Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

RICERCA

DOCUMENTO

LINEE GUIDA DI VIGILANZA DEL COLLEGIO SINDACALE SULLA ADOZIONE DELL'INTELLIGENZA ARTIFICIALE

AREA DI DELEGA CNDCEC

Sistemi di controllo e revisione legale (*financial* e non *financial*)

COMMISSIONE DI STUDIO

Aggiornamento e revisione dei principi di comportamento del collegio sindacale e dell'organo di controllo di società quotate

CONSIGLIERI DELEGATI

Gian Luca Ancarani

Maurizio Masini

PRESIDENTE

Riccardo Losi

3 DICEMBRE 2025

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente
Elbano de Nuccio

Vice Presidente
Antonio Repaci

Consigliere Segretario
Giovanna Greco

Consigliere Tesoriere
Salvatore Regalbuto

Consiglieri
Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
David Moro
Eliana Quintili
Pierpaolo Sanna
Liliana Smargiassi
Gabriella Viggiano
Giuseppe Venneri

Collegio dei revisori

Presidente
Rosanna Marotta

Componenti
Maura Rosano
Sergio Ceccotti

Composizione della Fondazione Nazionale di Ricerca dei Commercialisti

Consiglio di gestione

Presidente
Antonio Tuccillo

Vice Presidente
Giuseppe Tedesco

Consigliere Segretario
Andrea Manna

Consigliere Tesoriere
Massimo Da Re

Consiglieri
Francesca Biondelli
Antonia Coppola
Cosimo Damiano Latorre
Claudia Luigia Murgia
Antonio Soldani

Collegio dei revisori

Presidente
Rosario Giorgio Costa

Componenti
Ettore Lacopo
Antonio Mele

Area di delega CNDCEC "Sistemi di controllo e revisione legale (*financial* e non *financial*)"

Commissione di studio "*Aggiornamento e revisione dei principi di comportamento del collegio sindacale e dell'organo di controllo di società quotate*"

Consiglieri CNDCEC delegati

Gian Luca Ancarani
Maurizio Masini

Presidente

Riccardo Losi

Componenti

Antonella Bientinesi
Simona Bonomelli
Francesca Burigo
Roberto Cairo
Ciro Di Carluccio
Francesco Fallacara
Nadia Fontana
Ines Gandini
Massimo Gatto
Severino Gritti
Maurizio Lauri
Mauro Lonardo
Claudio Miglio
Andrea Negri
Monica Petrella
Marco Seracini
Massimiliano Troiani
Luigi Raffaele Vassallo
Michela Zeme

Esperti

Niccolò Abriani
Giovanni Barbara
Rosalba Casiraghi
Marco Maugeri

Staff tecnico

Cristina Bauco - *Coordinatrice area giuridica FNC-Ricerca*
Matteo Pozzoli - *Ufficio legislativo CNDCEC*

A cura di

Ciro Di Carluccio e Claudio Miglio

Sommario

Introduzione

Negli ultimi anni, l'Intelligenza Artificiale (IA) ha accelerato l'innovazione in molti settori, trasformando i processi decisionali, i modelli di business e le interazioni con gli stakeholder. Tuttavia, l'adozione dell'IA introduce rischi significativi che possono minacciare la sostenibilità e la fiducia degli stakeholder.

L'IA non è semplicemente una tecnologia avanzata, ma un vero e proprio agente strategico capace di ridefinire i modelli di business e il posizionamento competitivo delle imprese. Non si limita a svolgere compiti tecnici o operativi, ma influisce sulle decisioni aziendali di alto livello, consentendo alle organizzazioni di adattarsi rapidamente ai cambiamenti del mercato, ottimizzare le risorse e innovare in modo sostenibile. Questa natura strategica rende l'IA una leva cruciale per le imprese, in particolare per quelle quotate, dove l'innovazione tecnologica deve essere allineata a obiettivi di trasparenza e creazione di valore per gli azionisti.

Nell'ambito delle imprese, queste tecnologie offrono opportunità significative. Tra le applicazioni più diffuse vi sono: l'ottimizzazione dei processi produttivi, il miglioramento della *customer experience* tramite assistenti virtuali e sistemi di personalizzazione, la gestione dei rischi finanziari mediante analisi predittive e la sicurezza dei dati attraverso algoritmi di rilevamento delle minacce informatiche. Per le imprese, l'IA rappresenta un valore aggiunto strategico, consentendo non solo di migliorare la trasparenza e la governance interna attraverso strumenti automatizzati di monitoraggio, ma anche di rispondere più rapidamente alle mutevoli esigenze degli investitori e dei regolatori.

L'integrazione dell'IA nelle imprese quotate è un fattore critico di differenziazione sul mercato, migliorando l'efficienza operativa e contribuendo al raggiungimento degli obiettivi. L'avvento dell'intelligenza artificiale non è un semplice upgrade tecnologico, ma una trasformazione che ridisegna catene del valore, ruoli professionali, processi decisionali e aspettative degli stakeholder. In questo scenario, con l'indirizzo del consiglio di amministrazione od organo equivalente[1], una società quotata è chiamata a prevedere e governare in modo proattivo gli impatti dell'IA su produttività, organizzazione del lavoro, competenze, dipendenze da terze parti e profili di rischio (operativi, legali, reputazionali), perché tali impatti possono incidere in modo significativo sulla gestione ordinaria e, nei casi più critici, sulla stessa continuità aziendale. Ciò implica una pianificazione esplicita: valutazioni d'impatto *ex ante*, percorsi di *reskilling* e riallocazione delle persone, tenendo anche conto della necessità di integrazione dei presìdi di compliance nei processi, dei piani di continuità e sicurezza per sistemi dipendenti da modelli, e di una reportistica per gli organi di gestione.

