari rispetto all'acquisto di soluzioni ICT tradizionali e richiede, pertanto, un approccio consapevole e strutturato da parte delle Pubbliche Amministrazioni. I sistemi di IA sono infatti 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 e dell'evoluzione tecnologica complessiva dell'ecosistema in cui sono inseriti.

A differenza delle soluzioni software tradizionali, i sistemi di IA non si limitano a eseguire istruzioni predeterminate, ma possono incidere in modo diretto e significativo su procedimenti amministrativi, diritti fondamentali, aspettative di cittadini e imprese e modalità di esercizio della funzione pubblica. In molti casi, essi intervengono a supporto di attività valutative, istruttorie o decisionali, influenzando l'organizzazione del lavoro amministrativo e il rapporto tra amministrazione e utenti.

Per tali ragioni, l'azione delle Pubbliche Amministrazioni nel procurement di sistemi di Intelligenza Artificiale deve essere orientata da un insieme di principi generali che assumono valore trasversale rispetto alle diverse fasi del ciclo di vita del contratto, dalla programmazione e progettazione fino all'affidamento, alla stipula e all'esecuzione. Tali principi costituiscono il quadro di riferimento entro il quale devono essere assunte le decisioni di procurement e devono trovare concreta attuazione nelle scelte tecniche, organizzative e contrattuali operate dalle amministrazioni.

In coerenza con il Codice dei contratti pubblici, il procurement di sistemi di IA deve innanzitutto perseguire **il principio del risultato**, orientando le scelte verso soluzioni capaci di generare valore pubblico, migliorare la qualità dei servizi e garantire tempi di implementazione compatibili con le esigenze dell'azione amministrativa. Ciò implica la definizione chiara degli obiettivi del sistema, la

misurabilità delle prestazioni, la definizione di indicatori di qualità, il monitoraggio continuo dei tempi di implementazione, dei benefici attesi e della capacità della soluzione di generare valore pubblico.

Accanto a tale principio, assume rilievo **il principio della fiducia**, che si traduce nella responsabilizzazione delle amministrazioni, in qualità di stazioni appaltanti, rispetto alle scelte tecnologiche e contrattuali e nella valorizzazione delle competenze interne. L'adozione di sistemi di IA richiede infatti un presidio pubblico effettivo e consapevole, nonché la capacità di esercitare funzioni di indirizzo, controllo e supervisione lungo l'intero ciclo di vita del sistema. Ciò implica, inoltre, la semplificazione delle procedure ove compatibile con il livello di rischio, la valorizzazione delle competenze interne e il presidio effettivo sul sistema.

Parimenti centrale è **il principio dell'accesso al mercato**, che impone alle amministrazioni di favorire la più ampia partecipazione degli operatori economici, sia evitando requisiti non discriminatori o ingiustificatamente restrittivi sia promuovendo l'utilizzo di standard aperti, architetture modulari e soluzioni interoperabili. Ciò contribuisce a prevenire fenomeni di lock-in tecnologico ed economico e a rafforzare la contendibilità delle forniture nel tempo.

Nel solco di tali principi generali si collocano ulteriori principi operativi che assumono particolare rilevanza nel contesto dei sistemi di Intelligenza Artificiale.

Il principio di trasparenza richiede che la Pubblica Amministrazione sia in grado di comprendere, descrivere e documentare il funzionamento complessivo del sistema, almeno a livello architetturale, funzionale e decisionale. Ciò implica la conoscenza del ruolo svolto dall'orchestratore descritto nelle linee guida sullo sviluppo IA, delle tipologie di modelli impiegati, delle fonti dei dati utilizzati, delle modalità di trattamento delle informazioni lungo il ciclo di vita del sistema e delle interazioni con gli utenti finali.

La trasparenza non deve essere intesa esclusivamente in senso tecnico, ma assume una valenza amministrativa e istituzionale più ampia. Essa rappresenta un presupposto essenziale per la rendicontabilità dell'azione pubblica, per la legittimazione delle decisioni adottate con il supporto dell'IA e per l'esercizio dei poteri di controllo interno ed esterno. Nel procurement, tale principio deve tradursi in requisiti informativi chiari, documentazione completa e clausole contrattuali che assicurino all'amministrazione un adeguato livello di visibilità sul funzionamento del sistema di IA. In questo quadro, la tracciabilità deve essere garantita come caratteristica tecnica e organizzativa del fornitore,

affinché l'amministrazione possa accedere alle informazioni necessarie a comprendere, governare e verificare il comportamento del sistema lungo tutto il suo ciclo di vita.

Il principio di responsabilità implica che la Pubblica Amministrazione mantenga la piena titolarità delle decisioni amministrative e degli effetti prodotti attraverso l'impiego dei sistemi di IA. Anche quando il sistema è fornito da operatori economici esterni o erogato in modalità cloud, l'amministrazione non può delegare la responsabilità delle decisioni né rinunciare alla capacità di intervenire sul funzionamento del sistema.

Il procurement deve pertanto essere strutturato in modo da garantire la permanenza di un presidio pubblico effettivo sul sistema e sulla sua evoluzione nel tempo, attraverso la definizione di ruoli chiari, meccanismi di supervisione e strumenti di governance adeguati. Tale principio assume particolare rilievo nei contesti in cui l'IA incide su procedimenti amministrativi sensibili o su diritti giuridicamente rilevanti.

Il principio di proporzionalità richiede che le soluzioni di Intelligenza Artificiale siano adeguate rispetto agli obiettivi perseguiti, alla rilevanza del procedimento o del servizio coinvolto e al livello di rischio associato al loro utilizzo. In termini di procurement, questo comporta analisi del rischio, valutazione comparativa delle soluzioni, verifica dell'adeguatezza dell'IA rispetto al contesto tecnico-amministrativo e agli impatti sui diritti. Sistemi caratterizzati da elevata complessità o bassa spiegabilità devono essere adottati solo in presenza di benefici chiaramente motivati e documentati, evitando l'introduzione di soluzioni sovradimensionate o non necessarie.

Il principio di controllo si traduce nella necessità per la Pubblica Amministrazione di mantenere margini effettivi di supervisione tecnica, funzionale e organizzativa sul sistema. Ciò include la possibilità di monitorarne in modo continuo il comportamento, verificarne le prestazioni tramite audit, modificarne la configurazione, sostituirne componenti anche critiche e, ove necessario, sospenderne o cessarne l'utilizzo, nonché di attivare modalità operative alternative - quali meccanismi di fallback - idonee a garantire la continuità del servizio anche in presenza di malfunzionamenti, degrado delle prestazioni o indisponibilità di specifiche componenti tecnologiche. Il controllo rappresenta un elemento qualificante del procurement pubblico di IA e deve essere assicurato lungo l'intero ciclo contrattuale, con particolare attenzione alla fase di esecuzione.

Il principio di sostenibilità, infine, impone di considerare l'impatto economico, organizzativo, tecnologico e ambientale del sistema nel medio-lungo periodo. Le scelte di procurement devono tenere conto non solo dei costi iniziali di acquisizione, ma anche dei costi di esercizio, manutenzione, aggiornamento, formazione del personale e dismissione del sistema, assicurando un equilibrio tra CAPEX e OPEX (conto capitale e spesa corrente). Una valutazione sull'intero ciclo di vita consente di evitare soluzioni che, pur risultando convenienti nel breve periodo, generino nel tempo rigidità o oneri incompatibili con le esigenze della Pubblica Amministrazione.

Tabella 1Principi generali rilevanti per il procurement di IA

Principio	Implicazioni nel procurement
Risultato	Definizione chiara degli obiettivi del sistema di IA, misurabilità delle prestazioni, indicatori di qualità, monitoraggio dei tempi di implementazione e capacità della soluzione di generare valore pubblico.
Fiducia	Responsabilizzazione della stazione appaltante nelle scelte tecnologiche e contrattuali, semplificazione delle procedure ove compatibile con il livello di rischio, valorizzazione delle competenze interne e presidio effettivo sul sistema.
Accesso al mercato	Requisiti non discriminatori, apertura a soluzioni alternative, utilizzo di standard aperti e architetture modulari, prevenzione del lock-in tecnologico ed economico, favorendo la contendibilità delle forniture.
Trasparenza	Requisiti informativi, documentazione tecnica, accesso ai log, tracciabilità, spiegabilità e comprensibilità del funzionamento del sistema, nonché garanzia di contestabilità delle decisioni automatizzate e disponibilità di evidenze verificabili a supporto delle stesse.
Responsabilità	Ruoli chiari, supervisione umana, governance del sistema e permanenza della titolarità decisionale in capo alla PA.
Proporzionalità	Analisi del rischio, valutazione comparativa delle soluzioni, adeguatezza dell'IA rispetto al contesto tecnico-amministrativo e agli impatti sui diritti.
Controllo	Monitoraggio continuo, verificabilità tramite audit, possibilità di intervento tecnico e organizzativo, sostituibilità delle componenti critiche.

Principio	Implicazioni nel procurement
Sostenibilità	Analisi di ciclo di vita, valutazione dei costi evolutivi, equilibrio tra CAPEX e OPEX (conto capitale e spesa corrente), continuità operativa e capacità di governare l'evoluzione tecnologica.

I principi sopra richiamati si coordinano con quelli previsti dalle Linee Guida sull'adozione e lo sviluppo dei sistemi di IA, dei quali costituiscono una declinazione specifica in chiave di procurement.

3.2 Famiglie di sistemi di IA ai fini del procurement

Per una descrizione di dettaglio delle famiglie di sistemi di IA si rimanda al capitolo 3 delle Linee guida sullo sviluppo. Di seguito si riportano, per ciascuna famiglia, descrizione sintetica, caratteristiche prevalenti, implicazioni per il procurement e fabbisogno infrastrutturale.

Livello tecnologico: Artificial Intelligence

Con l'espressione "Artificial Intelligence" si intende l'insieme delle tecnologie capaci di svolgere compiti che richiedono capacità tipicamente umane, quali apprendimento, ragionamento o supporto decisionale.

La caratteristica prevalente è che si tratta di una "categoria ombrello", che comprende approcci eterogenei con livelli di complessità variabili.

In termini di procurement, ciò implica:

- la necessità di valutazioni preliminari strutturate sul contesto d'uso, sul rischio e sul valore pubblico atteso;
- la centralità della governance.

Il fabbisogno infrastrutturale è variabile in funzione della tecnologia adottata.

Livello tecnologico: AI statistica / data-driven

Con l'espressione "AI statistica / data-driven" si intendono sistemi basati su modelli statistici, analisi dei dati e tecniche predittive.

Le caratteristiche prevalenti di tali sistemi afferiscono alla maggiore prevedibilità dei comportamenti, il dominio applicativo generalmente circoscritto e la minore autonomia decisionale.

In termini di procurement, ciò implica:

- requisiti tecnici ben definiti;
- maggiore facilità di definizione delle prestazioni contrattuali;

- minore rischio di lock-in.

Il fabbisogno infrastrutturale è generalmente contenuto; spesso è compatibile con infrastrutture già disponibili.

Livello tecnologico: Machine Learning

Con l'espressione "Machine Learning" si intendono sistemi che apprendono automaticamente dai dati, migliorando le proprie prestazioni nel tempo.

Le caratteristiche prevalenti di tali sistemi sono la dipendenza significativa dalla qualità dei dataset; la necessità di addestramento e aggiornamento periodico; i risultati probabilistici.

In termini di procurement, ciò implica:

- il rafforzamento dei requisiti sulla gestione dei dati, sul monitoraggio delle performance e sulla documentazione del modello;
- l'opportunità di prevedere clausole evolutive.

Il fabbisogno infrastrutturale è moderato ma crescente; può richiedere capacità computazionali dedicate per l'addestramento.

Livello tecnologico: Neural Networks

Con l'espressione "Neural Networks" si intendono modelli ispirati alla struttura delle reti neurali biologiche, in grado di individuare pattern complessi nei dati.

Le caratteristiche prevalenti di tali modelli sono un'elevata capacità di elaborazione, una minore spiegabilità rispetto ai modelli statistici tradizionali e una maggiore complessità tecnica.

In termini di procurement, ciò implica:

- maggiore attenzione a trasparenza, auditabilità e controllo umano;
- incremento del rischio contrattuale legato alla complessità del modello.

Il fabbisogno infrastrutturale è medio-alto; è frequente la necessità di acceleratori hardware.

Livello tecnologico: Deep Learning

Con l'espressione "Deep Learning" si indica una sottocategoria delle reti neurali basata su architetture multilivello ad alta intensità computazionale.

Caratteristiche prevalenti sono: prestazioni avanzate ma minore spiegabilità; elevata dipendenza dall'infrastruttura e dall'ottimizzazione tecnica.

In termini di procurement, ciò implica:

- necessità di governance rafforzata, valutazioni approfondite di sostenibilità economica;
- presidio dei rischi di dipendenza tecnologica.

Il fabbisogno infrastrutturale è elevato; tipicamente richiede GPU o infrastrutture specializzate, con impatti rilevanti sugli OPEX.

Livello tecnologico: Generative AI

Con l'espressione "Generative AI" si indicano sistemi basati su modelli fondazionali in grado di generare contenuti originali (testo, immagini, codice, audio o video) a partire da dati di addestramento su larga scala. Operano prevalentemente tramite modelli di grandi dimensioni e architetture avanzate, spesso erogate come servizio.

Caratteristiche prevalenti di questi sistemi sono: elevata flessibilità d'uso; capacità generaliste; comportamento non sempre pienamente deterministico; forte dipendenza dalla qualità dei prompt, dall'orchestrazione e dai meccanismi di controllo; possibile variabilità degli output.

In termini di procurement, ciò implica:

- necessità di governance rafforzata;
- particolare attenzione alla gestione dei dati in input e output;
- requisiti stringenti su trasparenza, logging e supervisione umana;
- valutazione del rischio di lock-in tecnologico;
- opportunità di prevedere clausole su portabilità, auditabilità e controllo dei costi di utilizzo.

Il fabbisogno infrastrutturale è generalmente elevato ma spesso esternalizzato. È inoltre frequente il ricorso a servizi cloud o API; si rilevano, infine, limitata eseguibilità on-premises salvo disponibilità di infrastrutture ad alte prestazioni e rilevante incidenza dei costi operativi legati al consumo.

Tabella 2 Famiglie di sistemi di IA e implicazioni per il procurement

Livello tecnologico	Descrizione sintetica	Caratteristiche prevalenti	Implicazioni per il procurement	Fabbisogno infrastrutturale
Artificial Intelligence	Insieme delle tecnologie capaci di svolgere compiti che richiedono capacità tipicamente umane, quali apprendimento, ragionamento o	Categoria ombrello che comprende approcci eterogenei con livelli di complessità variabili.	Necessità di valutazioni preliminari strutturate sul contesto d'uso, sul rischio e sul valore pubblico atteso; centralità della governance.	Variabile in funzione della tecnologia adottata.

Livello tecnologico	Descrizione sintetica	Caratteristiche prevalenti	Implicazioni per il procurement	Fabbisogno infrastrutturale
	supporto decisionale.			
AI statistica / data-driven	Sistemi basati su modelli statistici, analisi dei dati e tecniche predittive.	Maggiore prevedibilità dei comportamenti, dominio applicativo generalmente circoscritto, minore autonomia decisionale.	Requisiti tecnici ben definiti, maggiore facilità di definizione delle prestazioni contrattuali; minore rischio di lock-in.	Generalmente contenuto; spesso compatibile con infrastrutture già disponibili.
Machine Learning	Sistemi che apprendono automaticamente dai dati migliorando le proprie prestazioni nel tempo.	Dipendenza significativa dalla qualità dei dataset, necessità di addestramento e aggiornamento periodico, risultati probabilistici.	Rafforzamento dei requisiti sulla gestione dei dati, sul monitoraggio delle performance e sulla documentazione del modello; opportuno prevedere clausole evolutive.	Moderato ma crescente; può richiedere capacità computazionali dedicate per l'addestramento.
Neural Networks	Modelli ispirati alla struttura delle reti neurali biologiche, in grado di individuare pattern complessi nei dati.	Elevata capacità di elaborazione, minore spiegabilità rispetto ai modelli statistici tradizionali, maggiore complessità tecnica.	Maggiore attenzione a trasparenza, auditabilità e controllo umano; incremento del rischio contrattuale legato alla complessità del modello.	Medio-alto; frequente necessità di acceleratori hardware.

Livello tecnologico	Descrizione sintetica	Caratteristiche prevalenti	Implicazioni per il procurement	Fabbisogno infrastrutturale
Deep Learning	Sottocategoria delle reti neurali basata su architetture multilivello ad alta intensità computazionale.	Prestazioni avanzate ma minore spiegabilità, elevata dipendenza dall'infrastruttura e dall'ottimizzazione tecnica.	Necessità di governance rafforzata, valutazioni approfondite di sostenibilità economica e presidio dei rischi di dipendenza tecnologica.	Elevato; tipicamente richiede GPU o infrastrutture specializzate, con impatti rilevanti sugli OPEX.
Generative AI	Sistemi basati su modelli fondazionali in grado di generare contenuti originali (testo, immagini, codice, audio o video) a partire da dati di addestramento su larga scala. Operano prevalentemente tramite modelli di grandi dimensioni e architetture avanzate, spesso erogate come servizio	Elevata flessibilità d'uso; capacità generaliste; comportamento non sempre pienamente deterministico; forte dipendenza dalla qualità dei prompt, dall'orchestrazione e dai meccanismi di controllo; possibile variabilità degli output	Necessità di governance rafforzata; particolare attenzione alla gestione dei dati in input e output; requisiti stringenti su trasparenza, logging e supervisione umana; valutazione del rischio di lock-in tecnologico; opportunità di prevedere clausole su portabilità, auditabilità e controllo dei costi di utilizzo	Generalmente elevato ma spesso esternalizzato; frequente ricorso a servizi cloud o API; limitata eseguibilità on-premises salvo disponibilità di infrastrutture ad alte prestazioni; rilevante incidenza dei costi operativi legati al consumo.

3.3 Architettura logica di riferimento: implicazioni per il procurement

Per la descrizione dell'architettura logica di riferimento, si rinvia al capitolo 3 delle Linee guida sullo sviluppo di sistemi IA.

Di seguito, si riportano, per ciascun macro-componente, le implicazioni di tale architettura in termini di requisiti di procurement e contrattuali.

Orchestratore

L'obiettivo di governabilità dell'orchestratore è quello di mantenere il controllo sui flussi operativi e sulle logiche di integrazione.

In termini di procedura di acquisto, questo comporta il richiedere configurabilità, documentazione tecnica e trasparenza delle regole di funzionamento.

In termini di requisiti contrattuali, si raccomanda di prevedere obblighi di documentazione, diritto di accesso alle configurazioni e condizioni per la sostituibilità.

Modelli di IA

Gli obiettivi di governabilità nel macro-componente Modelli di IA sono due: evitare dipendenze tecnologiche e preservare la possibilità di evoluzione.

In termini di procedura di acquisto, questo implica il prevedere requisiti di separabilità dall'orchestratore e criteri di sostituibilità.

In termini di requisiti contrattuali, si raccomanda di prevedere clausole di aggiornamento, diritti di utilizzo, supporto alla migrazione verso modelli alternativi.

Dati

Gli obiettivi di governabilità nel macro-componente Dati consistono nel garantire disponibilità, accessibilità e portabilità.

In termini di procedura di acquisto, questo implica richiedere standard aperti, formati interoperabili e tracciabilità dei trattamenti.

In termini di requisiti contrattuali, si raccomanda di presidiare diritti di accesso, portabilità, obblighi di restituzione e divieto di utilizzi non autorizzati.

Tool applicativi

Gli obiettivi di governabilità nel macro-componente Tool applicativi consistono nell'assicurare integrazione con l'ecosistema digitale dell'ente.

In termini di procedura di acquisto, questo implica valutare compatibilità con sistemi esistenti e capacità di interoperabilità.

In termini di requisiti contrattuali, si raccomanda di prevedere presidi di continuità operativa, condizioni di subentro e supporto all'integrazione.

Tabella 3: Implicazioni dell'architettura logica sui requisiti di procurement e contrattuali

Macro-componente architetturale	Obiettivi di governabilità	Implicazioni per la procedura di acquisto	Presidi contrattuali raccomandati
Orchestratore	Mantenere il controllo sui flussi operativi e sulle logiche di integrazione	Richiedere configurabilità, documentazione tecnica e trasparenza delle regole di funzionamento	Obblighi di documentazione; diritto di accesso alle configurazioni; condizioni per la sostituibilità
Modelli di IA	Evitare dipendenze tecnologiche e preservare la possibilità di evoluzione	Prevedere requisiti di separabilità dall'orchestratore e criteri di sostituibilità	Clausole di aggiornamento; diritti di utilizzo; supporto alla migrazione verso modelli alternativi
Dati	Garantire disponibilità, accessibilità e portabilità	Richiedere standard aperti, formati interoperabili e tracciabilità dei trattamenti	Diritti di accesso; portabilità; obblighi di restituzione; divieto di utilizzi non autorizzati
Tool applicativi	Assicurare integrazione con l'ecosistema digitale dell'ente	Valutare compatibilità con sistemi esistenti e capacità di interoperabilità	Presidi di continuità operativa; condizioni di subentro; supporto all'integrazione

3.4 Ruolo del dato nel procurement

Nel procurement di sistemi di Intelligenza Artificiale, il dato assume un ruolo centrale e strutturale, che va ben oltre la funzione di semplice input per il funzionamento dei modelli algoritmici. I dati costituiscono infatti un vero e proprio **asset pubblico**, strettamente connesso all'esercizio della funzione tecnico-amministrativa, alla qualità dei servizi erogati e alla capacità della Pubblica Amministrazione di mantenere il controllo, la governabilità e la continuità operativa dei sistemi di IA nel tempo.

A differenza di quanto avviene per molte soluzioni ICT tradizionali, nei sistemi di IA il valore della soluzione tecnologica è fortemente dipendente dalla disponibilità, dalla qualità e dalla gestione dei dati utilizzati. In assenza di un adeguato presidio sul dato, anche sistemi tecnologicamente avanzati possono produrre risultati inaffidabili, distorsivi o non coerenti con le finalità pubbliche perseguite. Per tale ragione, il dato deve essere considerato una componente autonoma e qualificante del sistema di IA, distinta dai modelli e dagli strumenti applicativi, e deve essere oggetto di valutazione esplicita sin dalle fasi di programmazione e progettazione del procurement.

Le Pubbliche Amministrazioni sono pertanto chiamate a integrare il ruolo del dato in modo sistematico nelle proprie scelte di procurement, evitando approcci nei quali la gestione dei dati sia implicitamente demandata al fornitore o trattata come elemento accessorio. Il dato rappresenta infatti un fattore determinante ai fini della sostenibilità dell'investimento, della riduzione dei rischi di lock-in e della tutela dell'interesse pubblico nel medio-lungo periodo.

