Costituzione dell'Intelligenza Artificiale Aziendale

Riccardo Bovetti

Who am I? | LinkedIn | All you need is thought

9 aprile 2026

Sommario

La presente Costituzione è al tempo stesso un testo di principio e un portale di accesso operativo a tutta la "conoscenza" che ho accumulato in questi quasi tre anni di lavoro a fianco delle organizzazioni nei processi di A(i)doption. Ogni articolo enuncia un principio fondante del governo dell'AI in azienda ed indica contestualmente a quale fase e strumento del percorso A(I)doption quel principio si traduce in azione concreta. Il framework A(I)doption articola il percorso di trasformazione AI in quattro fasi integrate (AI Maturity Model, Upskilling & Adoption, Discovery Use Case, Pilot & Transform) ed in dieci step operativi che trasformano le condizioni di partenza in risultati misurabili. La Costituzione non sostituisce questo percorso: lo fonda, lo legittima stabilendone i confini. Il presente documento nasce da una domanda semplice nella formulazione, ma radicale nelle implicazioni: è sufficiente una policy per governare l'intelligenza artificiale in azienda? La risposta che emerge dall'analisi comparata dei modelli di adozione più avanzati è scevra d'ogni equivoco: è dannatamente indispensabile, ma non è sufficiente. Una policy regola comportamenti, accessi, diritti e processi. Una costituzione, invece, stabilisce i principi che precedono ed anticipano (quasi come un quadro etico di riferimento) qualsiasi regola, i diritti che nessuna norma operativa può comprimere, i poteri che devono essere riconosciuti e bilanciati, e le garanzie che rendono il sistema legittimo agli occhi di chi lo abita e lo attraversa. La differenza non è di forma: è di natura. Questo testo si ispira consapevolmente alla struttura della nostra Costituzione italiana, non per esercizio retorico, ma perché quella struttura ha dimostrato di saper tenere insieme, in modo duraturo e intelligente, visione e norma con principi e ordinamento nel rispetto di diritti e doveri. La stessa architettura è ciò di cui le organizzazioni hanno bisogno quando l'AI smette di essere un progetto e diventa un regime operativo permanente. La struttura adottata, costituita da Preambolo, Principi fondamentali, Parte I sui diritti e doveri, Parte II sull'ordinamento e sul ciclo di vita dei sistemi AI, Disposizioni finali, è volutamente calibrata per anticipare la maturità organizzativa, non per fotografarla nella sua essenza. Il tono è istituzionale ma non per forza notarile. La provocazione risiede nella tesi: l'AI in azienda è una questione di ordinamento prima ancora che di tecnologia.

Indice

Preambolo

L'intelligenza artificiale è entrata nell'impresa. Come strumento (con qualche secchiata di licenze comprate a caso), come progetto pilota o come sperimentazione di laboratorio "permanente": ma è oramai diventata, silente, forza operativa che ridistribuisce attenzione, velocità, capacità di decisione, produzione di valore e allocazione del rischio. Chi la governa acquisisce vantaggio competitivo, efficienza ed inattesa efficacia. Chi la subisce senza regole espone l'organizzazione a derive di irresponsabilità, dipendenza acritica e resa cognitiva fino alla potenziale perdita di controllo sui propri processi fondamentali. Il paradosso che molte organizzazioni vivono oggi è emblematico: le persone percepiscono da subito dei "miglioramenti" (perché i tempi di esecuzione, soprattutto perché mai prima misurati si riducono). La familiarità con gli strumenti cresce rapidamente ed il singolo arriva a non poterne più fare "a meno" ma l'impatto strutturale sull'organizzazione resta limitato. Quando mancano governance, processi, cultura condivisa e fiducia sistemica la distanza tra performance individuale e trasformazione organizzativa si amplifica. E questo gap non si colma con un barile di nuove licenze o con il tentativo di "acquisizione" di nuovi strumenti: si colma con un carta, penna e calamaio con le quali si scrive un ordinamento. La presente Costituzione stabilisce i principi ultimi (o primi, in quanto principi) dell'AI aziendale, i diritti e i doveri degli attori che vi partecipano, i meccanismi attraverso cui l'AI viene legittimata, governata e, quando necessario, evitata, limitata o dismessa. Ogni altro necessario strumento di governance (ovverosia il Manifesto, la Policy, il Target Operating Model, i framework di compliance normativa) trova in questo testo il proprio fondamento e proprio ambito insieme al proprio limite. L'azienda che la adotta afferma che l'AI è una questione di ordinamento prima ancora che di tecnologia, e si assume la responsabilità di costruire un ecosistema in cui il valore generato dall'intelligenza artificiale deve essere reale e per questo deve diventare (in qualche modo misurabile).