[1] Le indicazioni contenute nel documento, pur indirizzandosi principalmente agli organi di amministrazione e controllo del sistema tradizionale di governance, possono riferirsi anche agli organi di amministrazione e controllo dei due sistemi alternativi.

La crescente regolamentazione, in particolare il c.d. AI Act dell'Unione Europea e l'emergere di standard come la norma ISO/IEC 42001[2] per i sistemi di gestione dell'IA, richiedono tuttavia di affiancare alle scelte tecnologiche un'adeguata attenzione ai profili di conformità, gestione dei rischi e responsabilità. Ciò comporta che, accanto all'organo di amministrazione, responsabile per l'istituzione e l'implementazione dei sistemi di AI, anche il collegio sindacale deve sviluppare un nuovo approccio di vigilanza, verificando che l'adozione di tali tecnologie sia conforme alle leggi, agli standard di buona governance e agli interessi di lungo termine degli azionisti e svolgere un'azione di *oversight* generale sulla coerenza e sull'effettiva attuazione della pianificazione, affinché l'uso dell'IA generi valore sostenibile senza esporre l'impresa a rischi non solo di compliance ma anche di business non governati.

Il documento offre quindi un quadro pratico per supportare il collegio sindacale nell'attuazione di tale vigilanza, mantenendo il focus del controllo sulle aree più rilevanti, quali sono:

1. la gestione strategica della transizione verso l'AI;
2. la valutazione strategica dell'IA;
3. la supervisione della governance interna;
4. la gestione dei rischi legati all'IA;
5. la compliance normativa e regolamentare;
6. l'utilizzo dei sistemi di AI da parte degli organi di governance.

Il documento propone raccomandazioni di carattere orientativo per l'organo di controllo in ordine all'impiego dell'IA. Le indicazioni non introducono obblighi ulteriori rispetto a quelli derivanti dalla legge e dallo statuto, né costituiscono attestazioni tecniche o verifiche sostitutive dell'operato del management e del consiglio di amministrazione. Le espressioni utilizzate (ad esempio "richiedere", "si fa rappresentare", "sollecitare") descrivono condotte tipiche di presidio e non impongono adempimenti puntuali o standard minimi inderogabili; le attività di vigilanza vanno sempre calibrate secondo principi di proporzionalità, materialità adeguandole alle circostanze del caso concreto, sulla base di informazioni ragionevoli fornite dalle funzioni aziendali e, ove necessario, da competenze specialistiche esterne.

Anche gli "Use Case" riportati hanno valore esemplificativo e di supporto alla comprensione delle raccomandazioni esplicitate: non sono esaustivi né prescrittivi, non costituiscono una check-list e non ampliano i doveri del collegio sindacale; la mancata esecuzione di una specifica azione tra quelle esemplificate non può essere invocata come inadempimento quando sia stato mantenuto un presidio coerente con le funzioni di legge. L'organo di controllo non effettua test tecnici né rielabora modelli: esercita una vigilanza sulla qualità del processo decisionale e sull'idoneità degli assetti, fermo restando che responsabilità e attuazione operativa restano in capo al management e al consiglio di amministrazione.

[2] L'ISO/IEC 42001:2023, *Information technology - Artificial intelligence - Management system* è il primo standard internazionale pubblicato per fornire indicazioni per l'istituzione, l'implementazione, il mantenimento e il miglioramento continuo di un sistema di gestione dell'IA nel contesto di una struttura organizzativa che se ne servi.

Alcune delle responsabilità richiamate nel documento o descritte negli Use Case sono attribuite al consiglio di amministrazione ovvero ad amministratori delegati e quindi al management aziendale. La distinzione di responsabilità fra consiglio di amministrazione e management è stabilita dalle norme di legge e può variare a seconda della estensione delle deleghe conferite agli amministratori con deleghe operative, delle modalità di eventuale adozione del Codice di Corporate Governance e delle procedure aziendali e non è quindi oggetto del presente documento. I richiami a tali responsabilità, essendo attribuibili a coloro che sono preposti alla attività gestoria, hanno quale finalità esclusiva quella di contestualizzare l'oggetto della vigilanza del collegio sindacale e non quella di definire come le responsabilità siano attribuibili ai singoli amministratori.

Chiude il documento un'Appendice in cui è riportato un Glossario terminologico.