Un primo profilo di particolare rilevanza riguarda la **tipologia dei dati trattati dal sistema di IA**. Le amministrazioni dovrebbero distinguere in modo chiaro, documentato e verificabile tra:

- dati nella titolarità o nella disponibilità della Pubblica Amministrazione;
- dati personali, sensibili o appartenenti a categorie particolari, ai sensi della normativa vigente in materia di protezione dei dati personali;
- dati provenienti da fonti di terzi, inclusi dataset commerciali o open data esterni;
- dati generati dal sistema di IA nel corso del suo utilizzo, inclusi output, log di funzionamento, metadati, informazioni di tracciamento e dati di utilizzo.

Tale distinzione è essenziale ai fini della corretta definizione dei requisiti architetturali, delle misure di sicurezza e delle clausole contrattuali, nonché per una chiara ripartizione delle responsabilità tra amministrazione e fornitore. In particolare, la mancata distinzione tra dati di origine pubblica e dati generati o arricchiti dal sistema può determinare ambiguità nella titolarità e nei diritti di utilizzo, con effetti rilevanti sulla capacità della PA di riutilizzare o migrare il sistema nel tempo.

Un secondo profilo centrale concerne **la governance del dato**. Il procurement di sistemi di IA deve assicurare che la Pubblica Amministrazione mantenga un controllo effettivo sui dati utilizzati e generati dal sistema, chiarendo in modo esplicito e contrattualmente vincolante i diritti di accesso, utilizzo, conservazione, riutilizzo e portabilità dei dati.

In particolare, devono essere disciplinate con attenzione le condizioni alle quali i dati possono essere utilizzati dal fornitore, anche per finalità ulteriori quali l'addestramento, il miglioramento o il riuso dei modelli di IA. Tali utilizzi devono essere valutati in modo coerente con le finalità pubbliche perseguite, con la normativa vigente in materia di protezione dei dati personali e con il principio di minimizzazione del trattamento, evitando che il procurement determini forme di valorizzazione privata del dato pubblico non compatibili con l'interesse generale.

Le amministrazioni devono pertanto prevedere clausole contrattuali che limitino o regolamentino in modo stringente l'uso dei dati al di fuori del perimetro del servizio affidato, assicurando la piena trasparenza delle modalità di trattamento, nonché la tracciabilità delle operazioni effettuate sui dati e la possibilità di svolgere attività di audit e verifica sul loro utilizzo.

Particolare attenzione dovrebbe inoltre essere dedicata alla distinzione tra dati forniti dall'amministrazione, dati generati durante l'esercizio del sistema e dati eventualmente utilizzati dal fornitore per l'addestramento o il miglioramento dei modelli, al fine di evitare ambiguità nella titolarità e nelle modalità di utilizzo delle informazioni.

Un ulteriore profilo di rilievo riguarda la **localizzazione dei dati e le modalità di trattamento**. Le amministrazioni sono chiamate a valutare attentamente le scelte relative alla collocazione dei dati, considerando soluzioni on-premises, cloud o ibride in relazione alle esigenze di sovranità del dato, sicurezza delle informazioni, continuità operativa e conformità alla normativa vigente. In tale contesto, particolare attenzione deve essere riservata alle tecniche di protezione dei dati, incluse le misure di crittografia sia in transito sia a riposo, che rappresentano presìdi essenziali indipendentemente

dall'infrastruttura utilizzata. Tali scelte producono effetti diretti sulla capacità della PA di esercitare un controllo effettivo sul sistema di IA e di intervenire tempestivamente in caso di criticità o interruzioni del servizio.

Nel procurement, le decisioni sulla localizzazione dei dati devono essere coerenti con il livello di rischio associato al contesto applicativo e con la natura dei dati trattati. In particolare, per sistemi che incidono su procedimenti amministrativi sensibili o su diritti fondamentali, è opportuno adottare soluzioni che garantiscano un elevato grado di controllo e di resilienza, evitando dipendenze eccessive da infrastrutture non governabili.

Un quarto profilo riguarda la **qualità, l'affidabilità e l'aggiornamento dei dati**. La qualità dei risultati prodotti dai sistemi di IA è strettamente dipendente dalla qualità dei dati utilizzati, sia in fase di addestramento sia durante l'esercizio del sistema. Le amministrazioni devono pertanto prevedere, già in fase di procurement, requisiti specifici volti a garantire la correttezza, la completezza, la tracciabilità e l'aggiornamento continuo dei dati.

Tali requisiti devono essere accompagnati da meccanismi di verifica e controllo da attuare nel corso dell'esecuzione contrattuale, inclusi audit sui dati, procedure di validazione degli aggiornamenti e strumenti di monitoraggio delle prestazioni del sistema. In assenza di tali presidi, il rischio è che il sistema produca risultati progressivamente meno affidabili o non coerenti con le finalità amministrative.

Il ruolo del dato assume particolare importanza anche in relazione alla **continuità amministrativa** e alla fase di cessazione o transizione del contratto. Il procurement deve prevedere clausole idonee a garantire la restituzione, la portabilità o la conservazione dei dati al termine del rapporto contrattuale, assicurando che l'amministrazione possa continuare a esercitare le proprie funzioni anche in caso di cambio di fornitore o di tecnologia. La mancata previsione di tali clausole può determinare situazioni di dipendenza irreversibile dal fornitore e compromettere la capacità della PA di evolvere nel tempo.

Infine, il dato rappresenta un elemento chiave per la **valorizzazione del patrimonio informativo pubblico**. Le amministrazioni sono chiamate a valutare, nel rispetto della normativa vigente, le opportunità di riutilizzo e interoperabilità dei dati e a promuovere forme di cooperazione interistituzionale per la condivisione e l'integrazione delle basi informative tra amministrazioni. Tale cooperazione può realizzarsi, ad esempio, attraverso l'utilizzo di infrastrutture nazionali di

interoperabilità, la condivisione di basi dati tramite piattaforme pubbliche di scambio dati, la realizzazione di repository o knowledge base condivise tra enti, nonché mediante modelli di collaborazione tra amministrazioni centrali, regionali e locali finalizzati allo sviluppo e al riuso di dataset e servizi digitali basati sui dati. Approcci di questo tipo favoriscono economie di scala, riducono le duplicazioni informative e contribuiscono allo sviluppo di servizi pubblici più efficaci.

Il ruolo del dato, dunque, resta elevato lungo l'intero ciclo di procurement, acquisendo aspetti chiave diversi in funzione della specifica fase: programmazione, progettazione, affidamento, stipula. I principi a cui allinearsi sono, in ciascuna fase, il principio di risultato, il principio della fiducia e il principio dell'accesso al mercato.

In fase di programmazione sono da considerarsi aspetti chiave:

- un'analisi del fabbisogno basata su dati affidabili e aggiornati;
- la verifica della disponibilità, qualità e provenienza del dato;
- la mappatura delle fonti informative interne ed esterne;
- la valutazione preliminare dei rischi (tecnici, economici, organizzativi);
- la coerenza con le strategie digitali e di interoperabilità.

In virtù del principio di risultato, l'obiettivo per la PA è investire solo in iniziative sostenibili e ad alto valore pubblico.

In virtù del principio della fiducia, l'obiettivo per la PA è supportare decisioni motivate e tracciabili.

In virtù del principio dell'accesso al mercato, l'obiettivo per la PA è progettare fabbisogni non discriminatori e tecnologicamente neutri.

In fase di progettazione sono da considerarsi aspetti chiave:

- la definizione della titolarità e della governance del dato;
- i requisiti di sicurezza, protezione e conformità normativa;
- gli standard di qualità, interoperabilità e portabilità;
- le architetture aperte e documentate;
- i modelli di gestione e aggiornamento del dato.

In virtù del principio di risultato, l'obiettivo per la PA è garantire controllo, affidabilità e durabilità delle soluzioni.

In virtù del principio della fiducia, l'obiettivo per la PA è ridurre ambiguità progettuali e rischio di errori amministrativi.

In virtù del principio dell'accesso al mercato, l'obiettivo per la PA è evitare specifiche restrittive favorendo pluralità di operatori.

In fase di affidamento sono da considerarsi aspetti chiave:

- requisiti tecnici e funzionali chiari e verificabili;
- criteri di valutazione oggettivi e misurabili;
- trasparenza delle basi informative di gara;
- tracciabilità dei dati utilizzati nella valutazione delle offerte;
- coerenza con standard aperti e sicurezza;
- documentazione completa di dataset, metriche e benchmark.

In virtù del principio di risultato, l'obiettivo per la PA è selezionare l'offerta con il miglior rapporto qualità-prezzo.

In virtù del principio della fiducia, l'obiettivo per la PA è garantire procedure leggibili, motivate e difendibili.

In virtù del principio dell'accesso al mercato, gli obiettivi per la PA sono due: il primo è massimizzare concorrenza e partecipazione; il secondo è ridurre il rischio di contenzioso e dipendenza dal fornitore.

In fase di stipula sono da considerarsi aspetti chiave:

- clausole su accesso, proprietà, utilizzo e riuso dei dati;
- obblighi di portabilità e restituzione in formati aperti;
- livelli di servizio (SLA) misurabili;
- condizioni per interoperabilità e continuità operativa;
- meccanismi di audit e verifica.

In virtù del principio di risultato, l'obiettivo per la PA è assicurare piena disponibilità del dato lungo il ciclo contrattuale.

In virtù del principio della fiducia, l'obiettivo per la PA è definire responsabilità chiare tra PA e fornitore.

In virtù del principio dell'accesso al mercato, l'obiettivo per la PA è prevenire lock-in tecnologico e informativo.

Tabella 4: Ruolo del dato lungo il ciclo di procurement

Fase	Aspetti chiave del dato	Obiettivi per la PA (allineamento ai principi)
Programmazione	- Analisi del fabbisogno basata su dati affidabili e aggiornati - Verifica della disponibilità, qualità e provenienza del dato - Mappatura delle fonti informative interne ed esterne - Valutazione preliminare dei rischi (tecnici, economici, organizzativi) - Coerenza con strategie digitali e di interoperabilità	**Risultato:** investire solo in iniziative sostenibili e ad alto valore pubblico **Fiducia:** supportare decisioni motivate e tracciabili **Accesso al mercato:** progettare fabbisogni non discriminatori e tecnologicamente neutri
Progettazione	- Definizione della titolarità e della governance del dato - Requisiti di sicurezza, protezione e conformità normativa - Standard di qualità, interoperabilità e portabilità - Architetture aperte e documentate - Modelli di gestione e aggiornamento del dato	**Risultato:** garantire controllo, affidabilità e durabilità delle soluzioni **Fiducia:** ridurre ambiguità progettuali e rischio di errori amministrativi **Accesso al mercato:** evitare specifiche restrittive favorendo pluralità di operatori
Affidamento	- Requisiti tecnici e funzionali chiari e verificabili	**Risultato:** selezionare l'offerta con il miglior rapporto qualità-prezzo

Fase	Aspetti chiave del dato	Obiettivi per la PA (allineamento ai principi)
	- Criteri di valutazione oggettivi e misurabili - Trasparenza delle basi informative di gara - Tracciabilità dei dati utilizzati nella valutazione delle offerte - Coerenza con standard aperti e sicurezza - Documentazione completa di dataset, metriche e benchmark	**Fiducia:** garantire procedure leggibili, motivate e difendibili **Accesso al mercato:** massimizzare concorrenza e partecipazione. Ridurre rischio di contenzioso e dipendenza dal fornitore
Stipula	- Clausole su accesso, proprietà, utilizzo e riuso dei dati - Obblighi di portabilità e restituzione in formati aperti - Livelli di servizio (SLA) misurabili - Condizioni per interoperabilità e continuità operativa - Meccanismi di audit e verifica	**Risultato:** assicurare piena disponibilità del dato lungo il ciclo contrattuale **Fiducia:** definire responsabilità chiare tra PA e fornitore **Accesso al mercato:** prevenire lock-in tecnologico e informativo

3.5 Impatti delle scelte architetturali su costi, controllo e rischio

Le scelte architetturali adottate nel procurement di sistemi di Intelligenza Artificiale incidono in modo diretto e significativo sui costi complessivi del sistema, sul grado di controllo esercitabile dalla Pubblica Amministrazione e sull'esposizione a rischi tecnologici, economici e organizzativi. A differenza delle forniture ICT tradizionali, nei sistemi di IA l'architettura non rappresenta un elemento neutro o meramente tecnico, ma costituisce una leva strategica che condiziona l'intero ciclo di vita del contratto e la capacità dell'amministrazione di governare la soluzione nel tempo. Essa può inoltre comportare

la necessità di adattare i processi organizzativi e operativi dell'amministrazione, incidendo sulle modalità di erogazione dei servizi, sui flussi decisionali e sulle competenze richieste al personale

Per tali ragioni, il procurement di sistemi di IA deve adottare una prospettiva di **costo totale di possesso – Total Cost of Ownership - TCO**, superando una visione limitata ai soli costi di acquisizione iniziale. Le amministrazioni sono chiamate a considerare in modo sistematico i costi di esercizio, manutenzione, aggiornamento, integrazione, formazione del personale, gestione dei dati e, infine, di dismissione o transizione del sistema. Le scelte architetturali effettuate in fase di progettazione del procurement incidono in modo determinante su tutte queste dimensioni.

Un primo profilo di rilievo riguarda l'impatto dell'architettura sui **costi di esercizio e di evoluzione del sistema**. Architetture fortemente accentrate, proprietarie o scarsamente modulari possono apparire convenienti nella fase iniziale di affidamento, ma tendono a generare costi crescenti nel tempo, legati alla difficoltà di intervenire su singole componenti, alla necessità di ricorrere al medesimo fornitore per ogni aggiornamento e alla limitata contendibilità del servizio. Al contrario, architetture modulari e basate su interfacce documentate consentono una maggiore flessibilità e favoriscono una gestione più efficiente dei costi nel medio-lungo periodo.

Le scelte architetturali incidono inoltre sulla **capacità della PA di esercitare un controllo effettivo sul sistema di IA**. Un'architettura che separa in modo chiaro orchestratore, modelli, dati e tool applicativi consente all'amministrazione di monitorare il comportamento del sistema, di intervenire su singole componenti e di verificare la coerenza tra le prestazioni attese e quelle effettivamente erogate. In tale prospettiva, è opportuno privilegiare architetture che evitino la dipendenza da un'unica istanza del modello o da una singola pipeline tecnologica, favorendo configurazioni nelle quali possano coesistere modelli, strumenti e pipeline differenti. Ciò aumenta l'affidabilità complessiva del sistema, riduce il rischio di lock-in e rafforza la capacità dell'amministrazione di adattare la soluzione all'evoluzione tecnologica e alle esigenze operative. Al contrario, soluzioni monolitiche o opache riducono significativamente la capacità di controllo pubblico e possono compromettere la possibilità di garantire trasparenza e rendicontabilità dell'azione amministrativa.

Il grado di controllo esercitabile dalla PA è strettamente connesso anche alla **gestione del rischio**. Nel procurement di sistemi di IA, i rischi non si limitano a profili tecnici, ma includono rischi organizzativi, economici, reputazionali e, in taluni casi, profili di responsabilità amministrativa, civile, contabile e, ove rilevante, anche penale. Le scelte architetturali possono amplificare o mitigare tali

rischi, incidendo sulla prevedibilità del comportamento del sistema, sulla possibilità di intervenire in caso di malfunzionamenti e sulla resilienza complessiva della soluzione.

Un rischio particolarmente rilevante è rappresentato dal **lock-in tecnologico ed economico**, che può manifestarsi quando l'architettura del sistema rende di fatto impossibile o eccessivamente onerosa la sostituzione del fornitore o di singole componenti. Tale rischio è spesso associato all'utilizzo di orchestratori proprietari non sostituibili, di modelli strettamente integrati con l'infrastruttura del fornitore o di formati di dati non portabili. Il procurement deve pertanto valutare con attenzione tali profili, prevedendo misure architetturali e contrattuali idonee a preservare la libertà di scelta dell'amministrazione nel tempo.

Le scelte architetturali incidono anche sui **costi indiretti** del sistema di IA, spesso sottovalutati in fase di affidamento. Tra questi rientrano i costi di formazione del personale, necessari affinché l'amministrazione possa comprendere e governare il sistema, nonché i costi organizzativi legati all'adattamento dei processi tecnico-amministrativi e delle modalità operative. Architetture eccessivamente complesse e/o poco documentate possono aumentare in modo significativo tali costi, riducendo l'effettivo valore pubblico generato dalla soluzione.

Un ulteriore profilo riguarda l'impatto delle scelte architetturali sulla **continuità amministrativa**. Sistemi di IA fortemente dipendenti da infrastrutture esterne o da servizi erogati in modalità esclusiva dal fornitore possono esporre l'amministrazione a rischi di interruzione del servizio, difficoltà di migrazione o perdita di accesso ai dati. In tale prospettiva, le amministrazioni dovrebbero prevedere adeguati piani di continuità operativa e soluzioni di fallback, al fine di garantire la prosecuzione delle attività anche in presenza di malfunzionamenti, indisponibilità delle infrastrutture o cessazione del rapporto contrattuale. Il costo di un'eventuale transizione verso nuove soluzioni può risultare particolarmente elevato, sia in termini economici sia organizzativi.

Nel procurement, tali considerazioni devono tradursi in una valutazione ex ante dei rischi associati alle diverse opzioni architetturali e nella previsione di meccanismi di mitigazione adeguati. Ciò include, ad esempio, la definizione di clausole di uscita, la previsione di obblighi di supporto alla migrazione, la documentazione dell'architettura e delle configurazioni adottate e la disponibilità dei dati e dei modelli al termine del contratto.

Va tenuto conto, inoltre, che le scelte di deployment di sistemi di IA ad alta intensità computazionale possono generare effetti indiretti sulla disponibilità e affidabilità delle infrastrutture energetiche locali, in funzione delle specifiche esigenze di alimentazione e di connessione, in particolare in presenza di carichi concentrati, non programmabili o localizzati in aree non originariamente dimensionate per tali utilizzi. E' opportuno, pertanto, valutare adeguatamente la tipologia di sistema adottato anche in funzione delle eventuali esigenze di eventuali adeguamenti delle reti di distribuzione e trasmissione

Infine, le scelte architetturali assumono rilievo anche in relazione alla **valutazione economica complessiva del sistema**, che deve essere condotta in una prospettiva di ciclo di vita. Le amministrazioni sono chiamate a superare logiche di valutazione basate esclusivamente sul prezzo iniziale e ad adottare strumenti di analisi che consentano di stimare in modo più accurato i costi complessivi e i rischi associati alle diverse soluzioni. In tale contesto, l'architettura del sistema rappresenta una variabile fondamentale per comprendere la sostenibilità economica dell'investimento e per orientare scelte di procurement coerenti con il principio di buon andamento.

In conclusione, le scelte architetturali nel procurement di sistemi di Intelligenza Artificiale devono essere considerate come decisioni strategiche, in grado di influenzare in modo significativo costi, controllo e rischio lungo l'intero ciclo di vita del contratto. Un approccio consapevole e strutturato all'architettura consente alle Pubbliche Amministrazioni di rafforzare il proprio ruolo di governo della tecnologia, di ridurre l'esposizione a rischi non governabili e di massimizzare il valore pubblico generato dall'adozione dell'IA.

3.5.1 Neutralità hardware, acceleratori e portabilità dei sistemi di IA

I sistemi di Intelligenza Artificiale, in particolare quelli basati su modelli di machine learning e deep learning, possono richiedere elevate capacità computazionali nelle fasi di addestramento e inferenza. Per rispondere a tali esigenze, il mercato ha sviluppato acceleratori hardware specializzati — quali GPU, TPU e dispositivi analoghi — nonché ambienti software ottimizzati per il calcolo parallelo.

Molte di queste soluzioni presentano tuttavia un elevato grado di integrazione verticale tra hardware, software e servizi, che può tradursi in una dipendenza strutturale da specifiche tecnologie o fornitori. Nel medio-lungo periodo, tale dipendenza può limitare la capacità delle amministrazioni di migrare i

sistemi verso infrastrutture alternative, adattare le soluzioni a contesti operativi eterogenei e valorizzare infrastrutture locali, consortili o a controllo pubblico.

Architetture hardware-agnostic

Per architetture hardware-agnostic si intendono sistemi progettati in modo da separare il modello di IA e la logica applicativa dal livello hardware sottostante, consentendo l'esecuzione su infrastrutture differenti senza modifiche sostanziali al funzionamento del sistema.

Questo approccio non esclude l'impiego di acceleratori dedicati, ma evita che essi diventino un requisito imprescindibile per l'operatività. L'eventuale assenza di acceleratori può comportare una riduzione delle prestazioni, ma non deve determinare l'impossibilità di utilizzo del sistema.

Ottimizzazione dei modelli ed esecuzione su CPU

L'evoluzione delle tecniche di ottimizzazione consente oggi di ridurre significativamente il fabbisogno computazionale dei sistemi di IA. Tra queste rientrano, a titolo esemplificativo:

- la riduzione delle dimensioni del modello;
- l'uso di rappresentazioni numeriche a precisione ridotta;
- il trasferimento delle capacità di modelli complessi verso modelli più piccoli e specializzati.

Tali tecniche permettono, in molti casi, l'esecuzione dei modelli anche su infrastrutture basate su CPU general-purpose, , anche mediante l'uso di modelli di model compression, quantization e distillation per consentire l'esecuzione anche su CPU, anche in contesti agentici distribuiti, come descritto nella Linea Guida Sviluppo al paragrafo 5.1 (Pianificazione e design) e 4.2.6.2 (Uso dei dati nella fase di esercizio), ampliando le possibilità di distribuzione e contribuendo alla riduzione dei costi energetici e operativi.

Implicazioni per la Pubblica Amministrazione

Nel contesto della Pubblica Amministrazione, la portabilità dei sistemi di IA e la possibilità di esecuzione su hardware eterogeneo assumono una valenza strategica. Esse contribuiscono a:

- ridurre il rischio di lock-in tecnologico;
- aumentare la resilienza rispetto a vincoli di mercato o di approvvigionamento;
- favorire lo sviluppo di una filiera nazionale dell'IA;
- migliorare la sostenibilità ambientale attraverso un uso più efficiente delle risorse computazionali.

La neutralità hardware e l'efficienza dei modelli devono pertanto essere considerate fattori abilitanti nella progettazione e gestione dei sistemi di IA, e non meri aspetti tecnici.

Esempi di clausole contrattuali

Neutralità hardware

Il sistema di Intelligenza Artificiale deve essere progettato secondo principi di neutralità hardware, garantendo l'esecuzione su infrastrutture computazionali eterogenee ed evitando dipendenze strutturali da specifiche architetture, acceleratori o tecnologie proprietarie.

Portabilità e reversibilità

Il fornitore deve assicurare la portabilità del sistema e delle sue componenti essenziali, consentendo la migrazione verso ambienti alternativi senza oneri tecnici o economici non giustificati, né perdita di funzionalità rilevanti.

Efficienza e fallback CPU

Il sistema deve prevedere modalità di esecuzione alternative, basate su tecniche di ottimizzazione dei modelli, che consentano l'utilizzo anche su infrastrutture CPU-only, garantendo continuità operativa e livelli di servizio proporzionati al contesto d'uso.

Altri esempi di clausole contrattuali potranno essere riportati in apposito strumento.