Principi Fondamentali

Art. 1 — Finalità, centralità della persona e responsabilità indelegabile

L'intelligenza artificiale dovrebbe essere adottata dalle organizzazioni per aumentare capacità, qualità, sicurezza, competitività e apprendimento collettivo. Essa non costituisce (nella sua essenza, nella sua assenza e nella sua definizione) un fine in sé, ma una leva al servizio della strategia aziendale e del valore generato per le persone, i clienti, i partner e la comunità. Ogni sistema AI dovrebbe poter dimostrare, in modo verificabile, il proprio contributo a questi obiettivi. La persona (dipendente, collaboratore, cliente, cittadino) è il centro della decisione, della responsabilità della azione (e reazione) e della relazione. L'AI può amplificare le capacità umane, supportare il giudizio e accelerare l'esecuzione, ma non può sostituire la responsabilità morale e professionale delle persone, né ridurre l'essere umano a semplice terminale di esecuzione, a oggetto opaco di valutazione automatizzata, o ad anello passivo di un processo che non comprende non

governa e non ha contribuito a definire. La responsabilità degli atti, degli output e delle decisioni assistite o generate dall'AI resta sempre e integralmente in capo all'organizzazione e alle persone fisiche (umani, dotati sperabilmente di attributi di intelligenza) che le approvano, le utilizzano, le autorizzano o le negano. Non deve essere ammessa alcuna forma di deresponsabilizzazione per via algoritmica (ci manca solo più questa fattispecie, come se non ne avessimo già tante di scuse di deresponsabilizzazione): il fatto che una decisione sia stata supportata o prodotta da un sistema AI non riduce né trasferisce la responsabilità umana sugli esiti di quella decisione. La finalità dell'AI non può essere per sua natura dichiarativa, essa è naturalmente induttiva e si costruisce collegando ogni iniziativa agli obiettivi di business prima di qualsiasi scelta tecnologica affermando i principi nel Manifesto.

Art. 2 — Trasparenza, contestabilità e tutela del patrimonio semantico ed informativo

Ogni uso rilevante dell'AI dovrebbe essere riconoscibile nella sua natura, spiegabile in misura proporzionata al rischio e agli impatti, e contestabile attraverso un giudizio umano effettivo e non meramente formale. La trasparenza non è un requisito opzionale di comunicazione esterna: è una condizione strutturale di legittimità. Nessun sistema AI che opera in modo opaco e incontestabile può essere considerato conforme a questa Costituzione (e con questo statement potremmo, per il momento chiuderla qui ...). L'adozione dell'AI non può compromettere la riservatezza, la sicurezza, la proprietà intellettuale, la coerenza e l'integrità del patrimonio informativo dell'impresa (in termini di organizzazioni e di persone), dei clienti e di tutti i partecipanti alla "relazione" strutturale con l'impresa stessa. I dati sono una risorsa strategica, non una materia prima infinitamente consumabile. Il loro utilizzo nei sistemi AI è sempre subordinato a base giuridica, necessità, minimizzazione e controllo del rischio di esposizione al fine di preservarne il valore semantico ed epistemologico. I meccanismi Trasparenza e tutela del dato non sono valori astratti: essi devono corrispondere a regole operative nel Manifesto e nella Policy di utilizzo dell'AI.

Art. 3 — Proporzionalità del rischio ed equità

Il livello di requisiti, vincoli, valutazioni, autorizzazioni, controlli, tracciabilità e presidio umano applicati a un sistema AI è direttamente proporzionale al rischio che quel sistema comporta per le persone, i processi, i clienti e la reputazione dell'organizzazione. L'approccio basato sul rischio non è una semplificazione amministrativa: è il meccanismo che consente di innovare responsabilmente, concentrando l'attenzione di governance sui sistemi che la meritano di più. L'AI aziendale dovrebbe essere progettata, anticipatamente valutata e costantemente monitorata per prevenire ogni forma di bias sistematico che produca discriminazione, disparità di trattamento ingiustificata o lesione della dignità delle persone. La qualità degli output AI non si misura solo in termini di accuratezza tecnica, ma anche di equità dei risultati. L'organizzazione si deve impegnare a rilevare, documentare e rimuovere o mitigare i bias nei propri sistemi, con attenzione

prioritaria a quelli che impattano direttamente su persone. La proporzionalità al rischio è il principio fondante del framework di compliance all'AI Act di cui noi abitanti dell'Unione Europea siamo fortunati di poter disporre. E' responsabilità dell'azienda istituire un inventario, condurre risk assessment ed adottare pratiche di governance continua che lo rendano operativo.