1. La gestione strategica della transizione verso l'AI

1.1. La responsabilità del consiglio di amministrazione e quelle dei preposti alla gestione aziendale

Come accennato, il consiglio di amministrazione guida la transizione fissando obiettivi, priorità e tempi; al management spetta sviluppare l'analisi e realizzare le azioni. Il collegio sindacale dovrebbe aspettarsi che il primo passaggio sia una valutazione da parte del consiglio di amministrazione degli effetti dell'intelligenza artificiale sui processi e sulle persone: dove aumenta la produttività, dove migliora la qualità e i tempi di risposta, quali attività si svuotano parzialmente e quali, al contrario, si intensificano. Questa fotografia dovrebbe limitarsi ai confini dell'organizzazione ma considera anche clienti, fornitori e mercato del lavoro. Sulla base di questa analisi il consiglio di amministrazione dovrebbe così quantificare le ricadute sull'occupazione attuale e disegnare un percorso ordinato per le persone. La transizione delle persone dovrà necessariamente mettere in priorità il riassorbimento interno dal momento che non sarebbe realizzabile una alternativa di integrale sostituzione della forza lavoro attuale con una nuova in tempi compatibili con le esigenze che si andranno a manifestare. Per i ruoli più esposti alla standardizzazione sarà necessario progettare quindi percorsi di riqualificazione che supportino la riallocazione di risorse verso attività di maggior valore, come il controllo qualità, la gestione delle eccezioni e la relazione con il cliente. Per coloro che resteranno nelle loro attuali funzioni ma necessiteranno di nuovi strumenti sarà necessario che la gestione della Società pianifichi l'aggiornamento delle competenze che favoriscano l'adozione efficace di tali strumenti: capacità attraverso il *prompt engineering* di formulare richieste efficaci ai sistemi, lettura consapevole degli esiti, comprensione delle logiche di funzionamento senza entrare nella tecnica specialistica. La quota di capacità che non risulterà ragionevolmente assorbibile l'eccedenza per la quale il consiglio di amministrazione dovrebbe programmare in anticipo eventuali *layoff* con trasparenza e tutele attraverso percorsi di uscita pianificati per tempo. Tutto questo richiederà una forte integrazione con il piano strategico aziendale, un calendario realistico, collegato ai rilasci dei progetti, e un sistema

essenziale di indicatori che misurino avanzamento della formazione, cambi di ruolo effettivi, risultati operativi e problemi ricorrenti.

1.2. Azioni di *oversight* del collegio sindacale nella prospettiva della vigilanza sul rispetto dei principi di "corretta amministrazione", sulla adeguatezza degli assetti organizzativi e sul sistema di controllo interno di gestione dei rischi

Il collegio sindacale mantiene un presidio continuo sulla correttezza del processo decisionale e sulla tenuta del sistema dei controlli quando la società progetta, adotta e gestisce sistemi di intelligenza artificiale. In fase iniziale il primo obiettivo è rappresentare al consiglio di amministrazione l'importanza che può assumere l'ingresso dell'AI nell'agenda strategica. Dovrà quindi acquisire consapevolezza della logica con cui la società ha stimato impatti su processi, risultati e persone, e il modo in cui tali analisi sono state poste a base delle deliberazioni.

Laddove il consiglio di amministrazione deliberi atti di pianificazione o investimenti significativi, il collegio sindacale vigila che le proposte siano supportate da processi idonei (analisi dei rischi, piani di attuazione, oneri e benefici, profili regolatori e informativa al personale), anche avvalendosi di pareri tecnici ove necessari, così da garantire decisioni informate e prudenti. In presenza di segnali che possano toccare la continuità aziendale (per esempio, forte dipendenza da fornitori critici di tecnologia o ritardi che pregiudicano l'erogazione di servizi), richiede che il management offra un'informativa più approfondita e calendarizzi interventi conseguenti.

Nel corso del mandato, il collegio sindacale vigila sull'adeguatezza degli assetti organizzativi, del sistema di controllo interno e del sistema amministrativo-contabile rispetto alle aree interessate dall'implementazione di sistemi di IA. Ciò comprende un monitoraggio della qualità dei flussi informativi verso il consiglio di amministrazione; della coerenza tra ruoli, deleghe e responsabilità operative; dell'integrazione dei presìdi di rischio, sicurezza e qualità dei dati nei processi di sviluppo, rilascio e gestione dei modelli; della capacità della funzione di audit di coprire i processi e i sistemi rilevanti con metodologie adeguate e una reportistica comprensibile. Quando le informazioni disponibili evidenziano scostamenti rilevanti rispetto agli obiettivi o criticità nel controllo interno, il collegio sindacale sollecita chiarimenti e l'adozione di opportune iniziative di rientro, seguendo poi l'avanzamento delle azioni nel corso del mandato.

La partecipazione informata alle riunioni del consiglio di amministrazione e dei comitati endoconsiliari competenti, quando istituiti, acquisisce una importanza particolare dando l'opportunità ai suoi membri di formulare osservazioni quando ritengano che l'esecuzione di un progetto IA possa determinare effetti contrari alla legge o allo statuto, o comunque tali da porre in discussione i principi di corretta amministrazione e l'integrità patrimoniale della società.

Nel dialogo con le funzioni di controllo interno, il collegio sindacale raccoglie elementi utili circa l'idoneità e l'operatività del sistema di controllo interno: esiti delle verifiche su processi e modelli, grado di copertura dei piani di audit rispetto all'"universo" IA, rilievi sulla qualità dei dati e

sull'adeguatezza delle misure di contenimento del rischio. Questo insieme di condotte realizza un presidio sulla qualità del processo decisionale e sulla idoneità degli assetti a supporto delle scelte, con particolare riguardo ai progetti di intelligenza artificiale che incidono su strategia, rischio e informativa societaria.