3.6 Elementi di cybersicurezza per il procurement

La sicurezza dei sistemi di IA è un requisito essenziale per l'adozione, l'acquisizione e lo sviluppo dell'intelligenza artificiale nella Pubblica Amministrazione. Ciò riguarda direttamente anche il procurement: le scelte d'acquisto e le clausole contrattuali determinano la sicurezza e la resilienza delle soluzioni IA. Se da un lato, infatti, l'IA sembra poter fornire utili strumenti per rispondere alla crescente necessità di migliorare l'efficienza e l'efficacia nella gestione e nell'erogazione dei servizi pubblici, dall'altro, questa tecnologia introduce nuovi rischi, minacce e vulnerabilità che devono essere presi in considerazione nella sua implementazione.

In considerazione della loro natura inerentemente socio-tecnica – in cui elementi sociali (l'influenza delle dinamiche sociali e l'impatto sulle persone che li usano o che ne sono condizionati) e tecnici (quali dataset, algoritmi, modelli) risultano strettamente intrecciati tra loro – i sistemi di IA sono caratterizzati da specifiche peculiarità nell'ambito della sicurezza in particolare con riferimento ai rischi ai quali sono soggetti e agli attacchi dei quali possono essere vittima.

In questo capitolo sono discusse ed esaminate tali peculiarità: la successiva sezione introduce, ai fini dell'inquadramento del contesto, un modello del ciclo di vita dei sistemi, la seconda e la terza trattano rispettivamente la gestione del rischio e le tassonomie di attacco, l'ultima sezione elenca una serie di obiettivi di sicurezza specifici per l'ambito di applicazione delle presenti linee guida.

Ai fini dell'individuazione dei rischi e degli attacchi associati ai sistemi di intelligenza artificiale, è importante avere una comprensione del loro ciclo di vita.

La sicurezza dei sistemi di intelligenza artificiale deve essere mantenuta lungo tutto il ciclo di vita.

3.6.1 Gestione del rischio in cybersecurity

Come osservato nel paragrafo introduttivo, i sistemi di IA sono sistemi socio-tecnici caratterizzati da specifici rischi la cui gestione rappresenta un elemento imprescindibile per lo sviluppo e l'utilizzo responsabile dell'intelligenza artificiale.

Tale esigenza è chiaramente emersa anche a livello regolamentare unionale. Il Regolamento Europeo sull'Intelligenza Artificiale, cosiddetto AI Act[1], stabilisce infatti regole armonizzate per l'immissione sul mercato UE di sistemi di IA e, sulla base dei possibili rischi e del loro livello d'impatto, requisiti specifici per i sistemi di IA valutati ad alto rischio. In particolare, l'articolo 15 prevede che i sistemi di IA ad alto rischio[2] siano progettati e sviluppati in modo tale da conseguire un adeguato livello di

[1] Regolamento (UE) 2024/1689.

[2] La classificazione dei sistemi di IA ad alto rischio, come specificato dall'articolo 6 dell'AI Act, si basa sullo scopo previsto del sistema di IA. In particolare, fermo restando quanto disposto dal paragrafo 1 della richiamata norma rispetto ai Sistemi IA inseriti all'interno di prodotti o essi stessi prodotti sottoposti ad ulteriore normativa di armonizzazione europea (e.g. regolamento Macchine, regolamento Giocattoli), l'allegato III dell'AI Act individua otto settori di sistemi ad alto rischio: 1) Biometria, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso, 2) infrastrutture critiche, 3)

accuratezza, robustezza e cibersicurezza e operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.

Un'efficace strutturazione di un processo di gestione dei rischi di un sistema di IA deve necessariamente considerare le caratteristiche distintive di tali sistemi. A tale scopo è possibile fare riferimento a framework e standard specializzati, quale, ad esempio, il Risk Management Framework per l'intelligenza artificiale (AI RMF)[3] sviluppato dal National Institute of Standards and Technology (NIST).

Il framework è disegnato per assistere organizzazioni e individui, definiti come AI Actors[4], e fornisce un approccio strutturato per identificare, valutare e mitigare i rischi associati ai sistemi di IA. L'obiettivo è quello di minimizzare i potenziali impatti negativi e massimizzare quelli positivi in modo da avere sistemi di IA affidabili.

Potenziali impatti negativi derivanti dall'uso dei sistemi di IA sono classificati a seconda della tipologia di attore coinvolto:

- *impatti sugli individui*, come ad esempio gli impatti sulle libertà civili, sulla sicurezza fisica/psicologica o sulla sfera economica di un individuo;
- *impatti sulle organizzazioni*, come ad esempio gli impatti sulle attività commerciali, sulla reputazione o derivanti dalla compromissione di un'organizzazione;
- *impatti sull'ecosistema*, come ad esempio gli impatti su elementi e risorse interconnessi e interdipendenti, sul sistema finanziario, sulla catena di approvvigionamento o sulle risorse naturali e l'ambiente.

Il cosiddetto Core del framework individua le seguenti quattro funzioni (a loro volta suddivise in categorie e sottocategorie) per supportare le organizzazioni nella gestione dei rischi posti dai sistemi di IA:

- GOVERN: promuovere una cultura di gestione del rischio all'interno delle organizzazioni che progettano, sviluppano, acquisiscono e adottano sistemi di IA;
- MAP: stabilire il contesto nel quale inquadrare i rischi di un sistema di IA, identificare i rischi e i relativi fattori di rischio;

istruzione e formazione professionale, 4) occupazione, gestione dei lavoratori e accesso al lavoro autonomo, 5) Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi, 6) attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso, 7) Migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso, 8) Amministrazione della giustizia e processi democratici. .

[3] https://www.nist.gov/itl/ai-risk-management-framework.

[4] L'organizzazione per la cooperazione e lo sviluppo economico (OCSE) definisce gli *AI Actors* come coloro i quali svolgono un ruolo attivo nel ciclo di vita dei sistemi di IA, compresi le organizzazioni e gli individui che distribuiscono o gestiscono l'intelligenza artificiale.

- MEASURE: analizzare, valutare, confrontare e monitorare il rischio e i relativi impatti. Utilizza le informazioni acquisite dalla precedente funzione e fornisce indicazioni a quella successiva;
- MANAGE: definire le priorità e ad agire sui rischi identificati. Il trattamento del rischio comprende piani di risposta, recupero e comunicazione di incidenti o eventi.

La funzione GOVERN è trasversale e si applica a tutte le fasi del processo di gestione del rischio. Le funzioni MAP, MEASURE e MANAGE comprendono componenti della funzione GOVERN (in particolare quelle riguardanti la conformità o la valutazione) e possono essere utilizzate in contesti specifici e in determinate fasi del ciclo di vita dei sistemi di intelligenza artificiale.

Per supportare le organizzazioni nell'uso del Framework, il NIST ha sviluppato un playbook[5] allineato a ciascuna sottocategoria delle quattro funzioni.

L'individuazione dei rischi avviene tipicamente a partire dalle minacce cui può essere esposto un sistema e dai suoi asset, sui quali tali minacce tentano di sfruttarne le vulnerabilità.

In ragione di ciò, nei seguenti paragrafi sono elencati, sulla base del modello del ciclo di vita discusso nella precedente sezione, le categorie di asset e minacce relative ai sistemi di intelligenza artificiale.

Asset

Un sistema di IA è costituito da un insieme di asset. Per asset si intende tutto ciò che ha un valore per un individuo o un'organizzazione e che quindi deve essere protetto. In aggiunta agli asset caratteristici dell'IA (come, ad esempio, i modelli e i parametri di configurazione) sono qui considerati anche gli asset dell'infrastruttura ICT (come, ad esempio, le reti di comunicazione e i sistemi operativi).

L'identificazione e la protezione degli asset di un sistema IA non sono soltanto questioni tecniche: riguardano direttamente il processo di approvvigionamento. Le scelte di procurement definiscono quali entrano nell'ecosistema (modelli, dataset, componenti software e hardware), chi ne detiene la responsabilità e con quali garanzie di sicurezza e tracciabilità vengono consegnati. Perciò, i requisiti di sicurezza devono essere tradotti in obblighi contrattuali, criteri di valutazione in gara e condizioni di accettazione per tutti gli asset acquisiti.

Gli asset di un sistema di IA possono essere categorizzati in[6] (tra parentesi è riportata la corrispondente fase del ciclo di vita dell'asset):

- *dati*, come ad esempio: dati grezzi (acquisizione dei dati), dati di valutazione (tuning del modello), dati etichettati (pre-elaborazione dei dati), dati di test (addestramento del modello);

[5] https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook

[6] Per la tassonomia completa si faccia riferimento all'annesso A del documento "AI Cybersecurity Challenges" pubblicato dall'ENISA (European Union Agency for Cybersecurity), https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

- *modelli*, come ad esempio: algoritmi (addestramento del modello), iperparametri (tuning del modello), algoritmi di addestramento (selezione del modello);
- *attori*, come ad esempio: fornitori di servizi cloud (raccolta dei dati, addestramento del modello, tuning del modello), proprietari dei dati (definizione dell'obiettivo, raccolta dei dati, esplorazione dei dati), fornitori dei dati (raccolta dei dati);
- *processi*, come ad esempio: acquisizione dei dati (raccolta dei dati), etichettamento dei dati (pre-elaborazione dei dati), comprensione dei dati (esplorazione e convalida dei dati);
- *strumenti*, come ad esempio: reti di comunicazione (raccolta dei dati), database (raccolta dei dati), sistemi operativi (distribuzione del modello, mantenimento del modello);
- *artefatti*, come ad esempio: politiche di gestione dei dati (raccolta dei dati), architettura del modello (selezione del modello, distribuzione del modello), casi d'uso (comprensione del business).

Minacce

Ogni fase del ciclo di vita è caratterizzata da una o più minacce, che possono essere individuate nelle seguenti categorie[7]:

- *attività malevole/abuso*: azioni intenzionali che prendono di mira sistemi, infrastrutture e reti ICT mediante atti malevoli con l'obiettivo di sottrarre, alterare o distruggere un obiettivo specifico (ad esempio[8] data poisoning e backdoors nel modello);
- *eavesdropping/ intercettazioni/ hijacking*: azioni volte a intercettare, interrompere o prendere il controllo di una comunicazione di terzi senza consenso (ad esempio divulgazione del modello e furto di dati);
- *attacchi fisici*: azioni che mirano a distruggere, esporre, alterare, disattivare, rubare o ottenere un accesso non autorizzato a risorse fisiche come infrastrutture, hardware o interconnessioni consenso (ad esempio sabotaggio del modello e DDoS);
- *danno non intenzionale*: azioni non intenzionali che causano distruzione, danni a proprietà o persone e che si traducono in un guasto o in una riduzione dell'utilità (ad esempio riduzione dell'accuratezza dei dati e compromissione della selezione delle caratteristiche);
- *guasti o malfunzionamenti*: funzionamento parziale o totalmente insufficiente di un asset hardware o software (ad esempio scarsità di dati e degradazione delle performance del modello);

[7] Negli annessi B e D del documento "AI Cybersecurity Challenges" di ENISA sono riportati, rispettivamente, la tassonomia completa delle minacce e la mappatura con le fasi del ciclo di vita. Per ogni categoria di minacce sono altresì individuati le specifiche minacce, le dimensioni di sicurezza potenzialmente impattate e gli asset impattati.

[8] Il paragrafo "Tassonomie di attacco" tratta le varie categorie di attacchi associati a questo tipo di minacce.

- *interruzioni*: interruzioni impreviste del servizio o diminuzione della qualità al di sotto di un livello richiesto (ad esempio interruzione dell'infrastruttura/sistemi, interruzione delle reti di telecomunicazione);

- *disastro*: incidente improvviso o catastrofe naturale che causa ingenti danni (ad esempio disastri naturali e fenomeni di cambiamento climatico);

- *legale*: azioni legali di terzi (ad esempio a causa di divulgazione di informazioni personali e profilazione degli utenti).

Oltre alle categorie di minaccia sopra elencate, va richiamata l'attenzione su rischi specifici relativi agli agenti IA. Gli agenti ampliano la superficie d'attacco perché combinano capacità decisionali, persistenza di stato e privilegi operativi; per questo motivo possono essere soggetti a tipologie di compromissione non pienamente coperti dalle tassonomie tradizionali.

Tra gli esempi più significativi si segnalano:

- *Escalation di privilegi* e *movimento laterale*: se un agente viene compromesso può utilizzare credenziali o API per propagarsi all'interno dell'infrastruttura.

- *Prompt injection* e *manipolazione delle istruzioni*: input malevoli o manipolazioni possono indurre l'agente a cambiare comportamento e compiere azioni non previste (per esempio divulgare informazioni o eseguire comandi non autorizzati).

- *Persistenza* e *backdoor comportamentali*: l'agente può conservare nello "stato" informazioni o istruzioni corrotte che, in momenti successivi, attivano comportamenti dannosi o difficili da rilevare.

- *Collusione* e *comportamenti emergenti*: quando più agenti interagiscono, possono coordinarsi - volontariamente o perché manipolati - per realizzare azioni dannose o sviluppare comportamenti inaspettati e non desiderati.

- *Esfiltrazione* e *abuse of capabilities*: un agente che ha accesso a dati sensibili o a canali esterni può trasferire informazioni fuori dall'organizzazione o usarle impropriamente.

- *Uso improprio di risorse*: un agente può consumare in modo eccessivo risorse di calcolo o di rete per scopi malevoli (per esempio attacchi DDoS o criptomining), degradando le prestazioni o causando interruzioni.

3.6.2 Tassonomie di attacco

In aggiunta ai tradizionali attacchi cyber[9] all'infrastruttura ICT ospitante, i sistemi di intelligenza artificiale sono soggetti ad attacchi a componenti specifiche dell'IA quali, ad esempio, i modelli e i dati di addestramento. La conoscenza delle varie tassonomie di attacco permette di porre in essere azioni di protezione e contenimento mirate e contestualizzate.

Come tassonomia di riferimento per gli attacchi ai sistemi di IA può essere usata quella sviluppata dal NIST[10] che prevede le seguenti macro-categorie di attacchi:

- *evasion attacks*;
- *poisoning attacks*;
- *privacy attacks*;
- *abuse attacks*;

Le prime tre categorie riguardano sia i modelli di IA predittiva che quelli di IA generativa, mentre l'ultima riguarda soprattutto i modelli di IA generativa.

Nei successivi paragrafi sono discussi brevemente queste categorie e possibili strategie di mitigazione.

Evasion attacks

Questa categoria di attacchi mira a indurre errori di classificazione introducendo perturbazioni negli input del modello. Tali perturbazioni, spesso impercettibili per l'occhio umano, vengono denominate *adversarial examples* (esempi avversari).

Gli attacchi di questo tipo sfruttano le vulnerabilità nel processo decisionale del modello e possono indurlo a prevedere un valore scelto dall'attaccante o, più in generale, a ridurne l'accuratezza.

Tra le principali strategie di mitigazione rientrano: l'*adversarial training*, ossia il riaddestramento del modello includendo *adversarial examples* etichettati correttamente, tecniche come il *randomized smoothing* e il *formal verification*, con i quali si cerca di rendere invariante il modello più robusto rispetto alle perturbazioni avversarie garantendone una maggiore affidabilità.

Poisoning attacks

[9] Attacchi nei quali l'attore malevolo fa uso di TTP (tattiche, tecniche e procedure che caratterizzano il comportamento di un attaccante per raggiungere il proprio obiettivo) tipiche del dominio cyber .

[10] Adversarial Machine Learning - A Taxonomy and Terminology of Attacks and Mitigations: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

Questa categoria di attacchi ha come obiettivo degradare le prestazioni di un modello o fargli generare uno specifico risultato alterando (avvelenando) i dati di addestramento del modello. Un esempio è il cosiddetto *label flipping*, in cui l'attaccante cambia l'etichetta dei dati di addestramento con l'obiettivo di addestrare il modello sulla base dell'etichetta da lui scelta[11] per spingerlo ad apprendere associazioni errate.

Questi attacchi possono essere distinti in:

- *availability poisoning*: determinano una violazione della disponibilità del modello tramite una degradazione delle sue prestazioni su tutti i sample di dati. Sono rilevabili monitorando le prestazioni del modello, possibili strategie di mitigazione prevedono la sanitizzazione dei dati di addestramento e l'apprendimento robusto (possono, ad esempio, essere addestrati molteplici modelli);

- *targeted poisoning*: determinano una violazione dell'integrità del modello alterandone la previsione su un numero ridotto di sample mirati. Possibili strategie di mitigazione prevedono l'implementazione di controlli di sicurezza sull'origine e sull'integrità dei dati;

- *backdoor poisoning*: analogamente agli attacchi targeted poisoning determinano una violazione dell'integrità del modello, in questo caso l'obiettivo è quello di indurre in errore il modello in risposta a uno specifico sample di dati (denominato trigger). Possibili strategie di mitigazione prevedono la sanitizzazione dei dati di addestramento, la ricostruzione del trigger, l'ispezione e la sanitizzazione del modello;

- *model poisoning*: modificano direttamente il modello addestrato iniettandovi funzionalità malevole. Possono determinare una violazione sia dell'integrità che della disponibilità e avvengono generalmente nell'ambito del cosiddetto apprendimento federato (federated learning) in cui sistemi client inviano aggiornamenti locali del modello a un server centrale che li aggrega in un modello globale. Sono inoltre possibili in scenari di supply chain quando vengono acquisiti modelli o relativi componenti che sono stati già avvelenati. Possibili strategie di mitigazione prevedono l'individuazione ed esclusione degli aggiornamenti malevoli o (nel caso di avvelenamenti del modello tramite backdoor) l'ispezione e la sanitizzazione del modello.

Privacy attacks

Questa categoria di attacchi ha come obiettivo compromettere le informazioni degli utenti ricostruendole a partire dai dati di addestramento. Possono essere distinti in:

- *data reconstruction*, ricostruiscono le informazioni a partire dalle informazioni aggregate;

[11] Ad esempio, nell'ambito dell'addestramento di un filtro anti-spam della posta elettronica, un avversario potrebbe cambiare le etichette dei dati di training da *spam* a *no-spam*, per indurre il modello addestrato a non filtrare correttamente i messaggi di posta elettronica che contengono spam.

- *membership inference*, determinano se un particolare record è stato incluso nel dataset utilizzato per l'addestramento di un modello, compromettendo le informazioni dell'utente;
- *model extraction*, ottengono informazioni sul modello, come ad esempio la sua architettura o i suoi parametri.
- *property inference*, accedono a informazioni globali sulla distribuzione dei dati di addestramento interagendo con il modello.

Per la mitigazione degli attacchi di ricostruzione è stato proposto l'uso di tecniche di protezione dei dati personali come la privacy differenziale, che - attraverso manipolazioni controllate dei dati – permette di fissare un limite su quanto un attaccante, con accesso ai risultati dell'algoritmo, può inferire su ogni singolo record del dataset.

Altre possibili strategie di mitigazione prevedono la limitazione del numero di interrogazioni dell'utente e il rilevamento delle interrogazioni sospette al modello.

Abuse attacks

Questa categoria di attacchi mira ad alterare il comportamento di un sistema di IA generativa per adattarlo ai propri scopi come, ad esempio, perpetrare frodi, distribuire malware e manipolare informazioni.

Le possibili strategie di mitigazione prevedono l'uso di metodi come l'apprendimento rinforzato con feedback umano, il filtraggio degli input o il rilevamento di valori anomali di output (outliers).

3.6.3 Obiettivi di sicurezza

In questa sezione sono enunciati gli obiettivi di sicurezza che devono guidare il procurement di intelligenza artificiale nella pubblica amministrazione.

In quest'ambito, può essere utile far riferimento al Procurement of AI Community[12] – gruppo costituito nell'ambito del Public Buyers Community[13] della Commissione Europea per supportare le organizzazioni pubbliche nell'acquisizione di sistemi di IA che siano affidabili, eque e sicure – le cui considerazioni sono state prese in esame nella formulazione dei contenuti del presente paragrafo.

Le raccomandazioni fornite per il raggiungimento dei già citati obiettivi sono da intendersi come pratiche di base, le cui implicazioni devono essere comprese e valutate attentamente in fase di realizzazione. Resta in capo a ciascuna amministrazione la valutazione, in esito alla differente

[12] https://public-buyers-community.ec.europa.eu/communities/procurement-ai.

[13] Piattaforma della Commissione Europea progettata per facilitare la cooperazione e la condivisione delle conoscenze tra gli acquirenti pubblici in Europa.

esposizione alle minacce e alla propria analisi del rischio, in merito all'individuazione e conseguente raggiungimento di ulteriori obiettivi di sicurezza per il rafforzamento della sicurezza cibernetica dei propri sistemi di intelligenza artificiale.

Requisiti di sicurezza per l'acquisizione

Nella stesura dei contratti, quando si definiscono i requisiti della sicurezza, si suggerisce alle amministrazioni di indirizzare i seguenti ambiti:

- *verifica delle clausole di sicurezza contrattuali*: verificare attentamente le clausole di sicurezza incluse nei disciplinari di gara assicurandosi che definiscano chiaramente le responsabilità, richiedano misure di sicurezza adeguate e garantiscano la conformità alle normative vigenti. È importante includere audit regolari per monitorare l'efficacia delle misure adottate, promuovendo così un approccio proattivo alla gestione dei rischi.

- *sistema di gestione dei rischi*: richiedere che il fornitore, prima della consegna del sistema di IA, istituisca, attui, documenta e mantenga un sistema di gestione dei rischi in relazione al sistema di IA fornito;

- *dati e relativa governance*[14]: richiedere che i dataset utilizzati nello sviluppo del sistema di IA (addestramento, validazione e test), siano soggetti a politiche dei dati adeguate al contesto di utilizzo e alle finalità previste dal sistema di IA;

- *documentazione tecnica e istruzioni per l'uso*: richiedere che i dataset utilizzati nello sviluppo del sistema di IA siano pertinenti, rappresentativi e, nella misura del possibile, privi di errori e che siano fornite documentazione tecnica e istruzioni chiare per l'uso;

- *conservazione dei log*: richiedere che il fornitore sviluppi il sistema di IA con capacità che consentano la registrazione automatica degli eventi (log) per la durata del ciclo di vista del sistema di IA, per garantire tracciabilità e verificabilità tramite audit;

- *trasparenza*: richiedere che il sistema di IA sia progettato e sviluppato in modo tale che il funzionamento sia sufficientemente trasparente da consentire all'organizzazione pubblica di interpretarne l'output e utilizzarlo adeguatamente;

- *supervisione umana*: prevedere che il sistema di IA sia progettato e sviluppato in modo tale, anche con adeguati strumenti di interfaccia uomo-macchina, da poter essere efficacemente supervisionato dalle persone fisiche durante il periodo in cui è in uso;

- *accuratezza, robustezza e cybersecurity*: prevedere che il sistema di IA sia progettato e sviluppato in modo tale da raggiungere un adeguato livello di accuratezza, robustezza, sicurezza e cibersicurezza e da operare in modo coerente sotto tali aspetti.

[14] Tale requisito è valido qualora i sistemi di IA acquisiti utilizzino tecniche che prevedono l'addestramento di modelli con dati.

- *lista delle operazioni autorizzate*: richiedere un elenco esaustivo delle azioni e delle risorse (API, permessi, canali esterni) che l'agente è autorizzato a utilizzare; l'agente non potrà eseguire operazioni non esplicitamente previste e autorizzate.