Art. 4 — Competenza diffusa e consapevolezza critica

L'uso responsabile dell'AI richiede formazione, disciplina intellettuale e consapevolezza critica derivante dalla conoscenza dei meccanismi di funzionamento. Nessuna diffusione dell'AI dovrebbe essere considerata legittima senza un investimento proporzionato nello sviluppo delle competenze delle persone che la devono utilizzare, progettare valutare o governare. La competenza non è un prerequisito opzionale: è una condizione di sicurezza operativa, di qualità degli output a tutela dell'organizzazione e delle sue persone. L'alfabetizzazione AI è insieme un diritto/dovere dei lavoratori e un dovere dell'organizzazione, che vi dovrebbe rispondere con programmi strutturati, accessibili e continuamente aggiornati. Il principio di competenza diffusa si traduce in percorsi Academy differenziati per ruolo e livello di rischio, e in un curriculum minimo di AI literacy da prevedere per tutta la popolazione aziendale.

Art. 5 — Continuità, sostenibilità e resilienza

L'AI deve essere adottata con criteri di continuità operativa, monitoraggio permanente, sostenibilità economica e attenzione agli impatti ambientali e sociali. I sistemi AI non dovrebbero essere introdotti se non è stata prevista la loro manutenzione, il loro aggiornamento progressivo e la gestione delle situazioni di malfunzionamento o di dismissione programmata. La resilienza dell'organizzazione non può dipendere da sistemi AI privi di piani di continuità: la dipendenza tecnologica non governata è un rischio operativo di primo ordine. La sostenibilità non si decide a valle: si progetta nella fase di scaling, quando l'industrializzazione della soluzione deve essere monitorata, governata e replicabile.

Art. 6 — Evoluzione governata

L'intelligenza artificiale è una tecnologia in rapida e continua trasformazione. Questa Costituzione riconosce che le regole di oggi potrebbero essere insufficienti o inadeguate domani, e istituisce per questo un principio di revisione obbligatoria periodica dell'intero sistema di governance. Nessuna scelta tecnologica così come nessuna policy, nessun processo operativo può considerarsi definitivo: l'intera struttura deve evolversi in coerenza con la maturità tecnologica, normativa e organizzativa dell'impresa. La revisione non è una debolezza della Costituzione: è la prova che essa è viva. L'evoluzione governata dovrebbe iniziare sempre con un bagno di realtà in forma di misurazione. Al fine di poter definire una baseline da cui ogni revisione possa partire è necessario condurre un assessment maturità percorrendo le sette dimensioni definitorie del Maturity Model e ripetere con frequenza stabilita questo triage organizzativo strutturato.

Parte I — Diritti e doveri dell'ecosistema AI aziendale

Titolo I — Rapporti con le persone e con il lavoro

Art. 7 — Diritti fondamentali delle persone nell'ecosistema AI

Ogni dipendente, collaboratore e funzione aziendale dovrebbe avere il diritto di sapere quando un processo, un contenuto, una raccomandazione o una decisione che lo riguarda è stata prodotta o significativamente influenzata da un sistema AI. Questo diritto alla conoscibilità non ammette eccezioni legate alla complessità tecnica: dovrebbe essere garantito attraverso meccanismi di comunicazione adeguati alla comprensione umana, non solo alla correttezza formale. Chiunque sia impattato in modo rilevante da un output o da una raccomandazione dell'AI dovrebbe avere diritto a un riesame umano effettivo e non meramente formale. Il lavoratore dovrebbe avere inoltre il diritto di ricevere formazione adeguata prima di essere esposto all'utilizzo di sistemi AI nel proprio contesto operativo, ed altresì di ricevere aggiornamenti periodici che tengano il passo con l'evoluzione degli strumenti e dei rischi connessi. I diritti alla conoscenza ed alla formazione trovano risposta strutturale nei percorsi Academy e nel curriculum minimo: non opzioni facoltative, ma standard di adozione.