Quanto alla vigilanza sulla corretta amministrazione da parte del collegio sindacale, giova richiamare che l'intelligenza artificiale non incide solo sull'organizzazione interna e sui profili di rischio, ma modifica in modo strutturale i mercati di fornitura di beni e servizi, inclusi quelli professionali e tecnologici. L'automazione di attività ripetitive, l'elaborazione massiva dei dati, la generazione assistita di documenti e la capacità predittiva riducono i tempi, i costi e le risorse umane necessarie per l'erogazione di numerosi servizi (consulenza, analisi dati, auditing, *cyber security*, ecc.).

GLI USE CASE DEL PARAGRAFO

Use Case 1: Transizione ordinata delle risorse umane in un progetto di automazione back-office

Contesto

Una società quotata di servizi avvia un programma di IA per automatizzare la riconciliazione contabile e l'estrazione dati da fatture. La stima preliminare indica un miglioramento di produttività tra il 25% e il 35% su tre processi, con impatto diretto su circa 60 addetti. Parte del lavoro diventa controllo qualità e gestione eccezioni; una quota residua di attività si riduce strutturalmente

Azioni dei preposti alla gestione aziendale

Il consiglio di amministrazione richiede una valutazione d'impatto che colleghi benefici operativi e ricadute sull'organizzazione. Il management presenta una mappa dei processi, individua i ruoli a rischio di obsolescenza parziale e quantifica l'eccedenza potenziale. Disegna quindi un percorso di riassorbimento interno: *reskilling* per 40 persone verso attività di controllo e data *quality*, *upskilling* per 15 persone che resteranno nei ruoli attuali con nuovi strumenti, mobilità interna per 3 unità con domanda crescente. La pianificazione della formazione precede il *go-live* di tre mesi; il rilascio dei modelli è scaglionato su 9 mesi. Vengono fissati indicatori semplici e leggibili (copertura formativa mensile, percentuale di cambi ruolo effettivi, tasso di eccezioni gestite senza ritardi, benefici economici realizzati rispetto al piano) e un calendario di aggiornamento al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale acquisisce informazioni sulla logica della valutazione d'impatto e la coerenza tra calendario di progetto e tempi dei percorsi per le persone. Nel corso dell'esecuzione prende visione dei cruscotti periodici e si concentra su due profili: l'aderenza ai traguardi dichiarati (formazione completata, riallocazioni effettive) e la stabilità dei risultati operativi. Quando emergono scostamenti ricorrenti in un'area, invita il management a spiegare il piano di rientro e ne segue l'attuazione nei cicli successivi.

Risultato atteso

La produttività cresce nei tempi attesi, il 90% della forza impattata viene riassorbito tramite *reskilling* e mobilità interna, la quota residua è gestita con percorsi di uscita concordati. L'azienda realizza i benefici senza tensioni organizzative e con una narrazione chiara verso il mercato e gli stakeholder interni.

2. Valutazione strategica dell'IA

Il collegio sindacale deve assicurarsi che l'IA non sia utilizzata in modo isolato, ma integrata nella strategia complessiva dell'organizzazione. In questo contesto, il collegio sindacale vigila che le scelte del consiglio di amministrazione siano supportate da analisi delle priorità aziendali, dalla definizione di obiettivi chiari e comunicati e da una pianificazione di lungo termine, con milestone utili a valutare l'efficacia delle iniziative. Questo richiede:

- una valutazione di come gli amministratori considerino l'IA nella definizione della strategia aziendale rispetto agli obiettivi di crescita ed innovazione incidendo nel caso sul modello di business nonché le minacce competitive che potrebbero mettere al rischio il posizionamento strategico attuale della impresa:
- di assicurarsi che esistano obiettivi chiari e comunicati all'interno della organizzazione.

2.1. Impatto strategico dell'IA

Analizzare come gli amministratori integrano l'IA nelle strategie aziendali significa esaminare documenti, verbali e piani per capire se la tecnologia viene considerata leva di crescita e di innovazione valutando anche eventuali minacce competitive. Questo include la vigilanza che la Società tenga conto di eventuali rischi competitivi e che la governance dell'IA sia coerente con i principi di trasparenza e gestione del rischio richiamati dall'AI Act e (se non esplicitamente adottata dalla società indicata da qui in poi solo come riferimento nei suoi principi generali) dalla ISO/IEC 42001.

2.2. Coinvolgimento degli stakeholder interni

Il collegio sindacale valuta che il consiglio di amministrazione coinvolga i dirigenti chiave (es. CIO, Chief AI Officer, responsabili di linea), garantendo che le decisioni su IA siano condivise e supportate dalle competenze necessarie.

Valuta la chiarezza delle responsabilità e la corretta allocazione dei ruoli, in linea con le raccomandazioni ISO e con le definizioni di ruolo (*deployer*, *provider*) dell'AI Act.

2.3. Pianificazione a lungo termine

Nello sviluppare un piano IA ben strutturato, la società deve prevedere fasi che comprendano controlli periodici e aggiornamenti per riflettere l'evoluzione normativa e tecnologica. Il collegio sindacale vigila sull'esistenza di questo piano e sulla sua attuazione, sulla sua sostenibilità finanziaria e coerenza con la politica degli investimenti, richiedendo evidenze periodiche di avanzamento e valutando l'adeguatezza rispetto ai requisiti di *risk management* previsti da ISO/IEC 42001 e alle scadenze normative dell'AI Act.