- *controllo di emergenza e ripristino*: prevedere la disponibilità di un controllo che consenta all'Amministrazione di sospendere o disabilitare temporaneamente l'agente in caso di comportamento anomalo, nonché di procedure documentate per il rapido ripristino.

Obblighi di sicurezza per i fornitori

Si suggerisce di prevedere, tra gli obblighi di sicurezza per i fornitori di sistemi di IA, quanto segue:

- *conformità*: garantire che il sistema di IA sia conforme ai requisiti indicati;

- *sistemi di gestione della qualità*: istituire un sistema di gestione della qualità che garantisca la conformità ai presenti requisiti;

- *valutazione della conformità*: garantire che il sistema di IA sia conforme a procedure di valutazione della conformità prima della consegna dello stesso;

- *misure correttive*: adottare tempestivamente misure correttive (con contestuale informazione all'organizzazione) per rendere conforme il sistema qualora il fornitore ritenga o abbia motivo di ritenere che il sistema di IA non sia conforme;

- *spiegazione del processo decisionale del sistema*: fornire spiegazioni comprensibili agli utenti su come il sistema giunga a una determinata decisione o risultato e quali modifiche è necessario apportare agli input per giungere a un diverso esito;

- *audit*: collaborare pienamente agli audit e alle ispezioni effettuate dall'organizzazione al fine di valutare l'adempimento del fornitore agli obblighi stabiliti.

Diritti di utilizzo dei dataset

Devono essere normati i diritti di utilizzo per i dataset, impiegati nella realizzazione dei sistemi di IA acquisiti da fornitori, per almeno i seguenti ambiti:

- *diritti di utilizzo dei dataset dell'amministrazione*: normare i diritti di utilizzo da parte del fornitore e di eventuali terzi sui dataset dell'organizzazione;

- *diritti di utilizzo dei dataset del fornitore e di terzi*: normare i diritti di utilizzo da parte dell'amministrazione sui dataset messi a disposizione dal fornitore e da eventuali terzi;

- *consegna dei dataset*: prevedere che il fornitore consegni, su richiesta dell'organizzazione, i dataset impiegati nella realizzazione del sistema di IA.

Condurre audit per la verifica dei requisiti e degli obblighi di sicurezza

In accordo all'analisi del rischio, devono essere previsti audit per la verifica dei requisiti di sicurezza dei sistemi di IA acquisiti da fornitori e degli obblighi dei fornitori di sistemi di AI.

3.7 Buone pratiche per il procurement lungo il ciclo di vita del contratto

Il procurement di sistemi di Intelligenza Artificiale richiede l'adozione di buone pratiche specifiche e coerenti con le peculiarità tecnologiche, organizzative ed economiche di tali sistemi. A differenza delle forniture tradizionali, i sistemi di IA presentano un'elevata dinamicità, una forte dipendenza dai dati e un impatto potenzialmente significativo sui procedimenti amministrativi e sull'esercizio della funzione pubblica. Per tali ragioni, le buone pratiche devono essere declinate lungo l'intero ciclo di vita del contratto, in coerenza con le fasi previste dal Codice dei contratti pubblici.

L'adozione di un approccio strutturato e consapevole consente alle Pubbliche Amministrazioni di ridurre i rischi, rafforzare il controllo pubblico e garantire che l'utilizzo dell'IA sia effettivamente funzionale al perseguimento dell'interesse generale.

Programmazione

Nella fase di programmazione, una buona pratica fondamentale consiste nel mantenere la centralità del fabbisogno pubblico, evitando approcci meramente technology-driven senza analisi dei processi. L'amministrazione dovrebbe interrogarsi preliminarmente sulle finalità perseguite, sulle criticità dei processi esistenti e sulle reali opportunità offerte dall'adozione di sistemi di IA, valutando se tali soluzioni siano coerenti con il fabbisogno ed effettivamente idonee a generare valore pubblico.

È buona pratica condurre una valutazione preliminare dei rischi tecnologici, organizzativi ed economici associati all'adozione dell'IA, nonché della sostenibilità dell'investimento nel medio-lungo periodo. In tale fase, è opportuno considerare il livello di maturità delle soluzioni disponibili sul mercato, la disponibilità e qualità dei dati necessari e la capacità dell'amministrazione di governare il sistema una volta acquisito.

La programmazione dovrebbe inoltre tenere conto delle opportunità di riuso, cooperazione inter-istituzionale e utilizzo di strumenti di procurement aggregato, al fine di ridurre duplicazioni e favorire economie di scala.

Progettazione

Nella fase di progettazione, le amministrazioni sono chiamate a tradurre il fabbisogno individuato in requisiti sostenibili, chiari e coerenti con le caratteristiche dei sistemi di IA. Una buona pratica consiste nel definire il fabbisogno in termini funzionali e di risultato, evitando specifiche tecnologiche eccessivamente rigide che possano limitare l'innovazione o favorire soluzioni proprietarie.

È essenziale chiarire, già in questa fase, le funzioni di governo del sistema che devono rimanere nella disponibilità dell'amministrazione, con particolare riferimento all'architettura logica, alla gestione dei dati e alle modalità di controllo. Le scelte progettuali dovrebbero favorire architetture modulari e governabili, coerenti con il principio di proporzionalità e con il livello di rischio associato al contesto applicativo.

La progettazione rappresenta inoltre il momento in cui definire i principali presidi di governance, inclusi i meccanismi di monitoraggio delle prestazioni, le modalità di gestione delle evoluzioni del sistema e le condizioni di uscita o transizione dal contratto. In tale prospettiva, le amministrazioni adottando una logica "di cantiere", dovrebbero prevedere assetti progettuali capaci di adattarsi progressivamente all'evoluzione tecnologica, di integrare componenti eterogenee e di supportare una pluralità di modelli, strumenti e pipeline dati. Questo, allo scopo di presidiare i rischi di lock-in architetturale, requisiti incompleti, eccessiva dipendenza dal fornitore.

Affidamento

Durante la fase di affidamento, le amministrazioni sono chiamate a privilegiare il criterio dell'offerta economicamente più vantaggiosa, valorizzando la qualità complessiva della soluzione, la sostenibilità del ciclo di vita e la capacità evolutiva del sistema, in coerenza con quanto previsto dal Codice dei contratti pubblici e con i principi di valutazione comparativa delle soluzioni ICT di cui all'articolo 68 del Codice dell'amministrazione digitale.

I criteri di aggiudicazione dovrebbero includere elementi relativi alla qualità architetturale, alla gestione dei dati, alla governabilità del sistema e alle misure proposte per ridurre i rischi di lock-in tecnologico ed economico. È opportuno valorizzare, nell'ambito dell'offerta tecnica, la chiarezza della proposta architetturale e la capacità del fornitore di supportare l'amministrazione lungo l'intero ciclo di vita del

sistema. Un ulteriore parametro da considerare in fase di affidamento è la sostenibilità ambientale e l'efficienza energetica dei sistemi di IA nel loro complesso (sia a livello infrastrutturale che di sistema).

Una buona pratica consiste inoltre nel prevedere, già in fase di gara, strumenti di verifica e monitoraggio delle prestazioni che possano essere utilizzati in modo continuativo durante l'esecuzione del contratto. I rischi da presidiare sono relativi all'eccessiva enfasi sul prezzo più basso; valutazioni tecniche insufficienti; scarsa comparabilità delle offerte.

Stipula

La fase di stipula del contratto rappresenta un momento cruciale per tradurre le scelte progettuali e di gara in obblighi giuridicamente vincolanti. È buona pratica assicurare che il contratto disciplini in modo puntuale i profili relativi alla gestione dei dati, alla documentazione del sistema, alle modalità di aggiornamento e alle condizioni di revisione del servizio.

Il contratto dovrebbe prevedere clausole che garantiscano la continuità operativa e piani di fallback, la portabilità dei dati e delle componenti e la possibilità per l'amministrazione di intervenire sul sistema in caso di criticità. La chiarezza contrattuale rappresenta un elemento essenziale per prevenire contenziosi e per rafforzare la capacità della PA di governare il rapporto con il fornitore.

In tal senso, è opportuno prevedere clausole contrattuali di adeguamento normativo al fine di disciplinare in modo esplicito la ripartizione degli oneri derivanti da modifiche del quadro regolatorio applicabile ai sistemi di IA. A tal fine può essere utile distinguere tra adeguamenti di natura ordinaria — riconducibili all'evoluzione prevedibile delle normative di settore o agli aggiornamenti periodici richiesti dalla disciplina vigente — e adeguamenti di natura straordinaria derivanti da interventi normativi che comportino modifiche sostanziali al funzionamento del sistema o ai requisiti tecnici della soluzione. Ciò, allo scopo di presidiari rischi connessi ad ambiguità contrattuali, limitata accessibilità alle informazioni, difficoltà di subentro.

Nei casi di adeguamento straordinario, il contratto dovrebbe prevedere meccanismi di revisione o riequilibrio delle condizioni economiche, al fine di garantire la sostenibilità della prestazione e la continuità del servizio.

Può risultare inoltre utile distinguere tra aggiornamenti di natura documentale o procedurale — quali l'aggiornamento della documentazione tecnica, delle informative o delle policy di utilizzo — e aggiornamenti di natura funzionale che comportino modifiche al sistema, ai modelli o alle componenti tecnologiche della soluzione.

Esecuzione

Durante la fase di esecuzione del contratto, il ruolo dell'amministrazione non può limitarsi alla verifica formale dell'adempimento contrattuale, ma deve tradursi in un presidio continuo sul funzionamento del sistema di IA. Una buona pratica consiste nel monitorare in modo sistematico le prestazioni del sistema, la qualità degli output e l'adeguatezza delle soluzioni adottate rispetto agli obiettivi iniziali.

L'esecuzione rappresenta inoltre il momento in cui verificare la sostenibilità economica e organizzativa del sistema, valutando eventuali scostamenti rispetto alle ipotesi formulate in fase di affidamento. In tale contesto, è opportuno rafforzare le competenze interne dell'amministrazione e documentare le esperienze maturate, anche al fine di supportare future iniziative di procurement.

Infine, è buona pratica pianificare sin dall'inizio le modalità di eventuale transizione o dismissione del sistema, assicurando la restituzione e la portabilità dei dati e la continuità dell'azione amministrativa.

Tabella 5 Buone pratiche per il procurement di sistemi di IA lungo il ciclo di vita del contratto

Fase del ciclo di procurement	Obiettivi prioritari	Buone pratiche operative	Rischi da presidiare
Programmazione	Garantire coerenza tra fabbisogno pubblico e soluzione tecnologica	Analizzare criticità dei processi esistenti e prevederne la reingegnerizzazione; valutare maturità delle soluzioni; verificare disponibilità e qualità dei dati; considerare opportunità di riuso e cooperazione	Adozione di soluzioni *technology-driven* senza analisi dei processi; sottostima dei costi di ciclo di vita; scarsa consapevolezza dei requisiti organizzativi
Progettazione	Tradurre il fabbisogno in requisiti governabili e sostenibili	Definire requisiti funzionali; evitare specifiche tecnologiche rigide; favorire	Lock-in architetturale; requisiti incompleti;

Fase del ciclo di procurement	Obiettivi prioritari	Buone pratiche operative	Rischi da presidiare
		architetture modulari; chiarire le funzioni di governo del sistema; progettare i presidi di monitoraggio	eccessiva dipendenza dal fornitore
Affidamento	Selezionare la soluzione più sostenibile nel medio-lungo periodo	Ricorrere all'Offerta Economicamente più vantaggiosa; valorizzare qualità architetturale e sostenibilità; includere criteri sulla gestione dei dati e sulla governabilità; prevedere strumenti di verifica delle prestazioni	Eccessiva enfasi sul prezzo più basso; valutazioni tecniche insufficienti; scarsa comparabilità delle offerte
Stipula	Rafforzare la capacità di governo contrattuale dell'amministrazione	Disciplinare gestione dei dati; prevedere clausole di aggiornamento; garantire portabilità; definire condizioni di revisione e continuità operativa anche con piani di fallback	Ambiguità contrattuali; limitata accessibilità alle informazioni; difficoltà di subentro

3.8 Gestione del rischio

Il procurement di sistemi di Intelligenza Artificiale comporta l'esposizione delle Pubbliche Amministrazioni a un insieme articolato di rischi che, per natura e intensità, differiscono da quelli tipicamente associati alle forniture ICT tradizionali. Tali rischi non si esauriscono in profili meramente tecnologici, ma includono dimensioni organizzative, giuridiche, economiche e reputazionali che incidono direttamente sulla capacità dell'amministrazione di esercitare le proprie funzioni istituzionali.

Una gestione consapevole del rischio rappresenta pertanto un elemento qualificante del procurement di sistemi di IA e deve essere integrata in modo sistematico lungo l'intero ciclo di vita del contratto, in coerenza con le fasi previste dal Codice dei contratti pubblici. L'obiettivo è di rendere il rischio conoscibile, governabile e proporzionato rispetto ai benefici attesi dall'adozione della soluzione tecnologica.

Un primo ambito di rischio riguarda i **profili tecnologici**, connessi alla complessità, all'evolutività e alla parziale imprevedibilità del comportamento dei sistemi di IA. In particolare, l'utilizzo di modelli adattivi o generativi può determinare scarsa spiegabilità dei modelli o variazioni nel tempo delle prestazioni del sistema, rendendo più complessa la verifica ex ante e il monitoraggio ex post dei risultati. Le amministrazioni devono pertanto considerare il rischio di scostamento tra prestazioni attese e prestazioni effettive, mitigabile ad esempio attraverso il ricorso ad un'architettura modulare, e prevedere meccanismi di controllo e di intervento adeguati, anche sulla base di audit periodici.

Accanto ai rischi tecnologici, assumono rilievo i **rischi organizzativi**, legati alla capacità dell'amministrazione di integrare il sistema di IA nei propri processi (anche reingegnerizzandoli) e di gestirne l'impatto sull'organizzazione del lavoro. L'introduzione di sistemi di IA può modificare flussi procedimentali, ruoli e responsabilità, richiedendo adattamenti che, se non adeguatamente governati, possono compromettere l'efficacia e l'efficienza dell'azione amministrativa. Il procurement deve pertanto tenere conto della capacità organizzativa dell'ente e prevedere misure di accompagnamento, formazione e supporto.

Un ulteriore profilo di rischio riguarda gli **aspetti giuridici e di conformità normativa**, in particolare con riferimento alla protezione dei dati personali, alla trasparenza dell'azione amministrativa e alla legittimità dei procedimenti supportati dall'IA. L'utilizzo di sistemi poco spiegabili o scarsamente documentati può esporre l'amministrazione a contenziosi, contestazioni e danni reputazionali. In tale contesto, la gestione del rischio richiede un attento coordinamento tra le scelte di procurement, le clausole contrattuali e i presìdi di controllo interno.

Particolarmente rilevante è inoltre il **rischio economico**, connesso alla sostenibilità dei costi nel medio-lungo periodo e alla possibilità di incorrere in situazioni di lock-in tecnologico ed economico. Tali dinamiche risultano particolarmente evidenti nelle scelte tra modelli di deployment on-premises, soluzioni cloud e servizi basati su metriche di consumo — ad esempio modelli tariffari per token o per richiesta — che, pur riducendo talvolta i costi iniziali, possono esporre l'amministrazione a una

minore prevedibilità della spesa. Soluzioni apparentemente vantaggiose in fase di affidamento possono generare costi crescenti nel tempo, legati a servizi accessori, aggiornamenti obbligati o limitata contendibilità del mercato. La gestione del rischio economico richiede pertanto una valutazione di ciclo di vita del sistema e una particolare attenzione alle scelte architetturali e contrattuali.

Il rischio di **dipendenza dal fornitore** assume una rilevanza specifica nel procurement di sistemi di IA, soprattutto quando il sistema è basato su componenti proprietarie, orchestratori non sostituibili o servizi erogati in modalità esclusiva. Tale rischio può limitare la capacità dell'amministrazione di modificare o sostituire la soluzione nel tempo e compromettere la continuità dell'azione amministrativa. Le amministrazioni sono pertanto chiamate a valutare preventivamente tali profili e a prevedere misure di mitigazione, quali clausole di portabilità, obblighi di documentazione e condizioni di uscita.

La gestione del rischio deve essere integrata in modo coerente nelle diverse fasi del ciclo di procurement. In fase di **programmazione**, è buona pratica effettuare una valutazione preliminare dei principali rischi associati all'adozione del sistema di IA, in relazione al contesto applicativo e al livello di impatto sui procedimenti amministrativi. In fase di **progettazione**, tali valutazioni devono tradursi in scelte architetturali e requisiti di gara idonei a mitigare i rischi individuati.

Durante la fase di **affidamento**, la gestione del rischio può essere supportata dalla definizione di criteri di aggiudicazione che valorizzino la qualità, la governabilità e la sostenibilità della soluzione proposta, nonché dalla richiesta di piani di gestione del rischio da parte dei concorrenti. In fase di **stipula**, le misure di mitigazione devono essere formalizzate in clausole contrattuali chiare e vincolanti.

Infine, nella fase di **esecuzione del contratto**, la gestione del rischio assume un carattere dinamico e continuo. Le amministrazioni devono monitorare l'evoluzione del sistema, verificare l'efficacia delle misure adottate e intervenire tempestivamente in caso di criticità. Il monitoraggio in esecuzione rappresenta uno strumento essenziale per mantenere il rischio entro livelli accettabili e per garantire la coerenza tra gli obiettivi iniziali e i risultati effettivamente conseguiti.

In conclusione, la gestione del rischio nel procurement di sistemi di Intelligenza Artificiale non può essere relegata a un adempimento formale, ma deve costituire una componente strutturale delle scelte di procurement. Un approccio sistematico e proporzionato alla gestione del rischio consente alle

Pubbliche Amministrazioni di sfruttare le opportunità offerte dall'IA riducendo al contempo le potenziali criticità e rafforzando la tutela dell'interesse pubblico.

Tabella 6 : Principali rischi nel procurement di IA e misure di mitigazione

Tipologia di rischio	Descrizione	Possibili misure di mitigazione
Tecnologico	Scarsa spiegabilità dei modelli, prestazioni variabili	Architettura modulare, audit periodici
Economico	Crescita dei costi nel tempo	Valutazione del ciclo di vita
Lock-in	Dipendenza dal fornitore	Clausole di portabilità e uscita
Organizzativo	Carenza di competenze	Formazione e trasferimento di conoscenze

4. Metriche, costi, monitoraggio e gestione del contratto

4.1 Finalità e ambito del capitolo

Il presente Capitolo disciplina gli aspetti relativi alla valutazione economica, alla sostenibilità finanziaria e alla comparabilità delle scelte di procurement dei sistemi di Intelligenza Artificiale da parte delle Pubbliche Amministrazioni. In un contesto tecnologico caratterizzato da rapida evoluzione, da modelli di servizio basati sul consumo e da architetture sempre più articolate, la dimensione economica del procurement assume un rilievo strategico, incidendo direttamente sulla capacità dell'amministrazione di programmare gli investimenti, governare i contratti e garantire la continuità dei servizi nel tempo.

L'obiettivo del Capitolo è fornire un quadro metodologico che consenta alle amministrazioni di superare approcci meramente contabili o limitati al breve periodo, adottando una prospettiva di analisi di ciclo di vita coerente con la complessità tecnica, organizzativa ed economica dei sistemi di IA. Tale prospettiva risulta particolarmente necessaria in presenza di soluzioni caratterizzate da costi variabili, da strutture tariffarie dinamiche e da una forte dipendenza dall'evoluzione tecnologica del mercato.

La valutazione economica dei sistemi di IA non può essere ridotta alla sola determinazione della spesa iniziale né alla verifica della copertura finanziaria dell'intervento. Essa deve configurarsi come un

processo continuo che accompagna l'intero ciclo di procurement — dalla programmazione fino alla fase di esecuzione — integrando considerazioni economiche con valutazioni relative al rischio, alla sostenibilità organizzativa e alla capacità di governo del sistema.

In tale prospettiva, il Capitolo mira a rafforzare la capacità delle amministrazioni di effettuare confronti attendibili tra soluzioni alternative, evitando che le decisioni di procurement siano influenzate da metriche parziali o da modelli di costo difficilmente comparabili. La comparabilità rappresenta infatti una condizione essenziale per garantire il rispetto dei principi di economicità, efficacia e buon andamento dell'azione amministrativa.

Le indicazioni contenute nel presente Capitolo devono essere interpretate in coerenza con il quadro normativo vigente in materia di contratti pubblici e con i principi che regolano la gestione delle risorse finanziarie pubbliche. Esse sono finalizzate a supportare le amministrazioni nella costruzione di basi d'asta realistiche, nella definizione di criteri di aggiudicazione coerenti con il valore complessivo delle soluzioni e nella predisposizione di strumenti di monitoraggio economico efficaci durante l'esecuzione del contratto.

Il presente Capitolo fornisce pertanto un quadro metodologico per l'adozione di pratiche di valutazione economica avanzate, lasciando alle singole amministrazioni la flessibilità necessaria per adattarle o modificarle in funzione delle proprie specificità organizzative e operative. L'obiettivo non è prescrivere modelli univoci, ma offrire strumenti interpretativi che consentano alle amministrazioni di affrontare con maggiore consapevolezza le sfide economiche connesse al procurement dei sistemi di IA.

Il Capitolo si applica a tutte le tipologie di sistemi di IA oggetto di acquisizione, inclusi, a titolo esemplificativo e non esaustivo:

- sistemi basati su modelli di linguaggio di grandi dimensioni (LLM);
- sistemi di IA tradizionale;
- soluzioni di machine learning supervisionato e non supervisionato;
- sistemi di IA agentica e non agentica.

Le indicazioni trovano applicazione indipendentemente dal modello di deployment adottato — servizi API, soluzioni cloud, infrastrutture on-premises o configurazioni ibride — e risultano particolarmente rilevanti nei casi in cui il costo del servizio sia legato ai livelli di utilizzo o a parametri di consumo.
Il presente Capitolo si pone inoltre in continuità con le indicazioni del Capitolo 2, sviluppandone le implicazioni economiche e contrattuali. Se il Capitolo precedente ha posto l'accento sulla governabilità dei sistemi e sulla gestione del rischio, il presente Capitolo mira a fornire alle amministrazioni gli strumenti per tradurre tali principi in scelte economicamente sostenibili e coerenti con la responsabilità di gestione delle risorse pubbliche.