Art. 8 — Doveri degli utenti e divieto di automazione irresponsabile

Ogni utente che utilizza un sistema AI dovrebbe avere il dovere ineludibile di verificare accuratezza, coerenza, pertinenza, completezza, tono, conformità normativa e impatti degli output prodotti, prima di qualsiasi utilizzo interno o esterno. Gli output AI dovrebbero sempre essere trattati come bozze soggette a revisione critica, non come prodotti finiti. A questo dovere di verifica puntuale si affianca un dovere di aggiornamento continuo delle proprie competenze. Dovrebbe essere vietata ogni forma di utilizzo dell'AI che produca dipendenza acritica dagli output o produzione di contenuti plausibili ma non corretti. Questo divieto si dovrebbe applicare indipendentemente dal fatto che l'esito dannoso sia intenzionale o derivi da negligenza (ed anzi, nel caso della negligenza dovrebbe esser ancor maggiormente considerato grave). I doveri degli utenti si dovrebbero rendere esecutivi attraverso un TOM (target operative model) perchè ruoli, responsabilità e processi non possono essere considerati impliciti, devono essere espliciti.

Titolo II — Rapporti con dati, strumenti e casi d'uso

Art. 9 — Classificazione degli strumenti, regime dei dati e Registro AI

Gli strumenti AI disponibili nell'organizzazione dovrebbero essere classificati in quattro categorie: approvati per uso generale, approvati con limitazioni specifiche, in fase di valutazione, vietati. Nessuno strumento può essere utilizzato al di fuori della classe assegnata. Negli strumenti non approvati dovrebbe essere categoricamente vietato inserire dati personali, informazioni riservate, documenti di clienti, proprietà intellettuale protetta o qualsiasi informazione sensibile relativa all'organizzazione o ai suoi stakeholder. L'organizzazione dovrebbe mantenere ed aggiornare un

inventario centrale (una sorta di registro AI, fosse per me rigorosamente da compilare con carta e penna) di tutti i sistemi AI utilizzati, sviluppati o valutati, con indicazione di finalità d'uso, funzione owner, classificazione di rischio, stato del processo di valutazione ed esito decisionale. Il Registro diventa strumento fondamentale di trasparenza interna e di compliance normativa: la sua tenuta è attività permanente e obbligatoria, non un adempimento da svolgere alla vigilia di un audit.

Titolo III — Rapporti con clienti, partner, mercato e comunità

Art. 10 — Trasparenza esterna, equità e responsabilità nella catena del valore

L'organizzazione dovrebbe comunicare in modo chiaro, proporzionato e coerente con il suo stile e modo comunicativo il proprio utilizzo dell'AI quando questo è rilevante per clienti, partner, candidati, fornitori, comunità di riferimento o autorità di vigilanza. La trasparenza verso l'esterno non è solo un obbligo normativo: è un fattore competitivo e di fiducia, che si esprime attraverso clausole contrattuali standard, politiche di comunicazione pubblica e procedure strutturate di risposta alle richieste di informazione. Le richieste dei clienti di limitare, escludere o disciplinare l'uso dell'AI nell'ambito dei servizi loro erogati devono essere formalizzate, rese operative con tempestività e rispettate integralmente. Nessun sistema AI di terzi può essere adottato senza un processo di due diligence proporzionato al rischio: la responsabilità non si esternalizza con il fornitore. La comunicazione esterna sull'AI non si improvvisa: il Manifesto dovrebbe essere il documento con cui l'organizzazione dichiara pubblicamente il proprio approccio, i propri valori e i propri limiti nell'uso dell'AI.

Parte II — Ordinamento dell'AI aziendale

Titolo I — Organi della Governance

Art. 11 — Struttura di governance: indirizzo, coordinamento e presidio locale

La governance dell'AI aziendale, nella sua forma più estesa, si può articolare su tre livelli tra loro complementari e interdipendenti. Il Comitato Strategico AI è l'organo supremo di indirizzo: definisce priorità, criteri di investimento, limiti di rischio accettabile e principi etici a livello di Gruppo. Presiede l'allineamento tra le iniziative AI e la strategia aziendale complessiva, e promuove la revisione periodica di questa Costituzione. L'AI Center of Excellence (AI CoE) è l'organo tecnico-metodologico centrale: definisce standard, metodi e linee guida operative; supporta i progetti nelle funzioni; presidia la coerenza tecnica, metodologica e normativa dell'intero portafoglio; mantiene il Registro AI. Ad esso si affianca il Comitato Operativo AI, che coordina l'esecuzione delle iniziative approvate, monitora gli avanzamenti e risolve i blocchi interfunzionali. I Comitati locali e i Change Agents sono i nodi periferici della governance: raccolgono use case dalle funzioni, facilitano l'adozione operativa, accompagnano il cambiamento e riportano al centro criticità, risultati e opportunità emergenti. Sono la garanzia che la governance non rimanga un