Il collegio sindacale, nel rispetto delle proprie funzioni, segue la coerenza tra analisi strategica, piano di lungo termine e deliberazioni del consiglio di amministrazione chiedendo di essere tenuto aggiornato con cadenze definite su avanzamento, variazioni di perimetro e impatti attesi.

GLI USE CASE DEL PARAGRAFO

Use Case 2: Analisi delle priorità aziendali e impatto strategico dell'IA

Contesto

Un'azienda del settore manifatturiero sta affrontando pressioni competitive da parte di nuovi attori che utilizzano l'IA per ottimizzare la produzione e ridurre i costi. Gli amministratori intendono esplorare come l'IA possa supportare la transizione verso un modello di business basato su una produzione più agile e personalizzata.

Azione dei preposti alla gestione aziendale

- Integrare l'IA nella pianificazione strategica e nei piani industriali, specificando obiettivi e priorità e definendo l'investimento previsto;
- Condurre benchmarking periodico sulle pratiche dei concorrenti per individuare best practice e rischi emergenti.
- Preparare report periodici per il consiglio di amministrazione che illustrino l'impatto atteso dell'IA su competitività, costi e innovazione.
- Evidenziare rischi da ritardo nell'adozione e definire misure di mitigazione.

Azione del collegio sindacale

Il collegio sindacale verifica se il consiglio di amministrazione abbia considerato l'IA come una leva strategica per mantenere il vantaggio competitivo. Ciò include:

- l'esame dei documenti strategici aziendali per identificare come l'IA contribuisce agli obiettivi di crescita e innovazione;
- la valutazione se la Società abbia compreso e considerato nella elaborazione della propria strategia come i concorrenti stanno utilizzando l'IA per innovare;

- la consapevolezza che gli Amministratori abbiano preso in considerazione i rischi competitivi, come la perdita di mercato dovuta a ritardi nell'adozione dell'IA.

Risultato atteso

L'integrazione dell'IA nella strategia aziendale consente all'impresa di adottare tecnologie come la manutenzione predittiva e la personalizzazione dei prodotti, mantenendo la competitività di fronte alle minacce emergenti.

Use Case 3: Definizione degli obiettivi da parte della Società per l'IA

Contesto

Un'azienda del settore retail decide di adottare l'IA per migliorare l'esperienza cliente, aumentando la precisione delle raccomandazioni sui prodotti e ottimizzando la gestione degli stock. Tuttavia, manca una chiara definizione degli obiettivi e delle responsabilità legate a questo progetto.

Azioni dei preposti alla gestione aziendale

- Redigere una roadmap progettuale con obiettivi SMART (Specifici, Misurabili, Accessibili, Rilevanti, Temporali).
- Identificare metriche di business associate (es. aumento *conversion rate*, riduzione costi inventario).
- Assegnare responsabilità chiare a sponsor di progetto e team operativi.
- Attivare un piano di comunicazione interna per allineare tutti i livelli organizzativi.

Azioni dell'organo di controllo

Il collegio sindacale verifica che gli obiettivi relativi all'IA siano chiari e comunicati a tutti i livelli dell'organizzazione, intervenendo ove necessario nei seguenti modi:

- sollecita una mappatura degli obiettivi di business associati al progetto di IA, come l'aumento del tasso di conversione delle vendite o la riduzione dei costi di inventario;
- verifica che gli obiettivi siano Specifici, Misurabili, Raggiungibili, Rilevanti e Temporali;
- si accerta che esista un piano di comunicazione interna per garantire che i team coinvolti comprendano come il progetto di IA si allinei agli obiettivi aziendali complessivi.

Risultato atteso

L'IA viene implementata con obiettivi ben definiti, come un aumento del 20% nella precisione delle previsioni della domanda entro il primo anno, migliorando l'efficienza e l'allineamento strategico interno.

Use Case 4: Valutazione del rischio competitivo derivante dall'IA

Contesto

Un'azienda tecnologica affronta l'ingresso sul mercato di un concorrente che utilizza l'IA generativa per accelerare lo sviluppo di nuovi prodotti software. Gli amministratori vogliono capire come posizionarsi per contrastare questa minaccia.

Azioni dei preposti alla gestione aziendale

- Aggiornare regolarmente le analisi SWOT aziendali con focus specifico su minacce/opportunità IA.
- Valutare attivamente scenari di alleanze, partnership o M&A in ambito IA.
- Proporre al consiglio di amministrazione business case per eventuali investimenti mirati (es. infrastruttura, talenti, R&D IA).
- Monitorare il posizionamento dei concorrenti attraverso analisi di mercato dedicate.

Azioni dell'organo di controllo

Il collegio sindacale analizza come il consiglio di amministrazione valuti il rischio competitivo e in particolare se quest'ultimo, stia considerando:

- la revisione delle analisi SWOT aziendali, verificando se il rischio rappresentato dall'IA concorrente è stato considerato;
- l'identificazione di possibili partnership strategiche o acquisizioni che potrebbero rafforzare le capacità aziendali nell'IA;
- la supervisione di eventuali decisioni di investimento per accelerare l'adozione di tecnologie IA all'interno dell'azienda.

Risultato atteso

L'azienda adotta una strategia di risposta competitiva, implementando l'IA generativa nei propri processi di ricerca e sviluppo, accelerando il time-to-market per nuovi prodotti.