4.2 Limiti degli approcci economici tradizionali

Le pratiche correnti di valutazione economica dei sistemi di Intelligenza Artificiale si fondano spesso su indicatori parziali, quali il costo per token, il costo per chiamata API, la fatturazione per ora di calcolo o, in alcuni casi, il Total Cost of Ownership (TCO). Tali indicatori, pur risultando utili per specifiche finalità di rendicontazione o controllo della spesa, non sono generalmente sufficienti a rappresentare in modo completo e comparabile l'impatto economico dei sistemi di IA.
La crescente diffusione di modelli di servizio basati sul consumo rende infatti la struttura dei costi meno prevedibile rispetto alle forniture ICT tradizionali. Il rischio principale consiste nell'assumere decisioni di procurement sulla base di metriche che riflettono solo una parte dei costi effettivi, trascurando componenti essenziali quali l'integrazione nei sistemi esistenti, la gestione dei dati, le attività di orchestrazione, i presìdi di sicurezza e gli obblighi di conformità normativa.
I costi unitari per token o per inferenza rappresentano indicatori immediati e facilmente comunicabili, ma non includono gli investimenti necessari per rendere il sistema effettivamente operativo nel contesto amministrativo. Essi tendono a misurare il consumo tecnologico piuttosto che il valore del servizio erogato, con il rischio di orientare le decisioni verso soluzioni apparentemente economiche ma strutturalmente onerose.
Analogamente, la fatturazione per ora di calcolo riflette il consumo di risorse infrastrutturali senza considerare adeguatamente i costi di progettazione, gestione operativa e governo del sistema. Una valutazione fondata esclusivamente su tali parametri può esporre l'amministrazione a dinamiche di spesa difficilmente prevedibili, soprattutto in presenza di variazioni nei volumi di utilizzo.

Il ricorso al *Total Cost of Ownership* rappresenta un approccio teso a considerare l'insieme dei costi associati a una soluzione tecnologica, ma presenta limiti significativi nel contesto dei sistemi di IA. In assenza di criteri standardizzati per la normalizzazione dei costi rispetto all'output prodotto, il TCO può risultare poco efficace ai fini della comparazione tra soluzioni alternative. Inoltre, esso non sempre consente di rappresentare adeguatamente la distribuzione temporale degli investimenti, elemento particolarmente rilevante per sistemi caratterizzati da forte variabilità della domanda.

Un'ulteriore criticità deriva dalla tendenza a considerare separatamente le componenti di costo, senza coglierne le interdipendenze. Nei sistemi di IA, le scelte architetturali, le modalità di gestione dei dati e il modello di deployment incidono simultaneamente su più voci di spesa, rendendo necessaria una valutazione integrata.

Alla luce di tali considerazioni, le Pubbliche Amministrazioni sono chiamate ad adottare modelli di valutazione economica più evoluti, capaci di collegare la spesa sostenuta al valore effettivamente generato dal sistema e di supportare decisioni di procurement coerenti con la complessità delle soluzioni di IA.

4.3 Approccio del ciclo di vita e costo livellato dell'IA (LCOAI)

Al fine di superare le criticità sopra descritte, le Pubbliche Amministrazioni dovrebbero adottare un approccio di valutazione economica fondato sull'analisi di ciclo di vita dei sistemi di IA. Tale approccio consente di rappresentare in modo unitario i costi di investimento e quelli di esercizio, nonché di valutare la sostenibilità complessiva della soluzione nel tempo.

In questa prospettiva assume un rilievo interessante il concetto di Costo Livellato dell'Intelligenza Artificiale (Levelized Cost of Artificial Intelligence – LCOAI)[15], quale metrica proposta per l'analisi economica comparativa delle diverse strategie di procurement e deployment.

Il LCOAI esprime il rapporto tra il costo complessivo di ciclo di vita del sistema e l'output produttivo effettivamente generato, misurato in termini di inferenze valide o servizi erogati. Il costo complessivo

[15] Si veda articolo di Eliseo Curcio *"Evaluating the lifecycle economics of AI: The levelized cost of artificial intelligence (LCOAI)"* pubblicato su "Information Systems" 136 (2026)

include sia le spese in conto capitale (CAPEX) sia le spese operative ricorrenti (OPEX), opportunamente considerate lungo l'orizzonte temporale di riferimento.
L'adozione di una metrica di costo livellato consente di rendere confrontabili soluzioni caratterizzate da strutture di costo profondamente diverse, quali:

- soluzioni basate su servizi API forniti da terzi;
- soluzioni cloud-hosted con infrastruttura dedicata;
- soluzioni self-hosted con investimenti infrastrutturali rilevanti;
- architetture ibride che combinano più modalità di deployment.

Il LCOAI non deve essere interpretato come un indicatore meramente contabile, ma come uno strumento di supporto alle decisioni pubbliche, utile per orientare le scelte di investimento, rafforzare la trasparenza e prevenire fenomeni di lock-in economico.

4.4 Monitoraggio del comportamento del sistema in esercizio

La sostenibilità economica di un sistema di IA non può essere valutata esclusivamente in fase di affidamento, ma richiede un monitoraggio continuo durante l'esecuzione del contratto. Il comportamento del sistema incide infatti sia sui livelli di servizio sia sull'andamento della spesa.

Le amministrazioni devono dotarsi di strumenti di monitoraggio che consentano di verificare la conformità del sistema ai requisiti contrattuali e di individuare tempestivamente eventuali anomalie.

Conformità ai requisiti

Il monitoraggio deve accertare che il sistema operi in coerenza con le prestazioni attese, con gli standard di qualità definiti in sede di gara e con le condizioni contrattuali. Ciò implica la definizione di indicatori misurabili e la raccolta strutturata di dati relativi al funzionamento del sistema.

Gestione delle anomalie

Particolare attenzione deve essere dedicata agli scostamenti significativi rispetto ai livelli di prestazione attesi, ai comportamenti non coerenti del sistema e alle variazioni inattese dei costi. Il contratto deve disciplinare le modalità di segnalazione, analisi e risoluzione delle anomalie, nonché le responsabilità delle parti coinvolte.

Il monitoraggio in esercizio rappresenta un presidio essenziale del governo contrattuale e contribuisce a garantire che l'adozione dell'IA avvenga nel rispetto dei principi di economicità, efficacia e buon andamento.

Indicazioni operative

Il monitoraggio delle prestazioni e dei costi non dovrebbe limitarsi alla sola produzione di report periodici, ma deve essere accompagnato da meccanismi operativi di gestione e mitigazione. In presenza di scostamenti significativi rispetto alle previsioni iniziali — ad esempio in termini di volumi di inferenza, consumo computazionale o costi di esercizio — le amministrazioni dovrebbero prevedere specifiche azioni correttive, quali la revisione delle configurazioni del sistema, l'ottimizzazione dei modelli utilizzati, la ridefinizione dei livelli di servizio o la rinegoziazione delle condizioni contrattuali. Nei casi in cui il servizio non sia interrompibile per esigenze di continuità operativa, tali interventi dovrebbero essere pianificati attraverso appositi piani di mitigazione concordati con il fornitore.

Il monitoraggio dei sistemi di IA non riguarda esclusivamente la gestione contrattuale della fornitura, ma include anche una dimensione funzionale legata all'utilizzo e al governo operativo del sistema. Accanto alle attività di verifica tipicamente attribuite al RUP e alle strutture responsabili del contratto, è pertanto necessario coinvolgere anche le strutture organizzative responsabili dei processi amministrativi supportati dal sistema, al fine di valutare l'effettivo comportamento del modello in esercizio, la qualità dei risultati prodotti e l'impatto sui procedimenti amministrativi.

4.5 Componenti di costo rilevanti

Ai fini della valutazione economica di ciclo di vita, le amministrazioni dovrebbero considerare in modo sistematico tutte le categorie di costo che concorrono al funzionamento del sistema. Nei sistemi di Intelligenza Artificiale, la distinzione tra spese in conto capitale (CAPEX) e spese operative (OPEX) dipende in larga misura dal modello di erogazione della soluzione — on-premises, cloud o ibrido —

nonché dalla struttura contrattuale adottata. Una medesima componente può pertanto assumere natura di investimento oppure di servizio.

Spese in conto capitale (CAPEX)

Rientrano generalmente tra le spese di investimento le componenti che determinano la creazione o l'acquisizione di asset durevoli sotto il controllo dell'amministrazione.

Si tratta, quindi, di investimenti iniziali, per la messa in esercizio, quando capitalizzabili secondo i principi contabili.

Comprendono, in via esemplificativa:

- acquisizione o predisposizione dell'infrastruttura di calcolo;
- storage on-premise;
- realizzazione o potenziamento di data center;
- sviluppo pipeline di dati;
- integrazione con i sistemi informativi esistenti;
- acquisto di licenze perpetue;
- attività iniziali di sicurezza, audit e compliance;
- setup e fine-tuning dei modelli;
- costi di avviamento del servizio.

L'impatto sul LCOAI è elevato nella fase iniziale ed incide sulla soglia di convenienza nel medio periodo.

Spese operative ricorrenti (OPEX)

Rientrano tra le spese operative i costi ricorrenti necessari al funzionamento, alla gestione e all'evoluzione del sistema.

Comprendono, in via esemplificativa:

- costi di inferenza e consumo computazionale comprensivo dei costi energetici, della capacità di calcolo e dell'utilizzo di acceleratori hardware eventualmente impiegati;

- storage, rete e servizi cloud;
- monitoraggio e auditing continuo;
- manutenzione correttiva ed evolutiva;
- aggiornamento e riaddestramento dei modelli, ove necessario per garantirne l'accuratezza nel tempo;
- canoni software;
- costi di personale;
- adeguamento normativo, manutenzioni evolutive e correttive.

Si tratta, quindi, di costi ricorrente e variabili in funzione dell'utilizzo; l'impatto sul LCOAI è continuativo e determina la sostenibilità economica nel tempo.

Una rappresentazione completa delle componenti di costo consente di costruire basi d'asta più aderenti alla realtà operativa e di ridurre il rischio di sottostime.

Oltre a CAPEX e OPEX, infatti, sono da considerare i costi organizzativi e i costi di uscita e transizione.

Costi organizzativi

I costi organizzativi comprendono, in via esemplificativa:

- formazione del personale;
- rafforzamento delle competenze;
- governance;
- revisione dei processi;
- gestione del cambiamento.

Si tratta di costi progressivi e strutturali, con un impatto sul LCOAI di medio-lungo periodo. Incidono, inoltre, sulla capacità di governo del sistema.

Costi di uscita e transizione

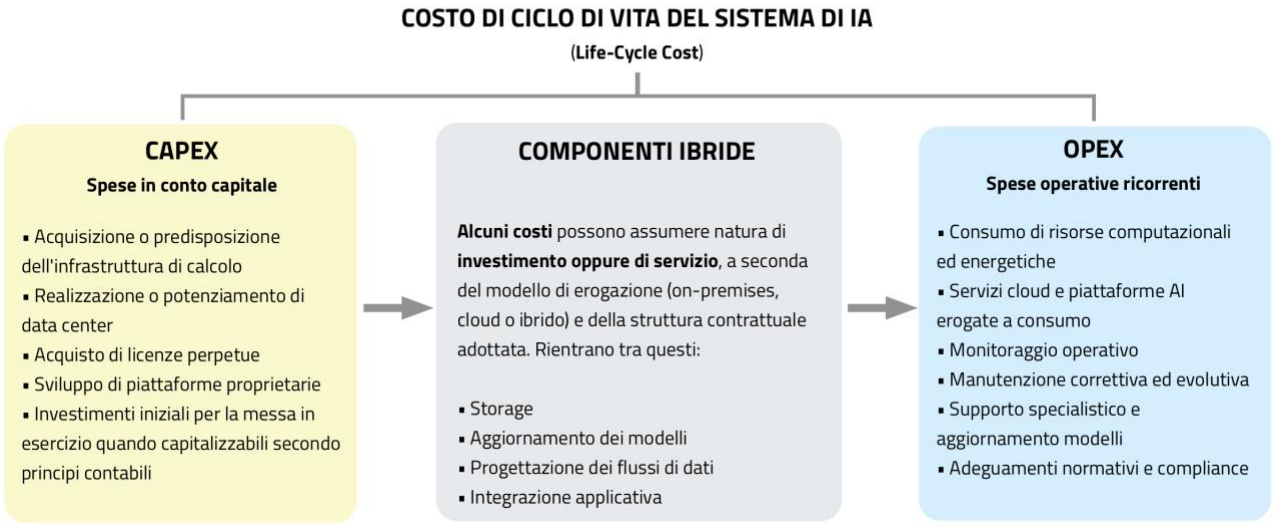
I costi di uscita e transizione comprendono, in via esemplificativa:

- migrazione dati;

- re-ingegnerizzazione delle integrazioni;
- sostituzione dei modelli;
- dismissione delle infrastrutture;
- supporto al subentro.

Si tratta di costi eventuali ma strategici, con un impatto critico sul LCOAI. Essi, inoltre, influenzano il rischio di lock-in e la flessibilità futura.

Tabella 7 - Struttura contabile dei costi nei sistemi di Intelligenza Artificiale



Categoria	Voci di costo	Natura del costo	Impatto sul LCOAI
CAPEX (Spese in conto capitale)	Acquisizione infrastrutture hardware; storage on-premises;; sviluppo pipeline dati; setup e fine-tuning dei modelli; adeguamenti di sicurezza iniziali	Investimento iniziale, ammortizzabile	Elevato nella fase iniziale; incide sulla soglia di convenienza nel medio periodo
OPEX (Spese operative ricorrenti)	Inferenza e consumo computazionale; servizi cloud; storage a consumo; manutenzione; monitoraggio; supporto operativo; canoni software	Ricorrente e variabile in funzione dell'utilizzo	Continuativo; determina la sostenibilità economica nel tempo
Costi organizzativi	Formazione del personale; rafforzamento delle competenze; governance; revisione	Progressivo e strutturale	Medio-lungo periodo; incide sulla capacità di governo del sistema

Categoria	Voci di costo	Natura del costo	Impatto sul LCOAI
	dei processi; gestione del cambiamento		
Costi di uscita e transizione	Migrazione dati; re-ingegnerizzazione delle integrazioni; sostituzione dei modelli; dismissione infrastrutture; supporto al subentro	Eventuale ma strategico	Critico; influenza il rischio di lock-in e la flessibilità futura

4.6 Output produttivo e misurabilità

Elemento centrale dell'approccio LCOAI è la definizione dell'output produttivo del sistema. Le amministrazioni dovrebbero identificare unità di output chiare, misurabili e verificabili, quali:

- risposte generate da sistemi conversazionali;
- decisioni parzialmente automatizzate o raccomandazioni;
- classificazioni e previsioni;
- servizi erogati a cittadini e imprese.

Dovrebbero essere esclusi dal computo i processi non direttamente finalizzati all'erogazione del servizio, al fine di evitare distorsioni nella valutazione economica

4.7 Applicazioni del LCOAI nel ciclo di procurement

L'approccio basato sul costo livellato dell'Intelligenza Artificiale (LCOAI) può essere applicato in modo trasversale nelle diverse fasi del ciclo di procurement, contribuendo a rafforzare la coerenza tra programmazione, progettazione, affidamento, stipula ed esecuzione del contratto. L'integrazione di tale metrica nei processi decisionali consente alle Pubbliche Amministrazioni di adottare una prospettiva economica di medio-lungo periodo, superando logiche valutative concentrate sul solo prezzo iniziale e favorendo scelte maggiormente sostenibili.

Applicazione nella fase di programmazione

Nella fase di programmazione, il ricorso a un'analisi di ciclo di vita supportata dal LCOAI consente all'amministrazione di valutare ex ante la sostenibilità economica delle diverse opzioni tecnologiche, tenendo conto non solo degli investimenti iniziali ma anche dei costi operativi attesi lungo l'intero periodo di utilizzo del sistema.

In tale contesto, il LCOAI può contribuire a:

- motivare in modo più robusto le scelte di investimento;
- migliorare la qualità delle analisi di fabbisogno;
- supportare la pianificazione pluriennale delle risorse;
- ridurre il rischio di sottostima dei costi di esercizio.

L'utilizzo di metriche di costo livellato già in fase programmatoria favorisce inoltre una maggiore trasparenza nei processi decisionali e rafforza la capacità dell'amministrazione di dimostrare la coerenza tra obiettivi perseguiti e risorse allocate.

Applicazione nella fase di progettazione

Durante la progettazione del procurement, il LCOAI rappresenta uno strumento utile per confrontare architetture alternative e modelli di deployment differenti, integrando i profili economici con i requisiti funzionali, prestazionali e di sicurezza. In particolare, esso consente di valutare in modo più consapevole i bilanciamenti tra costi iniziali e costi ricorrenti, evitando di privilegiare soluzioni caratterizzate da bassi investimenti iniziali ma da elevati oneri operativi nel tempo.

L'amministrazione può inoltre utilizzare il LCOAI per:

- definire basi d'asta più aderenti alla reale struttura dei costi;
- individuare le principali determinanti economiche del servizio;
- impostare requisiti tecnici coerenti con gli obiettivi di sostenibilità;
- orientare le scelte architetturali verso soluzioni maggiormente governabili;
- definire una precisa allocazione dei fondi necessari nei bilanci annuali e pluriennali.

Una progettazione supportata da metriche di ciclo di vita contribuisce a ridurre l'incertezza economica e a migliorare la qualità complessiva della documentazione di gara.

Applicazione nella fase di affidamento

Nella fase di affidamento, l'approccio LCOAI può essere utilizzato come supporto metodologico alla definizione dei criteri di aggiudicazione nell'ambito dell'offerta economicamente più vantaggiosa. In particolare, l'amministrazione può valorizzare, tra gli elementi di valutazione dell'offerta, la sostenibilità economica complessiva della soluzione proposta, la trasparenza della struttura dei costi, la prevedibilità degli oneri operativi e la capacità di contenere il costo di ciclo di vita del sistema.

Pur nel rispetto della disciplina vigente in materia di criteri di aggiudicazione, il LCOAI può costituire un riferimento utile per strutturare sub-criteri economici e tecnico-economici che favoriscano un confronto tra offerte fondato sul valore generato nel tempo, piuttosto che sul solo prezzo iniziale. Ciò risulta particolarmente rilevante nei sistemi di IA, nei quali la componente di costo operativo può superare significativamente quella di investimento.

L'adozione di tale approccio contribuisce inoltre a migliorare il dialogo con il mercato, incentivando gli operatori economici a presentare offerte maggiormente trasparenti e sostenibili.

Applicazione nella fase di stipula del contratto

Sebbene il LCOAI sia prevalentemente utilizzato come strumento di analisi ex ante, esso può produrre effetti rilevanti anche nella fase di stipula. Le ipotesi economiche formulate durante la gara possono infatti trovare adeguato riscontro nelle clausole contrattuali, in particolare per quanto riguarda:

- i meccanismi di determinazione dei corrispettivi;
- le condizioni di revisione dei prezzi;
- le soglie di consumo;
- le modalità di rendicontazione dei servizi;
- gli indicatori economici da monitorare.

Un allineamento tra modello economico e disciplina contrattuale consente di prevenire ambiguità interpretative e di rafforzare la governabilità del rapporto con il fornitore.

Applicazione nella fase di esecuzione

Nella fase di esecuzione, la valutazione di ciclo di vita consente di monitorare l'andamento dei costi effettivi rispetto alle stime formulate in sede di gara. L'amministrazione può utilizzare indicatori derivati dal LCOAI per verificare la coerenza tra livelli di servizio erogati, volumi di utilizzo e spesa sostenuta, individuando tempestivamente eventuali scostamenti.

Il monitoraggio economico assume particolare rilevanza nei contratti basati su modelli di pricing variabile, nei quali incrementi anche modesti dei volumi possono tradursi in aumenti significativi della spesa. In tali contesti, la disponibilità di metriche strutturate consente di adottare misure correttive, rinegoziare condizioni contrattuali ove consentito e prevenire fenomeni di crescita incontrollata dei costi, consentendo all'Amministrazione di attivare piani di fallback.

L'analisi continuativa del costo livellato può inoltre supportare le decisioni relative all'evoluzione del sistema, all'estensione degli ambiti applicativi o all'eventuale transizione verso soluzioni alternative.

In sintesi, l'applicazione del LCOAI lungo l'intero ciclo di procurement contribuisce a rafforzare la qualità delle decisioni pubbliche, favorendo un approccio maggiormente consapevole rispetto alla gestione delle risorse e alla sostenibilità degli investimenti in Intelligenza Artificiale. L'integrazione di tale o simili metriche nei processi di procurement rappresenta pertanto una buona pratica per le amministrazioni che intendano coniugare innovazione tecnologica e responsabilità nella gestione della spesa pubblica

4.8 Comparabilità delle strategie di deployment

L'analisi comparativa basata sul costo livellato dell'Intelligenza Artificiale (LCOAI) evidenzia come le diverse strategie di deployment dei sistemi di IA presentino profili economici, operativi e di rischio significativamente differenti. La possibilità di confrontare tali strategie attraverso una metrica normalizzata consente alle Pubbliche Amministrazioni di superare valutazioni fondate esclusivamente

sul costo iniziale e di adottare decisioni maggiormente coerenti con gli obiettivi di sostenibilità, governabilità e continuità del servizio.

Le principali modalità di deployment — soluzioni basate su API, infrastrutture cloud-hosted, modelli self-hosted e configurazioni ibride — non rappresentano alternative puramente tecnologiche, ma implicano scelte strategiche che incidono sull'intero ciclo di vita del sistema, sulla struttura dei costi e sul grado di controllo esercitabile dall'amministrazione, anche in base alle competenze del personale.

Le soluzioni basate su API fornite da terzi tendono a ridurre significativamente i costi iniziali, in quanto non richiedono investimenti infrastrutturali rilevanti né attività complesse di gestione operativa. Esse consentono una rapida attivazione del servizio e offrono elevata scalabilità, risultando particolarmente adatte in contesti caratterizzati da fabbisogni variabili o da elevata incertezza sui volumi di utilizzo. Tuttavia, tali soluzioni presentano generalmente una maggiore incidenza dei costi operativi ricorrenti e possono esporre l'amministrazione a dinamiche di spesa meno prevedibili, soprattutto in presenza di modelli tariffari basati sul consumo.

Un ulteriore elemento di attenzione riguarda il possibile rischio di dipendenza dal fornitore, che può manifestarsi qualora le interfacce, i modelli o le modalità di accesso al servizio non siano facilmente sostituibili. In tali contesti, l'analisi LCOAI consente di rendere più esplicito il costo complessivo associato a tale dipendenza, supportando valutazioni più consapevoli.

Le soluzioni self-hosted, al contrario, richiedono investimenti iniziali più elevati, legati all'acquisizione o alla predisposizione dell'infrastruttura di calcolo, alla gestione dei modelli e all'organizzazione delle attività operative. Esse comportano inoltre la necessità di disporre di competenze tecniche adeguate e di presìdi organizzativi in grado di garantire il funzionamento continuo del sistema.

Tuttavia, al crescere dei volumi di utilizzo, tali soluzioni possono beneficiare di economie di scala e offrire una maggiore prevedibilità della spesa nel tempo. Inoltre, esse tendono ad assicurare un livello più elevato di controllo sull'architettura, sui dati e sulle modalità di trattamento delle informazioni, risultando particolarmente coerenti con contesti applicativi caratterizzati da elevati requisiti di sicurezza o da esigenze di sovranità del dato. Senza trascurare l'opportunità di condivisione di queste soluzioni in sinergie inter-istituzionali.

Le soluzioni cloud-hosted si collocano generalmente in una posizione intermedia. Esse consentono di limitare gli investimenti infrastrutturali diretti, appaltando al fornitore la gestione delle risorse

tecnologiche, ma richiedono comunque un'attenta valutazione dei costi operativi, delle condizioni contrattuali e dei livelli di servizio garantiti. Il modello cloud può offrire elevata flessibilità e capacità di adattamento ai cambiamenti della domanda, ma implica la necessità di presidiare con attenzione i profili relativi alla localizzazione dei dati, alla sicurezza e alla continuità operativa.