esercizio di vertice, ma si radichi nei comportamenti quotidiani dell'organizzazione. La struttura di governance non è un organigramma formale e richiede chiarezza dei ruoli e di responsabilità, non sovrastrutture sovradimensionate in termini di risorse. Può essere molto semplificata e snella purché rappresenti tutte le diverse responsabilità. É importante che sia definita in un TOM che la rende operativa, definendo composizione dei comitati, responsabilità dei Change Agents, processi decisionali e strumenti di coordinamento.

Titolo II — Il ciclo di vita dei sistemi AI

Art. 12 – Il dato come fondamento operativo dell'AI

Nessun sistema AI produce valore superiore a quello complessivo della qualità dei dati su cui opera. Il dato non è un prerequisito tecnico dell'AI: è la sua materia prima cognitiva, e come tale va governato, curato e valorizzato prima ancora che qualsiasi modello venga addestrato, integrato o messo in produzione. Un'organizzazione che investe in AI senza aver prima investito nella qualità, coerenza e accessibilità del proprio patrimonio informativo sta costruendo su fondamenta instabili, con risultati prevedibilmente inaffidabili. Ai fini Costituzionali, il patrimonio di dati aziendale si articola in quattro domini distinti, ciascuno con proprie implicazioni di governance. I dati usati dall'AI sono le informazioni strutturate, semi-strutturate e non strutturate che alimentano i modelli e i sistemi: provengono prevalentemente dai sistemi fondazionali (ERP, CRM, data warehouse, sistemi MES e di campo), richiedono armonizzazione, pulizia e validazione prima dell'uso, e costituiscono la principale leva di differenziazione competitiva quando sono di qualità superiore alla media di settore. I dati trasformati per l'AI sono le rappresentazioni vettoriali, i tag semantici e gli embedding che convertono le informazioni grezze in formati processabili dai modelli: la loro produzione implica scelte architetturali non banali (quali modelli di embedding, quale granularità, quale strategia di aggiornamento) e richiede una governance specifica perché la loro obsolescenza può compromettere silenziosamente la qualità degli output senza che l'utente finale se ne accorga. I dati generati dall'AI sono gli output strutturati (previsioni, scoring, classificazioni) e non strutturati (testi, sintesi, raccomandazioni) prodotti dai sistemi: rappresentano una nuova categoria di asset informativo aziendale e devono essere governati in termini di qualità, tracciabilità e riusabilità, evitando che si disperdano nei silos operativi delle singole funzioni. I metadati dell'AI, infine, comprendono prompt library, tassonomie, source code, policy, materiali formativi e documentazione dei casi d'uso: sono il tessuto connettivo dell'ecosistema AI, spesso sottovalutato in fase di avvio e tremendamente costoso da ricostruire quando manca. L'organizzazione che adotta l'AI dovrebbe quindi, prima di avviare qualsiasi iniziativa rilevante, condurre una valutazione onesta della propria maturità sui dati lungo almeno tre assi: la qualità (accuratezza, completezza, aggiornamento e consistenza delle fonti primarie), l'accessibilità (capacità di rendere disponibili i dati giusti ai sistemi giusti nei tempi giusti, senza colli di bottiglia architetturali o barriere organizzative tra funzioni) e la governance (chi possiede i dati, chi li aggiorna, chi ne autorizza l'uso in contesti AI, chi risponde della loro qualità nel tempo). Un dato non governato è un rischio operativo: può alimentare bias, produrre output

errati con apparenza di correttezza, e generare danni reputazionali o legali difficilmente reversibili. La dimensione "Dati e Tecnologia" è una delle sette dimensioni su cui il Maturity Model di A(I)doption valuta la preparazione dell'organizzazione all'adozione: non a caso è spesso quella che registra i punteggi più bassi nelle organizzazioni che si trovano ancora in fase di sperimentazione. La ragione è strutturale: i dati si accumulano nel tempo in architetture costruite per scopi diversi dall'AI, e renderli utilizzabili richiede investimenti non glamour (integrazione, pulizia, tagging, normalizzazione) che nessun vendor di modelli ha interesse a enfatizzare nel proprio pitch commerciale. Prenderne coscienza prima di comprare licenze è uno degli atti di maturità più concreti che un'organizzazione possa compiere.