Use Case 5: Allineamento degli obiettivi di IA con la strategia aziendale

Contesto

Un'impresa del settore finanziario decide di implementare l'IA per migliorare il monitoraggio del rischio di credito e la personalizzazione delle offerte per i clienti. Tuttavia, non è chiaro come tali obiettivi si inseriscano nella strategia aziendale complessiva.

Azioni dei preposti alla gestione aziendale

- Collegare ciascun progetto di IA a obiettivi strategici aziendali (redditività, riduzione rischi, crescita).

- Definire KPI chiari e misurabili per il monitoraggio (es. % riduzione insolvenze).
- Implementare un processo di revisione periodica dei risultati per decidere eventuali estensioni ad altre aree aziendali.
- Documentare l'impatto dell'IA nei report gestionali e nella relazione sulla gestione.

Azioni dell'organo di controllo

Il collegio sindacale valuta l'esistenza di un processo che assicuri se:

- il progetto di IA è allineato ai principali obiettivi aziendali, come l'aumento della redditività o la riduzione del rischio operativo.
- sono stati definiti KPI specifici per misurare il contributo dell'IA alla strategia aziendale, come la riduzione delle insolvenze del 10% entro un anno.
- esiste un piano per estendere le applicazioni dell'IA ad altri processi aziendali una volta raggiunti i risultati iniziali.

Risultato atteso

Gli obiettivi di IA diventano una componente integrata della strategia aziendale, supportando la crescita sostenibile dell'azienda e migliorando la gestione del rischio.

3. Supervisione della governance interna

3.1. Strutture organizzative per l'IA

Il collegio sindacale vigila che l'IA non sia gestita unicamente come una tematica di carattere tecnologico, ma come parte integrante della governance aziendale[3]. Questo implica la verifica che l'organizzazione abbia strutture, policy e processi adeguati a garantire l'uso responsabile dell'IA, anche in linea con gli standard di best practices emergenti (ISO/IEC 42001) e con i requisiti normativi.

[3] Su tali aspetti, è opportuno segnalare lo schema di decreto legislativo recante attuazione della delega per la riforma del TUF, approvato in via preliminare dal Governo lo scorso 8 ottobre, che prevede l'introduzione di un nuovo art. 149-*ter* (Sistemi di monitoraggio e strumenti di controllo) dal seguente tenore:
"*Qualora ai fini del controllo interno siano adottati sistemi di monitoraggio continuo e strumenti di controllo automatici e predittivi, essi devono essere adeguati e proporzionati alla natura e alle dimensioni dell'impresa e ai rischi ai quali essa è esposta*". Del pari, giova osservare che, ai sensi dell'art. 123-*bis*, comma 2, del menzionato schema di decreto di riforma del TUF, la relazione sul governo societario, debba includere:
- una descrizione, ove adottate, delle politiche della società in materia di utilizzo e di monitoraggio delle nuove tecnologie, e in particolare dei sistemi di intelligenza artificiale, negli assetti amministrativi, organizzativi e contabili (lett. d-*ter*);
- una descrizione, ove adottate, delle politiche di gestione e di monitoraggio dei rischi informatici, inclusi i rischi di sicurezza cibernetica e i rischi derivanti dall'integrazione di nuove tecnologie negli assetti amministrativi, organizzativi e contabili (lett. d-*quater*).

L'adozione di sistemi di intelligenza artificiale in azienda richiede, ove l'impiego non sia meramente sporadico o sperimentale, la definizione di una policy aziendale formalmente approvata dal consiglio di amministrazione.

Tale documento assume la funzione di indirizzo e presidio di governance e dovrebbe:

- definire gli obiettivi e i principi generali dell'impiego dell'AI, in coerenza con l'interesse della società, la corretta amministrazione e la normativa applicabile (AI Act, privacy, *cybersecurity*, TUF);
- indicare i ruoli e le responsabilità delle funzioni aziendali coinvolte (management, IT, data owner, *risk management*, compliance, controllo interno) e i flussi informativi verso il consiglio di amministrazione e il collegio sindacale;
- stabilire le linee di indirizzo del consiglio di amministrazione sull'AI, indicando ambiti consentiti, limiti, necessità di supervisione umana, requisiti di tracciabilità e controllo sugli algoritmi e sui dati utilizzati;
- disciplinare i sistemi classificabili come "ad alto rischio" ai sensi dell'AI Act, prevedendo:
  - la conduzione di un AI *Risk Assessment* da parte del management;
  - l'informativa al consiglio di amministrazione e al collegio sindacale sulle risultanze e sulle misure di mitigazione adottate;
- prevedere modalità di aggiornamento periodico della policy e di verifica della sua concreta applicazione.

Il consiglio di amministrazione, in tale quadro, non si limita ad "approvare" la policy, ma:

- definisce gli indirizzi strategici sull'uso dell'AI nell'impresa;
- valuta la compatibilità delle soluzioni AI con l'assetto organizzativo e i rischi aziendali;
- assicura che siano disponibili risorse, competenze e controlli adeguati;
- vigila, anche attraverso i flussi informativi del management e le relazioni dell'organo di controllo, sulla sua attuazione e aggiornamento.