Sempre più diffuse risultano infine le architetture ibride, che combinano diverse modalità di deployment al fine di ottimizzare il rapporto tra costi, prestazioni e controllo. Ad esempio, l'amministrazione può scegliere di mantenere internamente componenti particolarmente sensibili — quali i dati o l'orchestratore — ricorrendo al contempo a servizi esterni per specifiche funzionalità ad alta intensità computazionale. Sebbene tali configurazioni possano offrire vantaggi significativi in termini di flessibilità, esse richiedono una maggiore capacità di progettazione architetturale e di governo contrattuale, e maggiori competenze.

Alla luce di tali differenze, le amministrazioni dovrebbero valutare i trade-off tra le diverse strategie di deployment non solo in termini di costo immediato, ma anche considerando una pluralità di fattori che incidono sulla sostenibilità complessiva della soluzione. Tra questi assumono particolare rilievo:

- il grado di controllo esercitabile sull'infrastruttura e sui modelli;
- le garanzie di sicurezza e protezione dei dati;
- la prevedibilità della spesa nel tempo;
- la scalabilità della soluzione;
- la flessibilità evolutiva;
- il rischio di lock-in tecnologico ed economico;
- la coerenza con le strategie digitali dell'ente;
- la disponibilità e il mantenimento di competenze interne.

L'utilizzo del LCOAI consente di integrare tali dimensioni in una valutazione economica più ampia, rendendo esplicite le conseguenze finanziarie delle scelte architetturali e favorendo decisioni maggiormente informate.

È opportuno sottolineare che non esiste una strategia di deployment universalmente preferibile. La scelta deve essere calibrata sul contesto amministrativo, sulla natura del servizio, sui livelli di rischio accettabili e sulla capacità dell'ente di governare la soluzione nel tempo. In particolare, le amministrazioni dovrebbero evitare approcci semplicistici fondati sulla riduzione dei costi iniziali,

qualora tali scelte possano compromettere la sostenibilità economica futura o limitare la libertà di evoluzione tecnologica.

L'analisi comparativa delle strategie di deployment assume inoltre rilievo nella fase di progettazione del procurement, in quanto consente di impostare requisiti tecnici e modelli contrattuali coerenti con la soluzione prescelta. Una valutazione economica condotta ex ante attraverso il LCOAI o metodi simili contribuisce a ridurre l'incertezza, a migliorare la qualità delle basi d'asta e a favorire un confronto competitivo più trasparente.

Una strategia di deployment con soluzioni basate su API, ad esempio, ha tipicamente CAPEX molto ridotti e OPEX variabili, legati al consumo. Il livello di controllo della PA è, dunque, limitato e la prevedibilità della spesa è medio-bassa. Di converso, il rischio di lock-in è medio-alto. Per tali motivi, queste soluzioni sono maggiormente idonee in contesti con fabbisogni incerti, sperimentazioni, servizi a domanda variabile.

Le soluzioni cloud-hosted, invece, presentano una struttura dei costi (LCOAI) con CAPEX contenuti e OPEX strutturati ma scalabili. Questo fa sì che il livello di controllo della PA si attesti su un livello intermedio, con una media prevedibilità della spesa. Il rischio di lock-in è medio: per queste ragioni, si tratta di soluzioni maggiormente idonee in contesti caratterizzate dalla presenza di servizi con crescita progressiva o necessità di flessibilità.

Le soluzioni self-hosted, al contrario, presentano CAPEX elevati e OPEX più stabili nel tempo. Il livello di controllo della PA è elevato e la prevedibilità della spesa alta. Essendo il rischio di lock-in basso o medio, si tratta di soluzioni maggiormente idonee in contesti ad alta sicurezza, sovranità del dato e dei modelli, volumi prevedibili.

Le architetture ibride, infine, si caratterizzano per un mix CAPEX/OPEX ottimizzabile, con un elevato livello di controllo della PA, se le architetture sono ben progettate. La prevedibilità della spesa è medio-alta e il rischio di lock-in variabile; per questo, sono maggiormente idonee in contesti caratterizzati dalla presenza di sistemi complessi, integrazione con asset esistenti, esigenze differenziate.

In conclusione, la comparabilità delle strategie di deployment rappresenta un passaggio essenziale per garantire che le decisioni di procurement dei sistemi di IA siano orientate non solo all'efficienza economica immediata, ma anche alla sostenibilità nel medio-lungo periodo. L'adozione di metriche di

costo livellato consente alle Pubbliche Amministrazioni di rafforzare la propria capacità decisionale, coniugando innovazione tecnologica e responsabilità nella gestione delle risorse pubbliche.

Tabella 8: Confronto delle strategie di deployment dei sistemi di IA ai fini del procurement

Strategia di deployment	Struttura dei costi (LCOAI)	Livello di controllo della PA	Prevedibilità della spesa	Rischio di lock-in	Contesti di maggiore idoneità
Soluzioni basate su API	CAPEX molto ridotti; OPEX variabili e legati al consumo	Limitato	Media–bassa	Medio–alto	Fabbisogni incerti, sperimentazioni, servizi a domanda variabile
Cloud-hosted	CAPEX contenuti; OPEX strutturati ma scalabili	Intermedio	Media	Medio	Servizi con crescita progressiva, necessità di flessibilità
Self-hosted	CAPEX elevati; OPEX più stabili nel tempo	Elevato	Alta	Basso–medio	Contesti ad alta sicurezza, sovranità del dato e dei modelli, volumi prevedibili
Architetture ibride	Mix CAPEX/OPEX ottimizzabile	Elevato (se ben progettate)	Media–alta	Variabile	Sistemi complessi, integrazione con asset esistenti, esigenze differenziate

4.9 Implicazioni per il procurement pubblico

L'integrazione sistematica di analisi del ciclo di vita e di metriche di costo livellato nei processi di procurement contribuisce in modo significativo a rafforzare la trasparenza, la responsabilità e la sostenibilità delle decisioni pubbliche in materia di Intelligenza Artificiale.

In un contesto caratterizzato da crescente complessità tecnologica e da modelli di costo sempre più articolati, la disponibilità di strumenti metodologici strutturati consente alle Pubbliche Amministrazioni di adottare decisioni maggiormente informate e coerenti con i principi di buon andamento, economicità ed efficacia dell'azione amministrativa.

L'utilizzo di metriche di ciclo di vita favorisce innanzitutto una maggiore **trasparenza dei processi decisionali**, rendendo esplicite le determinanti economiche delle scelte tecnologiche e permettendo di motivare in modo più robusto le opzioni di investimento.

Ciò assume particolare rilievo nei contesti in cui le soluzioni di IA comportano impegni finanziari pluriennali (la maggior parte dei casi) o presentano dinamiche di costo difficilmente prevedibili in assenza di un'analisi strutturata.

Al tempo stesso, l'approccio basato sul ciclo di vita contribuisce a rafforzare la **responsabilità amministrativa**, in quanto consente di dimostrare che le decisioni di procurement sono state assunte sulla base di valutazioni complete e proporzionate, e non esclusivamente orientate alla riduzione della spesa iniziale.

La capacità di rappresentare il costo complessivo del sistema lungo l'intero periodo di utilizzo costituisce infatti un elemento essenziale ai fini della rendicontabilità e del controllo della spesa pubblica.

Un ulteriore effetto positivo riguarda la **sostenibilità delle scelte tecnologiche**. L'adozione di metriche di costo livellato aiuta le amministrazioni a individuare soluzioni compatibili con le proprie capacità finanziarie e organizzative, riducendo il rischio di investimenti che, pur risultando sostenibili nel breve periodo, possano generare criticità nel medio-lungo termine.

In tale prospettiva, la sostenibilità deve essere intesa non solo in senso economico, ma anche come capacità dell'amministrazione di governare l'evoluzione del sistema e di garantirne la continuità operativa.

L'integrazione di tali strumenti analitici contribuisce inoltre a migliorare la **qualità del dialogo con il mercato**. Amministrazioni dotate di una chiara comprensione delle determinanti di costo sono infatti meglio posizionate per interagire con gli operatori economici, valutare le proposte ricevute e negoziare condizioni contrattuali più favorevoli.

La disponibilità di metriche condivisibili favorisce una maggiore simmetria informativa tra amministrazione e fornitori, riducendo il rischio di offerte caratterizzate da strutture di costo opache o difficilmente confrontabili.

Sotto il profilo operativo, l'approccio basato sul ciclo di vita può supportare le amministrazioni nella costruzione di basi d'asta più aderenti alla realtà dei costi, nella definizione di criteri di aggiudicazione coerenti con il valore complessivo delle soluzioni e nella predisposizione di meccanismi contrattuali capaci di governare l'evoluzione della spesa.

Ciò risulta particolarmente rilevante nei sistemi di IA, nei quali la componente di costo operativo può assumere un peso significativo e crescere nel tempo in funzione dei livelli di utilizzo.

Attraverso una rappresentazione più completa delle implicazioni economiche, le amministrazioni possono evitare fenomeni di dipendenza da soluzioni che, pur efficienti nella fase di avvio, risultino difficilmente gestibili nel lungo periodo.

Le implicazioni dell'approccio LCOAI si estendono anche alla fase di esecuzione del contratto. La disponibilità di indicatori economici chiari consente infatti di monitorare l'andamento della spesa, verificare la coerenza tra costi stimati e costi effettivi e adottare tempestivamente eventuali misure correttive.

In tal modo, la valutazione economica non rimane confinata alla fase di gara, ma diventa parte integrante del governo contrattuale.

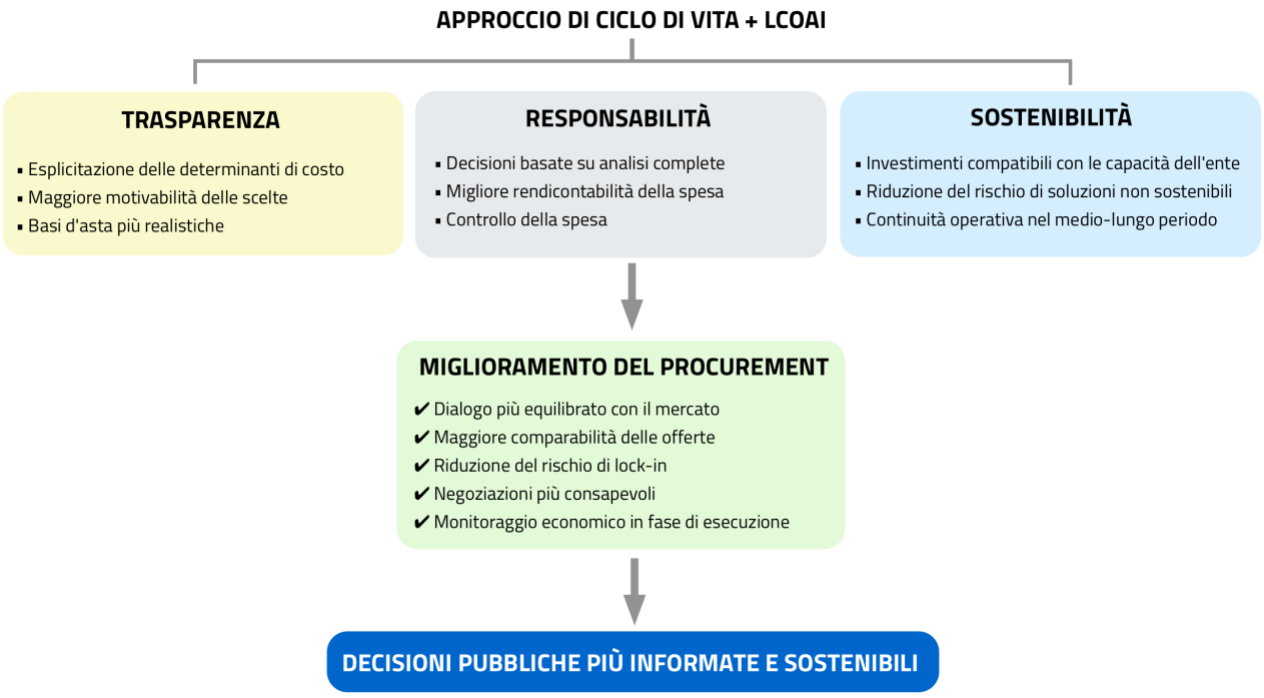
È opportuno sottolineare che l'introduzione di pratiche avanzate di valutazione economica non implica l'adozione di modelli rigidi o uniformi.

Le amministrazioni devono poter adattare gli strumenti metodologici alle proprie specificità organizzative, dimensionali e operative, nonché alla natura dei servizi da acquisire.

Il quadro di riferimento delineato nel presente Capitolo è pertanto concepito come un insieme di principi e criteri applicabili con il necessario grado di flessibilità, nel rispetto dell'autonomia organizzativa degli enti.

In questa prospettiva, l'integrazione sistematica di analisi basate sul ciclo di vita e di metriche di costo livellato rappresenta una buona pratica per le amministrazioni che intendano coniugare innovazione tecnologica e responsabilità nella gestione delle risorse pubbliche.

Figura - Impatti dell'approccio di ciclo di vita + LCOAI sul procurement pubblico



5. Strumenti di procurement e cooperazione tra PA

5.1 Finalità e ambito del capitolo

Il procurement di sistemi di Intelligenza Artificiale richiede una valutazione particolarmente attenta degli strumenti di approvvigionamento previsti dal Codice dei contratti pubblici. In un contesto tecnologico caratterizzato da elevata dinamicità e da modelli di servizio in continua evoluzione, la scelta dello strumento di procurement non assume una valenza meramente procedurale, ma incide in modo diretto sulla capacità della Pubblica Amministrazione di governare l'evoluzione del sistema, contenere i rischi tecnologici ed economici e garantire la sostenibilità degli investimenti nel medio-lungo periodo.

La selezione dello strumento di approvvigionamento rappresenta pertanto una decisione strategica, che deve essere assunta in coerenza con gli obiettivi perseguiti dall'amministrazione, con la corretta analisi del livello di maturità delle soluzioni disponibili sul mercato e con la capacità organizzativa dell'ente di presidiare le diverse fasi del ciclo contrattuale. Una scelta non adeguatamente ponderata può infatti limitare la flessibilità dell'amministrazione, ostacolare l'evoluzione del sistema o generare forme di dipendenza difficilmente reversibili.

A differenza di molte forniture ICT tradizionali, i sistemi di IA non si configurano come prodotti statici, ma come ecosistemi tecnologici complessi, spesso caratterizzati da una forte integrazione tra modelli, dati, infrastrutture e componenti applicative, in aggiunta alla natura intrinseca della molteplicità: di modelli, di strumenti, di pipeline dati. Tale natura sistemica rende particolarmente rilevante la capacità dell'amministrazione di selezionare strumenti di procurement idonei a governare non solo l'acquisizione iniziale, ma anche le successive fasi di adattamento, aggiornamento ed estensione del sistema.

I sistemi di IA presentano infatti alcune caratteristiche strutturali che devono essere attentamente considerate nella selezione dello strumento di procurement, tra cui:

- l'elevata complessità tecnica e architetturale, che richiede competenze specialistiche e modelli contrattuali capaci di disciplinare soluzioni articolate;

- la forte dipendenza dai dati e dal contesto applicativo, che rende necessario garantire adeguati livelli di controllo, sicurezza, interoperabilità e portabilità;
- la naturale tendenza all'evoluzione continua del sistema, determinata sia dall'avanzamento tecnologico sia dall'emergere di nuovi fabbisogni amministrativi;
- la difficoltà di definire ex ante prestazioni e comportamenti in modo pienamente statico, soprattutto nei sistemi basati su modelli adattivi;
- la crescente rilevanza della fase di esecuzione contrattuale, nella quale si concentra una parte significativa del valore del servizio e della spesa sostenuta.

Tali caratteristiche rendono spesso inadeguati approcci al procurement fondati su logiche rigidamente prescrittive o su specifiche tecniche eccessivamente dettagliate, che rischiano di limitare la capacità dell'amministrazione di adattare il sistema alle esigenze emergenti. Ne deriva l'esigenza di privilegiare strumenti contrattuali che consentano un adeguato grado di flessibilità, pur nel rispetto dei principi fondanti del Codice dei contratti pubblici, in particolare quelli di concorrenza, trasparenza e parità di trattamento.

La scelta dello strumento di approvvigionamento dovrebbe pertanto essere effettuata sulla base di una valutazione integrata che tenga conto, tra l'altro:

- del livello di maturità tecnologica della soluzione;
- della chiarezza e stabilità del fabbisogno pubblico;
- della durata prevista del ciclo di vita del sistema;
- del grado di incertezza associato all'evoluzione tecnologica;
- dell'intensità dei fabbisogni di integrazione;
- della capacità dell'amministrazione di governare il contratto.

In tale valutazione, le amministrazioni sono chiamate a considerare anche gli impatti economici complessivi delle diverse opzioni di procurement, adottando una prospettiva di costo di ciclo di vita coerente con quanto illustrato nel Capitolo 3 e, ove appropriato, facendo riferimento a metriche articolate come quella del costo livellato dell'Intelligenza Artificiale (LCOAI). L'integrazione tra scelte

procedurali e valutazioni economiche contribuisce infatti a ridurre il rischio di decisioni orientate esclusivamente al contenimento della spesa iniziale, ma potenzialmente onerose nel lungo periodo.

Particolare attenzione deve essere inoltre riservata alla relazione tra strumento di procurement e governabilità del sistema. Alcuni modelli contrattuali possono infatti rafforzare la capacità dell'amministrazione di mantenere il controllo sull'architettura, sui dati e sulle modalità di evoluzione della soluzione, mentre altri possono determinare vincoli difficilmente superabili. La valutazione ex ante di tali profili costituisce una componente essenziale di una strategia di procurement responsabile.

La scelta dello strumento di approvvigionamento assume rilievo anche in relazione alla gestione del rischio. Strumenti eccessivamente rigidi possono limitare la possibilità di intervenire in presenza di malfunzionamenti del sistema, variazioni dei fabbisogni, evoluzioni tecnologiche o criticità operative. Modelli contrattuali più flessibili possono invece favorire un adattamento progressivo della soluzione, riducendo l'esposizione a rischi difficilmente governabili. In tale prospettiva, il procurement deve essere inteso come una leva di gestione del rischio, oltre che come una procedura di acquisizione.Un ulteriore elemento di attenzione riguarda la capacità dello strumento selezionato di sostenere l'innovazione senza compromettere la stabilità dei servizi. Le amministrazioni sono chiamate a trovare un equilibrio tra l'esigenza di sperimentare soluzioni avanzate e la necessità di garantire continuità amministrativa, evitando interruzioni o regressioni nei livelli di servizio, facendo attenzione ai piani di fallback e a quelli di rollback per le specifiche soluzioni.

Il presente Capitolo si propone pertanto di fornire alle Pubbliche Amministrazioni un quadro di riferimento per l'utilizzo consapevole degli strumenti di procurement, promuovendo un approccio strategico che integri valutazioni tecnologiche, economiche e organizzative. In tale prospettiva, assumono particolare rilievo non solo le procedure di affidamento, ma anche le forme di cooperazione inter-amministrativa che possono contribuire a ridurre la frammentazione degli investimenti e a favorire lo sviluppo di ecosistemi pubblici di Intelligenza Artificiale.

Il rafforzamento delle pratiche cooperazione risponde inoltre all'esigenza di promuovere economie di scala e una più efficiente allocazione delle risorse. Tale approccio risulta particolarmente coerente con la natura dei sistemi di IA, nei quali il valore generato può spesso essere esteso a più contesti amministrativi simili.

In definitiva, la capacità di selezionare strumenti di procurement adeguati rappresenta una condizione essenziale affinché l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione avvenga in modo sostenibile, governabile e coerente con l'interesse pubblico. Il presente Capitolo intende supportare le amministrazioni in tale percorso, offrendo criteri interpretativi e indicazioni operative per orientare scelte consapevoli in un ambito caratterizzato da elevata complessità

5.2 Dalla progettazione del sistema alla definizione dell'oggetto di procurement

Di seguito viene descritto un quadro metodologico utile per le amministrazioni allo scopo di strutturare dei progetti di Intelligenza Artificiale ai fini del procurement. In particolare, viene proposto un modello di riferimento volto a supportare la scomposizione dei progetti nelle principali componenti tecniche, organizzative e contrattuali, facilitando la predisposizione dei capitolati tecnici e la definizione delle voci di fornitura.

Considerata la complessità che caratterizza i sistemi di IA, tale impostazione consente di rafforzare la capacità delle stazioni appaltanti di programmare gli interventi, migliorare la qualità della progettazione della gara e presidiare l'intero ciclo di vita della soluzione.

Per la corretta interpretazione di quanto segue, si precisa che il sistema di IA ed il progetto di IA sono due entità separate che potrebbero essere in relazione N a M (ad es. un sistema di IA potrebbe essere legato ad un progetto di implementazione e a più progetti di evoluzione; allo stesso tempo un progetto potrebbe avere ad oggetto più sistemi di IA).

Tenendo conto del modello del ciclo di vita di un sistema di IA definito dall'OCSE – adottato come riferimento nella Linea guida sull'adozione di IA nella pubblica amministrazione – nonché dell'AI lifecycle generic reference model definito da ENISA, si descrive di seguito il ciclo di vita di un progetto di IA suddiviso nelle fasi:

- **definizione dell'obiettivo**: l'amministrazione definisce l'obiettivo che il sistema di IA si prefigge di raggiungere; a tal fine devono essere identificati il contesto nel quale il sistema dovrà operare e i dati necessari;
- **raccolta dei dati**: si effettua la raccolta di un set di dati eterogeneo (in forma strutturata e non) dalle varie sorgenti (interne ed esterne alle amministrazioni) e dei corrispondenti metadati; l'acquisizione deve essere conforme alle politiche sulla gestione dei dati dell'amministrazione e di eventuali fornitori (dei dati) e alla normativa in materia di protezione dei dati personali;
- **esplorazione dei dati**: i dati raccolti sono analizzati al fine di verificarne la qualità, la completezza, la coerenza e l'idoneità rispetto agli obiettivi del sistema di IA. In tale fase assume particolare rilievo la presenza di metadati adeguati, l'adozione di ontologie o modelli semantici ove necessari e la verificabilità delle condizioni di utilizzo dei dati.;
- **pre-elaborazione dei dati**: consiste nella pulizia (correzione di errori, rimozione del rumore, anonimizzazione/pseudonimizzazione) e standardizzazione dei dati raccolti. (integrati dalle varie fonti e trasformati secondo le esigenze (ad esempio convertendoli in formato numerico); le caratteristiche più rilevanti dell'insieme di dati (dataset) sono identificate e selezionate, scartando quelle non di interesse, con l'obiettivo di ridurne il volume e il rumore[16];
- **selezione dell'architettura**: sulla base dei requisiti tecnici del sistema da realizzare e dell'obiettivo da raggiungere, si identifica l'istanza dell'architettura necessaria, secondo quanto descritto al capitolo 3;
- **selezione del modello (o dei modelli)**: individuazione del modello di IA [17] che maggiormente si adatta al sistema di IA da realizzare sulla base dell'obiettivo definito e dei dati disponibili; l'individuazione del (dei) modello (i) comporta anche la scelta della tipologia di algoritmo di apprendimento[18] con il quale verrà addestrato;
- **addestramento del (dei) modello (i)**: il modello di IA scelto è addestrato sulla base dei dati elaborati nelle fasi precedenti e dell'algoritmo di apprendimento individuato;

[16] Rumore: il termine indica qualsiasi tipo di disturbo, errore o variazione casuale nei dati. Questo fenomeno può verificarsi sia durante la raccolta dei dati sia durante l'addestramento. Il rumore rende più difficile per un modello apprendere correttamente le informazioni, riducendone la precisione e la capacità di generalizzazione.
[17] Modello di IA: un programma che è stato addestrato a partire da un insieme di dati con lo scopo di individuare schemi e relazioni, effettuare predizioni o creare nuovi contenuti.
[18] Tipologia di algoritmo di apprendimento: apprendimento supervisionato, non supervisionato e con rinforzo.