Art. 13 — Discovery, qualificazione, approvazione e architettura delle soluzioni AI

La fase di Discovery consiste nell'identificazione sistematica, raccolta e qualificazione dei casi d'uso AI provenienti dalle funzioni aziendali. Ogni caso d'uso viene formalizzato attraverso un template standardizzato che ne descrive finalità, processi impattati, benefici attesi espressi in termini misurabili, rischi, requisiti tecnici e normativi. Il processo produce una long list qualificata, l'identificazione dei quick win implementabili e una roadmap in termini di pipeline. Temporizzata. Ogni soluzione AI di qualsivoglia natura (sviluppo interno, acquistata sul mercato, embedded in piattaforme esistenti o fornita da vendor verticali) deve essere soggetta a un assessment formale che include: classificazione del rischio secondo l'AI Act; valutazione degli impatti su dati, privacy e proprietà intellettuale; analisi dell'integrazione architetturale; valutazione economica e di sostenibilità. L'esito produce una decisione formale di approvazione, approvazione con azioni correttive, o non approvazione. Workshop, interviste, process mapping e schede use case dettagliate con benefici, effort e fattibilità costituiscono il nucleo operativo della Discovery che non è brainstorming "da macchinetta del caffè", è un processo strutturato di prioritizzazione con output verificabili ed "azionabili" (era dal 2003 che non scrivevo la traduzione italiacana di "actionable" in un testo). La decisione su come realizzare un caso d'uso approvato non è meno importante della decisione di approvarlo. L'architettura delle soluzioni AI si declina secondo tre modalità fondamentali, ciascuna con implicazioni molto diverse in termini di costo, controllo, flessibilità e rischio, e la scelta tra esse deve essere esplicita, motivata e coerente con il profilo di maturità e con gli obiettivi strategici dell'organizzazione.

La modalità Make (costruire) comprende lo sviluppo interno di applicazioni, algoritmi e pipeline su misura: applicazioni proprietarie con interfacce dedicate e logica di business specifica; modelli e algoritmi sviluppati internamente (ad es. LLM fine-tuned su dati aziendali, modelli predittivi di dominio, pipeline RAG proprietarie); sistemi di automation e analytics costruiti su architetture dati aziendali. Questa modalità massimizza il controllo, la differenziazione competitiva e la protezione della proprietà intellettuale, ma richiede competenze tecniche interne elevate, tempi di sviluppo significativi e una governance del ciclo di vita del software rigorosa. È appropriata quando il caso d'uso è strategicamente differenziante, quando i dati utilizzati sono troppo sensibili per essere esposti a sistemi di terzi, o quando le soluzioni disponibili sul mercato

non coprono adeguatamente i requisiti specifici del dominio.

La modalità Build-Configure (configurare e integrare) comprende l'adattamento di piattaforme e framework enterprise-grade a flussi di lavoro specifici: configurazione di framework per agenti conversazionali e chatbot aziendali su modelli fondazionali disponibili via API; utilizzo di servizi cloud AI (computer vision, NLP, speech) integrati nei processi attraverso connettori e orchestratori; strumenti di personal automation e RPA intelligente configurati sulle specificità operative. Questa modalità bilancia velocità di implementazione e controllo, richiede competenze di integrazione e prompt engineering, ed è particolarmente efficace per casi d'uso di Co-Intelligence (assistenti al lavoro di conoscenza, strumenti di drafting e analisi) e per automazioni intelligenti di processo. Il rischio principale è la dipendenza da provider esterni e la tendenza a sotto-governare la configurazione: un sistema configurato male può produrre output sistematicamente errati per settimane prima che qualcuno se ne accorga.