La Policy AI deve essere oggetto di revisione periodica in occasione di significativi aggiornamenti normativi o tecnologici, e la responsabilità della sua attuazione e del suo aggiornamento compete al management, sotto la supervisione del consiglio di amministrazione, che ne valuta la coerenza con gli assetti organizzativi e i rischi aziendali, nonché con gli indirizzi strategici approvati.

In tale contesto, il collegio sindacale deve:

- valutare l'esistenza di strutture interne adeguate alla gestione dell'IA, come comitati consiliari dedicati o l'assegnazione di deleghe a comitati esistenti (ad es. rischi, controllo).
- richiedere informazioni sulla presenza e sulla efficacia di politiche aziendali aventi come oggetto l'utilizzo di IA (policy di sviluppo, utilizzo e monitoraggio degli algoritmi), che siano formalmente approvate e aggiornate, e che tengano conto delle definizioni di ruolo introdotte dall'AI Act (*provider*, *deployer*, etc.).

3.2. Ruolo della governance nella tecnologia AI

3.2.1. Governance dei sistemi di IA e supervisione operativa

Il collegio sindacale acquisisce informazioni riguardanti il sistema di controllo interno sui sistemi di IA, con metriche di performance (accuratezza, tasso di errore, automazione), trasparenza dei modelli (documentazione dei processi decisionali) e protocolli di implementazione coerenti con le policy. L'attenzione deve essere rivolta anche ai processi posti in essere dalla Società per prevenire errori o violazioni normative. L'AI Act richiede per esempio *logging*, sorveglianza umana e rispetto delle istruzioni per i sistemi ad alto rischio: il collegio sindacale deve chiedere conferma della esistenza di questi presidi. Un elemento fondamentale per garantire una governance efficace è il controllo sistematico sui sistemi di Intelligenza Artificiale (IA) utilizzati all'interno dell'organizzazione. Ciò richiede un'analisi approfondita da parte del management delle capacità tecnologiche implementate e un monitoraggio continuo per assicurare che tali sistemi funzionino in linea con gli obiettivi strategici e operativi dell'impresa. Ciò posto, le possibili attività di vigilanza possono includere l'ottenimento di informazioni su:

- la definizione da parte del management di metriche chiave per valutare l'efficacia e l'efficienza dei sistemi di IA, come la precisione delle previsioni, il tasso di errore e il livello di automazione raggiunto;
- come i processi della società assicurano che gli algoritmi utilizzati siano trasparenti e comprensibili per gli stakeholder interni.
- l'utilizzo dell'AI in modo coerente con le politiche aziendali e la presenza di protocolli chiari per l'adozione di nuove tecnologie IA.

3.2.2. Prevenzione dei bias algoritmici

Gli algoritmi di IA possono essere influenzati da bias involontari derivanti dai dati utilizzati per il loro addestramento. Poiché questi algoritmi basano i propri comportamenti e decisioni sui dati di apprendimento, elaborano conclusioni in funzione delle informazioni predominanti presenti in tali dati, spesso rappresentati da quelli più facilmente disponibili in formato digitale.

Il rischio maggiore risiede nel fatto che gli algoritmi possono produrre indicazioni, prendere decisioni o fornire risultati che riflettano semplicemente le tendenze dominanti osservate nei dati, invece di rappresentare la realtà oggettiva. Queste tendenze, spesso determinate dalla frequenza con cui certi dati vengono rilevati, possono portare a risultati inefficaci perché non tengono conto della complessità e della varietà delle situazioni analizzate.

Se i dati di addestramento sono parziali o distorti, gli algoritmi rischiano di sviluppare modelli che si focalizzano su pattern errati o incompleti. Questo compromette l'efficacia dei risultati, portando a conclusioni fuorvianti o inadatte per prendere decisioni strategiche.

Il problema di efficacia causato dai bias non riguarda solo la qualità del risultato finale, ma anche la capacità dell'algoritmo di adattarsi a nuovi contesti o di generalizzare correttamente. Quando i modelli sono addestrati su dati che non rappresentano correttamente il dominio operativo, si crea un disallineamento tra ciò che viene previsto e ciò che avviene nella realtà.

In un mondo caratterizzato da opinioni polarizzate, il rischio che l'AI possa fornire analisi non obiettive e soluzioni non efficaci, riducendo la sua capacità di supportare decisioni basate su una visione accurata e completa della realtà, è elevato.

Per questo motivo, può essere opportuno che l'Organo di Controllo vigili che la società abbia implementato misure efficaci per identificare e mitigare i rischi legati al bias. Queste possono includere:

- la diversificazione e validazione delle fonti dei dati di addestramento, per garantire una rappresentazione completa del contesto;
- la progettazione di metriche di valutazione che testino la capacità dell'algoritmo di gestire casi che non rientrano nelle tendenze predominanti dei dati;
- la revisione periodica dei risultati per identificare eventuali deviazioni o inefficienze nei modelli.

3.2.3. Rischio di "Decision Capture"

L'impiego di sistemi di intelligenza artificiale nei processi aziendali comporta, tra i rischi trasversali, quello di *decision capture*, inteso come la delega parziale o sostanziale della decisione dall'essere umano al sistema algoritmico.

Il fenomeno non si esaurisce nell'accettazione acritica dell'*output* (*automation bias*), ma può presentarsi in forme più evolute (*decision proxying*), nelle quali l'AI:

- elabora, seleziona o filtra le informazioni rilevanti;
- omette passaggi istruttori o logici non visibili all'utilizzatore;
- propone direttamente una conclusione o la opzione "ottimale", riducendo lo spazio deliberativo residuo.