- **ottimizzazione e tuning:** il modello viene sottoposto a diverse fasi di ottimizzazione per migliorarne le prestazioni regolando gli iperparametri[19] sulla base di un dataset di convalida, eseguendo fine-tuning sui compiti specifici, oppure si possono applicare tecniche come Lo.Ra. (Low-Rank Adaptation) o PEFT (Parameter efficient fine tuning);
- **distribuzione del modello:** il modello addestrato viene integrato nell'architettura di orchestrazione, con un'istanza che viene resa disponibile agli utenti;
- **monitoraggio e manutenzione:** il modello prescelto e i dati in ingresso vengono continuamente monitorati e manutenuti per gestire i cambiamenti, riaddestrando il modello ove necessario;
- **valutazione delle prestazioni:** viene svolta una misurazione delle prestazioni del modello con l'applicazione di una serie di metriche pertinenti per il compito specifico; questa fase risulta necessaria per determinare quanto bene il modello addestrato svolge il compito identificando eventuali aree di miglioramento attraverso le tecniche di under/over fitting;
- **validazione etica e legale:** le implicazioni etiche e legali dell'uso del modello, come la privacy dei dati, il contenuto generato, la discriminazione e altri aspetti etici e normativi devono essere valutati con attenzione in tutte le fasi;
- **valutazione del raggiungimento dell'obiettivo:** l'amministrazione misura la percentuale di avanzamento/raggiungimento dell'obiettivo prefissato del sistema di IA.

Sulla base di quanto sopra, si suggerisce alle PA che vogliano intraprendere un'iniziativa di procurement in campo IA di raggruppare le suddette fasi nelle componenti, indicate nella tabella che segue, che potranno essere inserite nel capitolato tecnico.

Le componenti in cui si suggerisce di raggruppare le fasi sono:

- raccolta e preparazione dati;
- selezione, addestramento e ottimizzazione del modello;
- monitoraggio e valutazione;
- integrazione e personalizzazione.

[19] Parametri che consentono di controllare il processo di addestramento del modello.

La componente **Raccolta e preparazione dati** raggruppa le fasi di:

- raccolta dei dati;
- esplorazione dei dati;
- pre-elaborazione dei dati.

La componente **Selezione, addestramento e ottimizzazione del modello** raggruppa le fasi di:

- selezione dell'architettura;
- selezione del modello;
- addestramento del modello;
- ottimizzazione e tuning;
- distribuzione del modello.

La componente **Monitoraggio e valutazione** raggruppa le fasi di:

- monitoraggio e manutenzione;
- valutazione delle prestazioni;
- validazione etica e legale;
- valutazione del raggiungimento dell'obiettivo.

Questa componente raggruppa, dunque, le attività che permettono di monitorare e analizzare l'efficacia del modello di IA addestrato, verificando che rispetti i requisiti operativi, normativi e di accuratezza. Essa, inoltre, copre la verifica periodica delle prestazioni dei modelli IA e dei risultati prodotti in termini di efficienza, risparmio dei costi e miglioramento dei servizi. Allo stesso modo, comprende la verifica di correttezza, equità e trasparenza dei modelli e delle decisioni IA, in particolare per prevenire bias o discriminazioni.

La componente **Integrazione e personalizzazione** raggruppa i servizi volti ad assicurare la corretta integrazione, compatibilità ed interoperabilità del nuovo sistema di IA con i sistemi, piattaforme tecnologiche e soluzioni già esistenti. Esempi sono:

- servizi per integrare il sistema di IA con le infrastrutture IT esistenti della PA come, ad esempio, sistemi di gestione documentale, ERP, database;

- personalizzazione del sistema di IA per soddisfare le specifiche esigenze della PA, anche attraverso lo sviluppo di dashboard o interfacce utente personalizzate.

Tabella 9: Indicazione componenti

	COMPONENTE	FASI
1	RACCOLTA E PREPARAZIONE DATI	Raccolta dei dati Esplorazione dei dati Pre elaborazione dei dati
2	SELEZIONE, ADDESTRAMENTO E OTTIMIZZAZIONE DEL MODELLO	Selezione dell'architettura Selezione del modello Addestramento del modello Ottimizzazione e tuning Distribuzione del modello
3	MONITORAGGIO E VALUTAZIONE Monitorare e analizzare l'efficacia del modello di IA addestrato, verificando che rispetti i requisiti operativi, normativi e di accuratezza. Verifica periodica delle prestazioni dei modelli IA e dei risultati prodotti in termini di efficienza, risparmio dei costi e miglioramento dei servizi. Verifica della correttezza, equità e trasparenza dei modelli e delle decisioni IA, in particolare per prevenire bias o discriminazioni.	Monitoraggio e manutenzione Valutazione delle prestazioni Validazione etica e legale Valutazione del raggiungimento dell'obiettivo
4	INTEGRAZIONE E PERSONALIZZAZIONE	Servizi per integrare il sistema di IA con le infrastrutture IT

COMPONENTE	FASI
Assicurare la corretta integrazione, compatibilità ed interoperabilità del nuovo sistema di IA con i sistemi, piattaforme tecnologiche e soluzioni già esistenti. Servizi per integrare il sistema di IA con le infrastrutture IT esistenti della PA (ad esempio, sistemi di gestione documentale, ERP, database). Personalizzazione del sistema di IA per soddisfare le specifiche esigenze della PA, anche attraverso lo sviluppo di dashboard o interfacce utente personalizzate.	esistenti (ad esempio, sistemi di gestione documentale, ERP, database)

Definizione delle voci di fornitura a partire dalle componenti

Per una puntuale definizione tecnica ed economica la stazione appaltante tiene conto dell'insieme delle attività relative alle Fasi sopra descritte in termini di *effort* di risorse umane e di risorse strumentali al fine di definire puntualmente la programmazione delle stesse attività e dei relativi costi.

A ciascuna delle componenti della tabella 9 è possibile associare un elenco di servizi disponibili sul mercato: servizi di base e servizi complementari. I servizi di base sono finalizzati all'implementazione del sistema di IA, mentre i servizi complementari hanno l'obiettivo di integrare il sistema stesso con i processi già in essere nell'organizzazione e a consentire al personale dell'amministrazione di utilizzare il sistema in coerenza con il quadro normativo e in accordo con gli obiettivi dell'amministrazione.

5.3 Gare per l'approvvigionamento di sistemi di IA

Le procedure di gara costituiscono lo strumento ordinario di approvvigionamento quando il fabbisogno pubblico risulta sufficientemente definito e il mercato è in grado di offrire soluzioni comparabili sotto il profilo tecnico ed economico. In tali contesti, il ricorso a procedure competitive consente di garantire il rispetto dei principi di concorrenza, trasparenza e parità di trattamento, favorendo al contempo l'individuazione della soluzione più idonea al perseguimento dell'interesse pubblico.

Nel caso dei sistemi di Intelligenza Artificiale, tuttavia, la Pubblica Amministrazione è chiamata ad adottare un approccio evoluto alla predisposizione della documentazione di gara, superando modelli

standardizzati mutuati da altre tipologie di forniture ICT. La natura adattiva dei sistemi di IA, la loro dipendenza dai dati e la frequente difficoltà di definire ex ante prestazioni pienamente statiche rendono infatti necessario un ripensamento delle modalità attraverso cui il fabbisogno viene tradotto in requisiti di gara.

Le gare per sistemi di IA non dovrebbero essere concepite come mere procedure di acquisizione tecnologica, ma come strumenti di governo dell'innovazione. In tale prospettiva, la qualità della progettazione della gara assume un ruolo determinante nel garantire che l'amministrazione mantenga un adeguato controllo sull'evoluzione del sistema e sulla sostenibilità economica dell'investimento.

In particolare, nelle gare per sistemi di IA le amministrazioni dovrebbero privilegiare una definizione del fabbisogno orientata ai risultati e alle prestazioni attese, piuttosto che a specifiche tecnologiche rigide e prescrittive. Un approccio eccessivamente vincolante rischia infatti di limitare la partecipazione del mercato e di precludere soluzioni innovative potenzialmente più efficienti. Al contrario, una definizione funzionale del fabbisogno consente agli operatori economici di valorizzare le proprie competenze progettuali, favorendo la presentazione di proposte tecniche maggiormente evolute.

Tale impostazione non implica una riduzione del controllo pubblico, ma richiede, al contrario, una maggiore capacità dell'amministrazione di identificare con chiarezza gli obiettivi da conseguire, i livelli di servizio attesi e i criteri di misurazione delle prestazioni.

Gli atti di gara dovrebbero pertanto essere strutturati in modo da:

- definire requisiti funzionali chiari, misurabili e verificabili, evitando formulazioni generiche che possano generare ambiguità interpretative;
- esplicitare l'architettura logica di riferimento, in coerenza con quanto illustrato nel Capitolo 2, nonché i requisiti di governabilità del sistema;
- disciplinare il ruolo dei dati, incluse le modalità di accesso, utilizzo, conservazione e portabilità, prevenendo situazioni di dipendenza tecnologica;
- individuare requisiti di sicurezza, resilienza e continuità operativa adeguati alla criticità dei servizi coinvolti;
- prevedere meccanismi strutturati di monitoraggio delle prestazioni e di verifica dei risultati.

Particolare attenzione dovrebbe essere riservata alla coerenza tra requisiti tecnici e modello contrattuale. Requisiti eccessivamente dettagliati possono risultare incompatibili con contratti che richiedono flessibilità evolutiva, mentre requisiti troppo generici possono rendere difficoltosa la verifica dell'adempimento.

Centralità della fase di progettazione della gara

La progettazione della gara assume un rilievo strategico nel procurement dei sistemi di IA. Una progettazione accurata consente infatti di ridurre l'incertezza, migliorare la qualità delle offerte e prevenire criticità nella fase di esecuzione.

In tale fase, le amministrazioni dovrebbero valutare l'opportunità di svolgere consultazioni preliminari di mercato, al fine di acquisire una migliore comprensione delle soluzioni disponibili, delle dinamiche tecnologiche e delle principali determinanti di costo. Ciò risulta particolarmente utile in un ambito caratterizzato da rapida evoluzione, nel quale la distanza informativa tra amministrazione e operatori economici può essere significativa.

La progettazione dovrebbe inoltre assicurare la coerenza tra:

- obiettivi del servizio;
- architettura del sistema;
- modello di deployment;
- struttura dei costi;
- durata contrattuale
- sostenibilità ambientale ed efficienza energetica.

Una mancata integrazione tra tali elementi può compromettere la sostenibilità dell'intervento e ridurre la capacità dell'amministrazione di governare il contratto.

Costruzione del capitolato tecnico

La costruzione del capitolato tecnico rappresenta uno dei passaggi più delicati e strategici nella progettazione delle gare per l'approvvigionamento di sistemi di Intelligenza Artificiale. Attraverso il capitolato, infatti, l'amministrazione traduce il proprio fabbisogno in requisiti tecnici e funzionali vincolanti, definendo al contempo il perimetro delle prestazioni richieste, i livelli di servizio attesi e le condizioni operative del sistema.

Nel contesto dell'IA, il capitolato non può essere concepito come un mero elenco di specifiche tecnologiche, ma deve configurarsi come uno **strumento di governo della soluzione lungo l'intero ciclo di vita contrattuale**. Una redazione inadeguata può infatti determinare rigidità incompatibili con l'evoluzione tecnologica oppure, al contrario, generare ambiguità che rendono difficoltosa la verifica dell'adempimento.

Per tali ragioni, la predisposizione del capitolato tecnico dovrebbe essere improntata ai principi del risultato, della fiducia e dell'accesso al mercato, assicurando un equilibrio tra apertura all'innovazione e capacità di controllo pubblico.

Approccio funzionale e orientato ai risultati

Nel procurement di sistemi di IA è generalmente preferibile adottare un approccio funzionale, orientato alla descrizione dei risultati attesi piuttosto che alla prescrizione puntuale delle tecnologie da utilizzare. La definizione di specifiche eccessivamente dettagliate rischia infatti di limitare il confronto competitivo e di favorire soluzioni implicitamente riconducibili a determinati operatori economici.

L'amministrazione dovrebbe pertanto:

- descrivere con chiarezza l'obiettivo tecnico-amministrativo da raggiungere;
- individuare gli obiettivi di servizio e i benefici attesi;
- definire indicatori di prestazione misurabili;
- esplicitare i vincoli normativi, organizzativi e tecnologici.

Un capitolato orientato ai risultati non comporta una riduzione del presidio pubblico, ma richiede una maggiore capacità progettuale da parte della stazione appaltante, chiamata a definire con precisione le condizioni di successo dell'intervento.

Strutturazione del capitolato per componenti del sistema di IA

Al fine di rafforzare la governabilità della soluzione, il capitolato dovrebbe riflettere l'architettura logica del sistema — orchestratore, modelli, dati e strumenti applicativi — disciplinando in modo distinto le principali componenti.

In particolare, è opportuno che il capitolato:

Con riferimento all'orchestrazione del sistema:

- richieda adeguata documentazione delle logiche di funzionamento;
- garantisca la configurabilità delle regole operative;
- eviti dipendenze tecniche che impediscano la sostituibilità dei modelli.

Con riferimento ai modelli di IA:

- definisca requisiti minimi di performance;
- disciplini le modalità di aggiornamento e riaddestramento;
- preveda evidenze documentali sulla qualità dei modelli.

Con riferimento ai dati:

- chiarisca titolarità, diritti di utilizzo e condizioni di accesso;
- stabilisca requisiti di qualità, integrità e tracciabilità;
- disciplini portabilità e restituzione al termine del contratto.

Con riferimento agli strumenti applicativi e alle interfacce:

- richieda standard aperti o documentati;
- assicuri l'integrazione con i sistemi esistenti;
- eviti vincoli tecnologici non necessari.

Una tale articolazione consente di ridurre il rischio di lock-in e di favorire un approccio modulare al procurement.

Definizione dei livelli di servizio e delle metriche di prestazione

Il capitolato dovrebbe individuare in modo esplicito i livelli di servizio (SLA) e le metriche attraverso cui valutare il corretto funzionamento del sistema. Nei sistemi di IA, tali metriche non possono limitarsi alla disponibilità infrastrutturale, ma devono includere indicatori qualitativi legati alle prestazioni.

Tra i parametri che possono essere considerati rientrano, a titolo esemplificativo:

- accuratezza dei risultati;
- tasso di errore;
- tempi di risposta;
- stabilità delle prestazioni nel tempo;
- qualità degli output generati;
- affidabilità operativa
- performance del modello (accuracy, precision, recall, F1-score)
- stabilità e robustezza (resistenza a drift e perturbazioni)
- explainability (comprensibilità delle decisioni, stabilità delle spiegazioni)
- usabilità e impatto sull'utente (tasso di escalation, soddisfazione utenti)

La definizione preventiva di tali indicatori rafforza la capacità dell'amministrazione di esercitare il controllo in fase di esecuzione e contribuisce a prevenire contenziosi.

Presidi di sicurezza, trasparenza e controllo

Considerato l'impatto potenziale dei sistemi di IA su procedimenti amministrativi e diritti degli interessati, il capitolato dovrebbe prevedere requisiti coerenti con il livello di rischio del sistema, includendo misure di sicurezza, verificabilità tramite audit e supervisione umana.

È opportuno, in particolare, richiedere:

- tracciabilità delle operazioni e accesso ai log;
- documentazione aggiornata del sistema;
- supporto alle attività di audit;
- meccanismi di intervento umano;
- procedure di gestione degli incidenti.

Tali elementi contribuiscono a rendere il sistema verificabile e ad assicurare la responsabilità dell'azione amministrativa.

Clausole evolutive e gestione del cambiamento tecnologico

Data la natura dinamica dell'Intelligenza Artificiale, il capitolato dovrebbe prevedere condizioni che consentano l'evoluzione della soluzione senza compromettere l'equilibrio contrattuale.

A tal fine, l'amministrazione può valutare l'introduzione di:

- meccanismi di aggiornamento tecnologico;
- opzioni contrattuali per l'estensione delle funzionalità;
- clausole di revisione coerenti con la normativa vigente;
- condizioni di sostituzione di componenti obsolete.

L'assenza di tali previsioni può determinare una rapida obsolescenza della soluzione o generare costi non previsti.

Chiarezza, verificabilità e neutralità tecnologica

Il capitolato tecnico dovrebbe essere redatto in modo chiaro, coerente e tecnicamente verificabile, evitando sia formulazioni eccessivamente generiche sia riferimenti impliciti a tecnologie proprietarie.

Il rispetto del principio di neutralità tecnologica favorisce l'accesso al mercato e rafforza la concorrenza, contribuendo al perseguimento del principio del risultato.

Il capitolato come strumento di governo del contratto

Più che in altri ambiti, nel procurement di sistemi di IA la qualità del capitolato incide direttamente sulla capacità dell'amministrazione di governare il contratto. Un capitolato ben strutturato:

- riduce l'incertezza in fase di gara;
- migliora la comparabilità delle offerte;
- facilita il monitoraggio delle prestazioni;
- rafforza la posizione della PA nel rapporto contrattuale.

Al contrario, capitolati incompleti o ambigui tendono a trasferire sul momento esecutivo criticità che avrebbero potuto essere prevenute in fase di progettazione.

In tale prospettiva, la redazione del capitolato tecnico non deve essere considerata un adempimento formale, ma una **leva strategica attraverso cui l'amministrazione esercita il proprio ruolo di governo dell'innovazione tecnologica**, assicurando che l'adozione dell'Intelligenza Artificiale avvenga in modo controllato, sostenibile e coerente con l'interesse pubblico.

A titolo di esempio, si propone a seguire una struttura di capitolato. Tale struttura, pur non avendo carattere prescrittivo, rappresenta un riferimento operativo volto a supportare le amministrazioni nella redazione di capitolati tecnici coerenti con i principi del Codice dei contratti pubblici e con le peculiarità dei sistemi di Intelligenza Artificiale.

Sezione: Oggetto dell'appalto

La sezione contiene una descrizione chiara del servizio o della soluzione di IA richiesta, del contesto amministrativo di utilizzo e del suo perimetro funzionale.

Le finalità di procurement sono quelle di ridurre ambiguità interpretative e di migliorare la comparabilità delle offerte.

In questo modo, si mitigano il rischio di offerte non coerenti con il fabbisogno e il rischio di contenzioso.

Sezione: Obiettivi e risultati attesi

La sezione contiene una descrizione dei benefici attesi, degli indicatori di performance e degli impatti sui processi amministrativi.

La finalità di procurement è quella di orientare la gara al principio del risultato.

In questo modo, si mitiga il rischio di acquisizione di soluzioni tecnologiche prive di valore operativo.

Sezione: Architettura logica di riferimento

La sezione contiene una descrizione delle componenti del sistema (orchestratore, modelli, dati, applicativi) e dei requisiti di modularità e integrazione.

Le finalità di procurement sono quelle di rafforzare la governabilità e di prevenire dipendenze tecnologiche.

In questo modo, si mitiga il rischio di lock-in architetturale.

Sezione: Requisiti funzionali

La sezione contiene una descrizione di funzionalità minime richieste, casi d'uso e livelli di servizio.

La finalità di procurement è quella di garantire l'adeguatezza della soluzione al contesto operativo.

In questo modo, si mitiga il rischio di soluzioni sovradimensionate o inadeguate.

Sezione: Requisiti tecnici

La sezione contiene una descrizione di interoperabilità, standard, compatibilità infrastrutturale, scalabilità.

La finalità di procurement è quella di favorire l'accesso al mercato e la neutralità tecnologica.

In questo modo, si mitiga il rischio di riduzione della concorrenza.

Sezione: Gestione dei dati

La sezione contiene una descrizione di titolarità, accesso, qualità, sicurezza, portabilità, condizioni di riuso.

La finalità di procurement è quella di preservare il controllo pubblico sul patrimonio informativo.

In questo modo, si mitigano il rischio di dipendenza dal fornitore e il rischio di perdita di dati.

Sezione: Prestazioni e SLA

La sezione contiene una descrizione di metriche di accuratezza, disponibilità del servizio, tempi di risposta e affidabilità.

La finalità di procurement è quella di rendere verificabile l'adempimento contrattuale.

In questo modo, si mitiga il rischio di difficoltà nel monitoraggio.

Sezione: Sicurezza e conformità normativa

La sezione contiene una descrizione di protezione dei dati, cybersecurity, auditabilità e logging.

La finalità di procurement è quella di garantire conformità normativa e responsabilità amministrativa.

In questo modo, si mitigano i rischi di violazioni di sicurezza e i rischi legali.

Sezione: Trasparenza e documentazione

La sezione contiene una descrizione di obblighi di documentazione tecnica, spiegabilità proporzionata e accesso alle informazioni.

La finalità di procurement è quella di rafforzare controllo e rendicontabilità.

In questo modo, si mitiga il rischio di opacità del sistema.

Sezione: Governance ed evoluzione del sistema

La sezione contiene una descrizione di modalità di aggiornamento dei modelli, gestione delle modifiche, supporto tecnico.

La finalità di procurement è quella di governare l'evoluzione tecnologica.

In questo modo, si mitiga il rischio di obsolescenza rapida.

Sezione: Competenze e trasferimento di know-how

La sezione contiene una descrizione della formazione del personale, di affiancamento operativo e documentazione.

La finalità di procurement è quella di ridurre la dipendenza dal fornitore.

In questo modo, si mitiga il rischio di lock-in operativo.

Sezione: Condizioni di portabilità e uscita

La sezione contiene una descrizione di restituzione dei dati, migrazione e subentro.

La finalità di procurement è quella di garantire continuità amministrativa.

In questo modo, si mitiga il rischio di dipendenza irreversibile.

Sezione: Monitoraggio e reporting

La sezione contiene una descrizione di strumenti di controllo, report periodici, indicatori economici e operativi.

La finalità di procurement è quella di supportare la fase di esecuzione dell'appalto.

In questo modo, si mitiga il rischio di crescita incontrollata dei costi.