La modalità Buy (acquistare) comprende l'adozione di soluzioni pronte all'uso: piattaforme enterprise integrate nei sistemi fondazionali (ERP, CRM, HCM) con funzionalità AI già embedded dai vendor; soluzioni verticali settoriali o funzionali già addestrate su dati di dominio specifico; agenti AI e personal assistant pre-configurati introdotti direttamente nei sistemi di produttività individuale. Questa modalità minimizza i tempi di attivazione e le competenze tecniche richieste, ma espone l'organizzazione al rischio di adottare sistemi dei quali non controlla né il modello, né i dati di addestramento, né le politiche di aggiornamento.

La due diligence su soluzioni Buy deve essere particolarmente rigorosa: ogni vendor che promette AI embedded in un prodotto esistente sta introducendo un sistema che, ai sensi dell'AI Act, può richiedere classificazione, documentazione e supervisione esattamente come qualsiasi sistema sviluppato internamente. "Lo fa il software" non è una risposta accettabile alla domanda "chi è responsabile di questo output". Nella pratica, la maggior parte delle organizzazioni opera simultaneamente su tutte e tre le modalità, con portafogli misti che includono sistemi fondazionali con AI embedded (Buy), assistenti configurati su modelli esterni (Build-Configure) e algoritmi sviluppati internamente per i casi d'uso più critici (Make). Governare questa complessità è uno degli obiettivi primari del Target Operating Model: il rischio non è la coesistenza di modalità diverse, ma la loro proliferazione non coordinata in assenza di criteri espliciti di selezione, standard di integrazione condivisi e un inventario che le renda visibili nella loro totalità.

Art. 14 — Pilot, rilascio in produzione e scala

La fase Pilot è il regime di iniziale realizzazione in cui la soluzione approvata viene realizzata tecnicamente, integrata nell'architettura aziendale, testata in termini di performance e comportamento in scenari operativi reali, e validata dagli utenti finali. Il Pilot è progettato con obiettivi di apprendimento espliciti: deve generare evidenza verificabile sull'effettiva capacità della soluzione di produrre il valore atteso, non solo in ambienti di test. Ogni Pilot include meccanismi di rollback e procedure di gestione dei malfunzionamenti. Dopo la validazione del Pilot, la soluzione viene rilasciata in produzione con formazione agli utenti, KPI di monitoraggio

e meccanismi di supervisione umana. Quando la produzione dimostra qualità, sicurezza ed equità dei risultati, la soluzione viene industrializzata e diffusa a scala, con un piano di change management dedicato per ogni nuova popolazione di utenti e funzione coinvolta. Le soluzioni che dimostrano valore replicabile vengono capitalizzate nell'AI Portal come patrimonio comune dell'azienda. Lo sviluppo del primo pilot deve costituire il momento in cui l'adozione smette di essere un progetto e diventa una capacità organizzativa strutturale.

Art. 15 — Riesame, aggiornamento e dismissione

Ogni sistema AI in produzione è soggetto a riesame periodico, con cadenza proporzionata al suo livello di rischio. Il riesame verifica la permanenza della conformità normativa, la coerenza con i principi di questa Costituzione, la persistenza del valore generato e l'assenza di derive comportamentali non previste. Se il riesame evidenzia non conformità, obsolescenza o rischi non mitigabili, il sistema viene limitato, aggiornato o dismesso secondo procedure documentate. La dismissione non è un fallimento: è l'esercizio maturo della governance. Il riesame periodico è il meccanismo che trasforma la governance da adempimento burocratico in generazione di valore continua: l'organizzazione non certifica una soluzione, la presidia nel tempo.

Titolo III — Infrastruttura Abilitante

Art. 16 — AI Portal, Academy e mobilitazione organizzativa

L'AI Portal dovrebbe essere il punto di accesso unico all'ecosistema AI aziendale: raccoglie strumenti approvati, casi d'uso, materiali di formazione, prompt library e best practice, riducendo frammentazione e duplicazioni. La conoscenza acquisita dall'organizzazione in materia di AI deve diventare patrimonio comune, riutilizzabile tra tutte le funzioni. La diffusione dell'AI deve essere sostenuta da un programma strutturato di Academy che copre: fondamenti e storia dell'AI, AI generativa e prompt engineering, automazione intelligente, analytics. Il programma è differenziato per ruoli, livelli di responsabilità e profili di rischio. Il change management non è un'attività collaterale: è un componente strutturale del modello operativo, che include comunicazione interna, raccolta sistematica di feedback dal campo e riconoscimento dei comportamenti virtuosi. Quanto di cui sopra non deve essere considerato come tre iniziative separate: sono i tre pilastri della trasformazione dell'interesse per l'AI in un assetto organizzativo governato, sostenibile e diffuso.

Titolo IV — Garanzie Costituzionali

Art. 17 — Compliance normativa continua, audit e gestione degli incidenti

L'organizzazione che adotta consapevolmente l'AI dovrebbe mantenere un modello permanente di compliance al Regolamento (UE) 2024/1689 (AI Act), alla Legge italiana n. 132/2025 e alla normativa nazionale e settoriale applicabile. La compliance va intesa come un processo continuo che richiede l'aggiornamento periodico del Registro AI, il riesame delle valutazioni di rischio e la formazione aggiornata degli attori coinvolti. Ogni incidente rilevante, uso improprio,

esposizione indebita di dati o deviazione dai principi di questa Costituzione dovrebbe essere segnalato, istruito e corretto secondo procedure documentate. L'ecosistema AI aziendale deve essere soggetto ad audit periodici interni anche informali. Chi segnala un problema relativo all'AI non deve essere esposto a conseguenze disciplinari per il solo fatto di aver reso visibile qualcosa che altrimenti sarebbe rimasto nell'ombra operativa: la segnalazione è un atto di responsabilità, non di delazione.

Art. 18 — Revisione costituzionale

La presente Costituzione è soggetta a revisione periodica obbligatoria, con cadenza almeno annuale o in occasione di cambiamenti tecnologici (od anche normativi) rilevanti ed in sincrono con l'evolvere della maturità AI dell'organizzazione. La revisione è promossa dal Comitato Strategico AI e condotta in modo partecipativo. Nessuna revisione può ridurre o eliminare il principio della responsabilità umana finale, il diritto al giudizio umano effettivo, il principio di proporzionalità del rischio o il principio di trasparenza e contestabilità: questi quattro principi costituiscono il nucleo irriducibile di questa Costituzione.

Disposizioni Finali

Art. 19 — Gerarchia degli strumenti di governance e rapporti con gli strumenti derivati

La presente Costituzione occupa il vertice della gerarchia degli strumenti di governance AI aziendale. Il Manifesto AI ne esprime la visione strategica pubblica. La Policy AI traduce i principi costituzionali in regole operative, classificazioni e responsabilità individuali. Il Target Operating Model ne organizza l'esecuzione attraverso organi, processi, strumenti e metriche. I framework di compliance ne presidiano la conformità normativa. In caso di conflitto tra questi strumenti, prevale il principio costituzionale più pertinente.

Art. 20 — Forma del testo, entrata in vigore e disposizione di salvaguardia

La presente Costituzione può essere adottata in una versione interna estesa, che ne costituisce il testo completo e vincolante, e in una versione pubblica sintetica da utilizzare per la comunicazione esterna. Le due versioni devono essere coerenti nei principi: la versione pubblica non può omettere né contraddire alcuno dei principi fondamentali enunciati agli articoli 1-6. La Costituzione entra in vigore con la sua adozione formale da parte del Comitato Strategico AI e, ove previsto, con l'approvazione degli organi societari competenti. Se una disposizione dovesse risultare in conflitto con la normativa vigente, le restanti disposizioni mantengono la loro piena efficacia. Il rispetto della normativa è condizione minima inderogabile: questa Costituzione si propone di andare oltre la mera compliance, non di scendere al di sotto di essa.

Nota Finale

Questo testo non è, e non vuole essere, un esercizio di retorica istituzionale. È la risposta a una questione pratica e urgente: come si governa l'AI in azienda in modo che il valore prodotto sia reale, le responsabilità siano chiare e le persone siano protette? La risposta che proponiamo è che occorre un ordinamento, non solo regole. Un ordinamento che distingua tra principi irrinunciabili e norme operative, tra diritti delle persone e doveri dell'organizzazione, tra organi di indirizzo e organi di esecuzione, tra fase di sperimentazione e fase di scala. Un ordinamento che sappia evolversi senza perdere la propria identità fondante. Il framework A(I)doption è la traiettoria concreta attraverso cui questo ordinamento prende forma: dalla valutazione della maturità alla costruzione delle competenze, dalla discovery dei casi d'uso al pilot, fino allo scaling strutturale nei processi. La Costituzione ne fissa i principi; A(I)doption ne realizza il percorso.

"La governance non è il contrario dell'innovazione. È ciò che la rende possibile nel lungo periodo." —