Tabella 10: struttura di capitolato

Sezione del capitolato	Contenuti essenziali	Finalità di procurement	Rischi mitigati
Oggetto dell'appalto	Descrizione chiara del servizio o della soluzione di IA richiesta, contesto amministrativo di utilizzo, perimetro funzionale	Ridurre ambiguità interpretative e migliorare la comparabilità delle offerte	Offerte non coerenti con il fabbisogno; contenzioso
Obiettivi e risultati attesi	Benefici attesi, indicatori di performance, impatti sui processi amministrativi	Orientare la gara al principio del risultato	Acquisizione di soluzioni tecnologiche prive di valore operativo
Architettura logica di riferimento	Descrizione delle componenti del sistema (orchestratore, modelli, dati, applicativi), requisiti di modularità e integrazione	Rafforzare la governabilità e prevenire dipendenze tecnologiche	Lock-in architetturale
Requisiti funzionali	Funzionalità minime richieste, casi d'uso, livelli di servizio	Garantire l'adeguatezza della soluzione al contesto operativo	Soluzioni sovradimensionate o inadeguate
Requisiti tecnici	Interoperabilità, standard, compatibilità infrastrutturale, scalabilità	Favorire l'accesso al mercato e la neutralità tecnologica	Riduzione della concorrenza
Gestione dei dati	Titolarità, accesso, qualità, sicurezza, portabilità, condizioni di riuso	Preservare il controllo pubblico sul patrimonio informativo	Dipendenza dal fornitore; perdita di dati
Prestazioni e SLA	Metriche di accuratezza, disponibilità del servizio, tempi di risposta, affidabilità	Rendere verificabile l'adempimento contrattuale	Difficoltà nel monitoraggio

Sezione del capitolato	Contenuti essenziali	Finalità di procurement	Rischi mitigati
Sicurezza e conformità normativa	Protezione dei dati, cybersecurity, auditabilità, logging	Garantire conformità normativa e responsabilità amministrativa	Violazioni di sicurezza; rischi legali
Trasparenza e documentazione	Obblighi di documentazione tecnica, spiegabilità proporzionata, accesso alle informazioni	Rafforzare controllo e rendicontabilità	Opacità del sistema
Governance ed evoluzione del sistema	Modalità di aggiornamento dei modelli, gestione delle modifiche, supporto tecnico	Governare l'evoluzione tecnologica	Obsolescenza rapida
Competenze e trasferimento di know-how	Formazione del personale, affiancamento operativo, documentazione	Ridurre la dipendenza dal fornitore	Lock-in operativo
Condizioni di portabilità e uscita	Restituzione dei dati, migrazione, subentro	Garantire continuità amministrativa	Dipendenza irreversibile
Monitoraggio e reporting	Strumenti di controllo, report periodici, indicatori economici e operativi	Supportare la fase di esecuzione	Crescita incontrollata dei costi

Criteri di aggiudicazione e valorizzazione della qualità

Nella definizione dei criteri di aggiudicazione, le amministrazioni dovrebbero ricorrere in modo sistematico all'offerta economicamente più vantaggiosa, in quanto maggiormente idonea a cogliere la multidimensionalità delle soluzioni di IA.

In tale ambito, dovrebbero essere valorizzati elementi quali:

- la qualità architetturale della soluzione;

- la sostenibilità economica di ciclo di vita;
- la scalabilità e la capacità evolutiva;
- la robustezza delle misure di sicurezza;
- le strategie di mitigazione del rischio;
- il grado di trasparenza e spiegabilità della soluzione proposta;
- la facilità di integrazione con l'ecosistema digitale dell'amministrazione.

Le valutazioni economiche possono essere utilmente supportate da indicatori di costo di ciclo di vita e, ove pertinente, da metriche come quella di costo livellato dell'Intelligenza Artificiale (LCOAI), utilizzate come strumenti di comparazione e supporto decisionale, e non come automatismi di aggiudicazione. Il prezzo iniziale, infatti, non dovrebbe costituire l'elemento prevalente di valutazione, soprattutto nei casi in cui una parte significativa della spesa sia destinata a manifestarsi durante la fase di esercizio.

L'adozione di criteri coerenti con una prospettiva di ciclo di vita contribuisce a orientare il mercato verso soluzioni maggiormente sostenibili e a ridurre il rischio di offerte caratterizzate da costi iniziali contenuti ma da elevati oneri operativi.

Strutturazione della base d'asta e prevedibilità dei costi

Un ulteriore profilo di attenzione riguarda la determinazione della base d'asta, che dovrebbe riflettere in modo realistico la struttura dei costi del servizio. Basi d'asta sottostimate possono compromettere la qualità delle offerte o generare tensioni nella fase di esecuzione, mentre basi d'asta non adeguatamente motivate possono ridurre l'efficacia del confronto competitivo.

In tale contesto, il ricorso a modelli di analisi di ciclo di vita può supportare l'amministrazione nella costruzione di stime economiche più robuste, migliorando la prevedibilità della spesa e la sostenibilità dell'investimento.

Centralità della fase di esecuzione contrattuale

Particolare attenzione deve essere riservata alla fase di esecuzione contrattuale, che nei sistemi di IA assume un ruolo centrale. A differenza di molte forniture tradizionali, infatti, una quota rilevante del

valore del servizio si realizza nel corso dell'esecuzione, attraverso attività di monitoraggio, aggiornamento, manutenzione ed evoluzione del sistema.

In tale fase, il monitoraggio dei costi effettivi e dei livelli di utilizzo del sistema consente di verificare dinamicamente le ipotesi economiche formulate in sede di gara, anche attraverso indicatori derivati dal costo di ciclo di vita e dal LCOAI, in coerenza con il quadro metodologico delineato nel Capitolo 3.

L'amministrazione dovrebbe pertanto prevedere:

- strumenti di controllo continuo delle prestazioni;
- meccanismi di rendicontazione trasparenti;
- indicatori economici e operativi misurabili;
- clausole di revisione coerenti con la disciplina vigente;
- dispositivi contrattuali idonei a governare l'evoluzione tecnologica.

Tali presìdi risultano essenziali per prevenire scostamenti rispetto agli obiettivi pubblici, contenere il rischio di crescita incontrollata dei costi e garantire la continuità dei servizi.

Gare come strumento di governo dell'evoluzione tecnologica

Le gare per l'approvvigionamento di sistemi di IA dovrebbero essere concepite non solo come strumenti di selezione del fornitore, ma come leve di governo dell'evoluzione tecnologica dell'amministrazione. Una progettazione attenta consente infatti di costruire un assetto contrattuale capace di accompagnare l'ente lungo l'intero ciclo di vita della soluzione.

In tale prospettiva, l'amministrazione è chiamata a trovare un equilibrio tra stabilità contrattuale e flessibilità evolutiva, evitando sia modelli eccessivamente rigidi sia configurazioni che possano compromettere la prevedibilità della spesa.

In definitiva, la qualità delle gare per sistemi di IA dipende in larga misura dalla capacità dell'amministrazione di integrare valutazioni tecnologiche, economiche e organizzative in un disegno coerente. Solo attraverso una progettazione consapevole è possibile garantire che l'adozione

dell'Intelligenza Artificiale avvenga in modo sostenibile, governabile e pienamente coerente con l'interesse pubblico

Le procedure aperte e ristrette continuano a rappresentare lo strumento ordinario di approvvigionamento anche nel procurement di sistemi di Intelligenza Artificiale, in particolare nei casi in cui il fabbisogno sia chiaramente definito e il mercato offra soluzioni tecnologicamente mature e comparabili. L'utilizzo di accordi quadro può garantire maggiore adattabilità della spesa nei casi caratterizzati da elevata variabilità dei fabbisogni o da rapida evoluzione tecnologica

Tuttavia, in presenza di specifiche condizioni — quali un fabbisogno non pienamente determinato, un'elevata incertezza tecnologica, la necessità di sperimentazione preliminare, una domanda difficilmente stimabile o una forte componente innovativa — le amministrazioni possono valutare il ricorso agli strumenti di procurement più flessibili previsti dall'ordinamento.

In tali contesti, istituti quali il dialogo competitivo o la procedura competitiva con negoziazione possono favorire un confronto strutturato con il mercato e consentire una più accurata definizione delle soluzioni progettuali. Analogamente, il partenariato per l'innovazione e gli appalti pre-commerciali risultano particolarmente idonei quando l'esigenza pubblica richiede attività di ricerca e sviluppo non ancora pienamente disponibili sul mercato.

La scelta dello strumento di affidamento dovrebbe pertanto essere effettuata in modo proporzionato alle caratteristiche del progetto, evitando approcci automatici e privilegiando una valutazione preliminare che tenga conto del livello di definizione del fabbisogno, della maturità del mercato e del grado di innovazione richiesto.

5.4 Interoperabilità e cooperazione tra amministrazioni

L'interoperabilità e la cooperazione tra Pubbliche Amministrazioni rappresentano fattori abilitanti essenziali per un uso efficace, sostenibile e scalabile dei sistemi di Intelligenza Artificiale. In assenza di un adeguato coordinamento, il rischio è quello di assistere a una proliferazione di soluzioni isolate, sviluppate per rispondere a esigenze specifiche ma prive di una reale capacità di integrazione con l'ecosistema pubblico complessivo.

La frammentazione tecnologica e la duplicazione degli investimenti costituiscono criticità particolarmente rilevanti in un contesto caratterizzato da rapida evoluzione delle tecnologie e da costi di sviluppo spesso elevati. L'adozione di approcci non coordinati può infatti determinare inefficienze, ridurre le economie di scala e compromettere la sostenibilità complessiva degli investimenti pubblici in IA.

In tale prospettiva, interoperabilità e cooperazione non devono essere considerate obiettivi accessori, ma elementi strutturali delle strategie di procurement e trasformazione digitale.

Interoperabilità come principio strategico

L'interoperabilità deve essere interpretata non solo come un requisito tecnico, ma come un principio organizzativo e istituzionale che orienta la progettazione dei sistemi e le modalità di collaborazione tra enti. Essa implica la capacità dei sistemi di IA di integrarsi con le piattaforme esistenti, di scambiare dati in modo sicuro e di operare in maniera coordinata tra diverse amministrazioni.

Un approccio realmente interoperabile consente di:

- evitare duplicazioni funzionali;
- favorire la circolazione delle informazioni;
- migliorare la qualità dei servizi;
- ridurre i costi di integrazione;
- accelerare l'adozione delle innovazioni.

L'interoperabilità dovrebbe pertanto essere considerata sin dalle fasi di programmazione e progettazione del procurement, evitando che soluzioni sviluppate in modo autonomo diventino difficilmente integrabili in un secondo momento.

Dal coordinamento tecnico alla governance condivisa

Nei sistemi di IA, l'interoperabilità assume una dimensione più ampia rispetto alle tradizionali integrazioni applicative. Essa riguarda non solo lo scambio di dati, ma anche la compatibilità delle architetture, l'allineamento dei modelli di governance e la coerenza delle scelte tecnologiche.

Ciò richiede un progressivo passaggio da logiche di coordinamento tecnico a forme più evolute di governance condivisa, nelle quali le amministrazioni collaborano alla definizione di standard, metodologie e pratiche operative comuni.

Una governance coordinata può contribuire a ridurre le asimmetrie tecnologiche tra enti e a rafforzare la capacità complessiva del settore pubblico di governare l'innovazione.

In ossequio al principio di sussidiarietà, tale governance, con riferimento alle soluzioni dispiegate dagli enti locali, deve tener conto del ruolo di intermediazione tecnologica che le Regioni possono svolgere nei confronti delle PA del territorio.

Laddove le Regioni si pongano come erogatori di servizi SaaS o di prototipazione di applicazioni di IA, esse possono adottare opportuni strumenti di repository della knowledge base finalizzati ad assicurare meccanismi di sovranità digitale, isolamento e protezione dei dati utilizzati per operazioni di addestramento, testing, fine tuning, etc. anche per conto di PA locali aderenti.

Cooperazione come leva di sostenibilità

La cooperazione inter-amministrativa rappresenta una leva fondamentale per migliorare la sostenibilità economica degli investimenti in IA. Attraverso iniziative congiunte, le amministrazioni possono condividere i costi di sviluppo, ridurre i rischi associati all'adozione di nuove tecnologie e beneficiare di competenze distribuite.

Tale approccio risulta pienamente coerente con una prospettiva di ciclo di vita degli investimenti e può contribuire a ottimizzare il rapporto tra risorse impiegate e valore generato.

Inoltre, la cooperazione può rafforzare il potere negoziale del settore pubblico nei confronti del mercato, favorendo condizioni contrattuali più vantaggiose e orientando l'offerta verso soluzioni maggiormente interoperabili. In tale prospettiva, assume particolare rilievo la dimensione delle iniziative di acquisto. Per i sistemi di Intelligenza Artificiale — spesso caratterizzati da elevati costi fissi, forte dipendenza dai dati e necessità di competenze specialistiche — è opportuno prevedere forme di aggregazione almeno a livello regionale o provinciale, soprattutto quando consentono di valorizzare economie di scala e di ridurre la frammentazione della domanda pubblica.

La scelta del livello più adeguato al quale collocare l'iniziativa di procurement dovrebbe pertanto essere valutata in relazione al contesto territoriale, al settore di intervento e al grado di omogeneità dei fabbisogni, evitando sia una dispersione delle iniziative sia modelli eccessivamente centralizzati non coerenti con le specificità operative delle singole amministrazioni.

Aggregazioni di acquisto e sistema a rete del procurement pubblico

Le aggregazioni di acquisto tra amministrazioni, e in particolare le centrali regionali e provinciali, costituiscono una leva strategica per rafforzare l'efficienza del procurement pubblico e migliorare la sostenibilità della spesa, soprattutto in ambiti caratterizzati da elevata complessità tecnologica e da dinamiche di mercato in rapida evoluzione quali i sistemi di Intelligenza Artificiale.

Nel contesto italiano, tali aggregazioni operano all'interno di un sistema a rete fondato sulla cooperazione tra la centrale di committenza nazionale — Consip — e i soggetti aggregatori regionali. Questo modello organizzativo mira a coniugare i benefici della centralizzazione degli acquisti con la capacità di intercettare i fabbisogni specifici dei territori, favorendo al contempo una maggiore uniformità nelle condizioni contrattuali e nei livelli di servizio.

I soggetti aggregatori regionali, quali le centrali di committenza qualificate istituite a livello territoriale, svolgono un ruolo crescente nel supportare le amministrazioni nella gestione delle procedure di gara e nella definizione di strumenti contrattuali idonei a soddisfare fabbisogni complessi. Attraverso tali strutture, le amministrazioni possono beneficiare di competenze specialistiche, ridurre i costi di gestione delle procedure e accedere a condizioni economiche generalmente più favorevoli grazie alle economie di scala.

La normativa vigente prevede, per specifiche categorie merceologiche, l'obbligo di ricorrere alle convenzioni o agli accordi quadro stipulati dai soggetti aggregatori o da Consip, limitando il ricorso a procedure autonome. Tale impostazione risponde all'esigenza di razionalizzare la spesa pubblica, ridurre la frammentazione degli acquisti e rafforzare il potere negoziale della domanda pubblica.

In questa prospettiva si inserisce anche il Piano integrato predisposto dal Ministero dell'Economia e delle Finanze, volto ad armonizzare le iniziative di acquisto dei diversi soggetti aggregatori e a garantire una copertura coordinata delle principali categorie merceologiche individuate a livello nazionale. Un approccio programmatorio condiviso consente infatti di migliorare la prevedibilità della domanda pubblica e di favorire una maggiore stabilità del mercato.

Tra gli strumenti più rilevanti utilizzati nell'ambito delle aggregazioni figura l'accordo quadro, che consente a più stazioni appaltanti di definire preventivamente condizioni di fornitura — quali prezzi, livelli di servizio e caratteristiche tecniche — per un determinato periodo temporale, mantenendo al contempo un adeguato grado di flessibilità nell'attivazione dei contratti applicativi. Tale strumento risulta particolarmente coerente con la natura evolutiva dei sistemi di IA, permettendo di gestire fabbisogni variabili e di accompagnare nel tempo l'aggiornamento delle soluzioni tecnologiche.

Le aggregazioni di acquisto non producono benefici esclusivamente sul piano economico, ma possono anche contribuire allo sviluppo dell'ecosistema produttivo, favorendo la partecipazione alle gare di operatori qualificati e stimolando la crescita di filiere tecnologiche nazionali e territoriali. In presenza di una domanda pubblica strutturata e prevedibile, il mercato è infatti maggiormente incentivato a investire in soluzioni innovative e sostenibili.

Alla luce di tali elementi, le amministrazioni dovrebbero valutare in modo sistematico le opportunità offerte dagli strumenti di procurement aggregato, soprattutto nei casi in cui la complessità tecnica, l'entità degli investimenti o la necessità di competenze specialistiche rendano poco efficiente il ricorso a procedure isolate. L'aggregazione, se adeguatamente governata, rappresenta pertanto non solo uno strumento di razionalizzazione della spesa, ma anche un fattore abilitante per un'adozione più matura e consapevole dell'Intelligenza Artificiale nel settore pubblico.

Si descrivono a seguire alcuni scenari in presenza dei quali aggregare gli acquisti di sistemi di Intelligenza Artificiale.

Scenario A - Fabbisogni comuni tra più amministrazioni

In questo scenario l'aggregazione evita duplicazioni progettuali e frammentazione della domanda.

I principali benefici attesi sono ravvisabili nel conseguimento di economie di scala e in una maggiore standardizzazione.

Gli strumenti consigliati sono accordi quadro multi-ente e convenzioni.

Scenario B - Elevata complessità tecnologica

In questo scenario l'aggregazione è utile perché l'elevata complessità tecnologica richiede competenze specialistiche non sempre disponibili nelle singole PA.

I principali benefici attesi sono ravvisabili in una migliore qualità tecnica delle procedure e nella riduzione del rischio di errori progettuali.

Gli strumenti consigliati sono centrali di committenza e il ricorso a soggetti aggregatori.

Scenario C - Investimenti infrastrutturali rilevanti

In questo scenario l'aggregazione rafforza il potere negoziale della domanda pubblica.

I principali benefici attesi sono ravvisabili in prezzi più competitivi e condizioni contrattuali più favorevoli.

Gli strumenti consigliati sono gare aggregate e partenariati.

Scenario D - Servizi di IA riusabili o scalabili

In questo scenario l'aggregazione è utile perché le stesse soluzioni possono essere adottate da più enti con adattamenti limitati.

I principali benefici attesi sono ravvisabili nella riduzione dei tempi di adozione e in una maggiore interoperabilità.

Gli strumenti consigliati sono piattaforme condivise e accordi quadro evolutivi.

Scenario E - Necessità di standard tecnici comuni

In questo scenario l'aggregazione è utile in quanto favorisce l'integrazione tra sistemi e la cooperazione inter-amministrativa.

I principali benefici attesi sono ravvisabili in ecosistemi digitali più coerenti e minori costi di integrazione.

Lo strumento consigliato è il procurement coordinato.

Scenario F - Rischio di lock-in tecnologico

In questo scenario l'aggregazione è utile perché una domanda aggregata aumenta la contendibilità del mercato.

I principali benefici attesi sono ravvisabili in una maggiore sostituibilità dei fornitori e in una migliore governabilità.

Lo strumento consigliato è quello delle procedure competitive centralizzate.

Scenario G - Mercati emergenti o poco maturi

In questo scenario l'aggregazione è utile perché aggregare la domanda riduce l'asimmetria informativa.

I principali benefici attesi sono ravvisabili in offerte più strutturate e maggiore trasparenza.

Lo strumento consigliato è quello di consultazioni di mercato congiunte.

Tabella 11: Quando aggregare gli acquisti di sistemi di Intelligenza Artificiale

Scenario	Perché favorire l'aggregazione	Benefici attesi	Strumenti consigliati
Fabbisogni comuni tra più amministrazioni	Evita duplicazioni progettuali e frammentazione della domanda	Economie di scala; maggiore standardizzazione	Accordi quadro multi-ente; convenzioni
Elevata complessità tecnologica	Richiede competenze specialistiche non sempre disponibili nelle singole PA	Migliore qualità tecnica delle procedure; riduzione del rischio di errori progettuali	Centrali di committenza; soggetti aggregatori

Scenario	Perché favorire l'aggregazione	Benefici attesi	Strumenti consigliati
Investimenti infrastrutturali rilevanti	L'aggregazione rafforza il potere negoziale della domanda pubblica	Prezzi più competitivi; condizioni contrattuali più favorevoli	Gare aggregate; partenariati
Servizi di IA riusabili o scalabili	Le stesse soluzioni possono essere adottate da più enti con adattamenti limitati	Riduzione dei tempi di adozione; maggiore interoperabilità	Piattaforme condivise; accordi quadro evolutivi
Necessità di standard tecnici comuni	Favorisce l'integrazione tra sistemi e la cooperazione inter-amministrativa	Ecosistemi digitali più coerenti; minori costi di integrazione	Procurement coordinato
Rischio di lock-in tecnologico	Una domanda aggregata aumenta la contendibilità del mercato	Maggiore sostituibilità dei fornitori; migliore governabilità	Procedure competitive centralizzate
Mercati emergenti o poco maturi	Aggregare la domanda riduce l'asimmetria informativa	Offerte più strutturate; maggiore trasparenza	Consultazioni di mercato congiunte

Standardizzazione e apertura tecnologica

L'interoperabilità richiede l'adozione di standard aperti e di architetture modulari, capaci di facilitare l'integrazione tra sistemi diversi e di prevenire situazioni di dipendenza tecnologica. Soluzioni eccessivamente proprietarie possono infatti ostacolare la cooperazione e limitare la possibilità di riuso.

Le amministrazioni devono pertanto orientare il procurement verso modelli tecnologici che favoriscano:

- la portabilità dei dati;
- la sostituibilità delle componenti;
- la trasparenza delle interfacce;
- la compatibilità con infrastrutture esistenti.

Interoperabilità e gestione del rischio

Un adeguato livello di interoperabilità contribuisce anche alla gestione del rischio. Sistemi progettati per operare in modo isolato possono risultare più vulnerabili sotto il profilo operativo e più difficili da sostituire in caso di criticità.

Al contrario, architetture aperte e integrate favoriscono la resilienza del sistema e riducono l'esposizione a interruzioni del servizio.

Sfide organizzative e culturali

È opportuno riconoscere che la cooperazione inter-amministrativa non rappresenta soltanto una sfida tecnologica, ma implica anche un'evoluzione organizzativa e culturale. La condivisione di soluzioni richiede infatti fiducia istituzionale, allineamento degli obiettivi e disponibilità ad adottare modelli di governance più collaborativi.

Le amministrazioni sono pertanto chiamate a sviluppare competenze non solo tecniche, ma anche relazionali e strategiche, capaci di sostenere percorsi di innovazione condivisa.

Equilibrio tra autonomia e coordinamento

La promozione dell'interoperabilità deve essere perseguita nel rispetto dell'autonomia organizzativa delle singole amministrazioni. L'obiettivo non è uniformare rigidamente le scelte tecnologiche, ma favorire un livello di compatibilità tale da consentire integrazione e cooperazione senza compromettere la capacità degli enti di rispondere alle proprie specificità.

Il raggiungimento di tale equilibrio rappresenta uno dei principali indicatori di maturità del sistema pubblico.

Strumenti:

- Strumento A: Termini e definizioni

- Strumento B: Guida al capitolato tecnico

- Strumento C: Esempio applicazione LCOAI