Tale rischio è amplificato quando:

- la decisione deve essere assunta immediatamente a seguito del verificarsi dei presupposti (es. *risk alert*, *trading* automatico, autorizzazioni di spesa, *scoring*);
- si utilizzano sistemi generativi o predittivi di nuova generazione, capaci di sostituire non solo l'analisi, ma anche la scelta;
- l'utente attribuisce all'AI una presunta neutralità, oggettività o infallibilità tecnica.

In tali casi, la decisione rimane formalmente in capo al soggetto umano, ma può risultare sostanzialmente condizionata o anticipata dal sistema, con conseguente riduzione della consapevolezza, della tracciabilità del processo deliberativo e della responsabilità. Al riguardo, si

segnala che a livello internazionale sono già disponibili metodologie e indicatori (es. AI Act, NIST, OECD) che consentono di classificare il grado di autonomia dei sistemi di AI e il livello di intervento o supervisione umana richiesto. La conoscenza e la consapevolezza di tali strumenti costituisce un utile riferimento per la valutazione del rischio di influenza o sostituzione del processo decisionale.

3.2.4. Sicurezza e resilienza dei sistemi di IA

I sistemi di IA possono essere vulnerabili a rischi di sicurezza, come attacchi informatici o manipolazioni dei dati. Una gestione proattiva della sicurezza è essenziale per proteggere i dati aziendali e mantenere l'affidabilità dei sistemi.

Il collegio sindacale vigila che siano presenti misure di protezione dei dati e dei modelli (crittografia, accessi controllati), monitoraggio costante e piani di continuità operativa. Il collegio sindacale verifica che le politiche di sicurezza siano documentate e aggiornate, che vengano effettuati audit periodici e che esistano meccanismi di risposta rapida a incidenti o attacchi (come richiesto anche dall'AI Act per il *reporting* di incidenti gravi).

3.2.5. Coinvolgimento degli stakeholder

L'intelligenza artificiale non deve essere relegata al dominio dei responsabili IT, come il CIO o il CTO, ma considerata un agente strategico che coinvolge tutti i principali stakeholder aziendali. Nella pratica, al rischio di un eccesso di controllo tecnologico si affianca quello che le funzioni di business e persino i singoli collaboratori della Società adottino in autonomia servizi esterni o soluzioni SaaS di IA senza un percorso di autorizzazione, con effetti su dati, responsabilità e rischi non presidiati.

La governance e l'integrazione dell'IA devono perciò essere trasversali, includendo il consiglio di amministrazione, i leader delle *business unit*, le funzioni tecniche e di controllo, così che l'IA entri nelle decisioni strategiche e nelle operazioni aziendali evitando fenomeni di "shadow AI". Questa prassi non va necessariamente limitata o scoraggiata dal momento che espande le capacità cognitive degli individui e dell'azienda e pertanto non va burocratizzata ma facilitata definendo responsabilità chiare per individui e funzioni di business con relativa *accountability* in caso di mancato rispetto, affiancate da un programma mirato di formazione, sensibilizzazione e diffusione capillare della importanza di poter sperimentare l'utilizzo di strumentazioni innovative sostenendone però le conseguenze nel caso di violazione delle normative interne in materia.

Il consiglio di amministrazione e i leader delle *business unit*, si adoperano affinché la IA diventi parte integrante delle decisioni strategiche e delle operazioni aziendali. È quindi essenziale:

- il coinvolgimento del consiglio di amministrazione, unico responsabile di assicurare che l'adozione e l'utilizzo dei sistemi di Intelligenza Artificiale siano coerenti con i requisiti di conformità e governance previsti dal Regolamento Europeo sull'AI (AI Act) e da buone prassi di governance (es. ISO/IEC 42001), garantendo adeguate politiche, risorse, controlli e una vigilanza costante sugli

impatti strategici, operativi ed etici nonché della integrazione dell'IA nel piano strategico per assicurare che le decisioni relative all'IA siano allineate agli obiettivi aziendali;

- creare un meccanismo di coordinamento tra i responsabili tecnologici, i dirigenti delle business unit e il top management per massimizzare il valore generato dall'IA;
- stabilire un flusso continuo di informazioni tra i responsabili tecnologici e il consiglio di amministrazione, garantendo che i progressi, i rischi e le opportunità legati ai sistemi di IA siano pienamente compresi;
- offrire programmi di formazione per sensibilizzare tutti i livelli dell'organizzazione, dal consiglio ai manager operativi, sulle potenzialità e i rischi dell'IA, promuovendo una cultura aziendale incentrata sull'uso strategico dell'intelligenza artificiale;
- istituire un processo unico di *intake* per tutti gli strumenti IA di terzi (inclusi i *trial*), che preveda le condizioni per consentire alle funzioni di business di poter innovare i propri processi e l'offerta di servizi e prodotti nel rispetto di principi generali di legge e dei modelli di controllo già esistenti.

Con riferimento alla necessità di garantire livelli sufficienti di alfabetizzazione in materia di intelligenza artificiale (AI literacy), in coerenza con gli artt. 3, n. 56 e 4 dell'AI Act, si osserva come tali livelli debbano garantire, non solo per il personale tecnico, bensì per qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, in forma proporzionata ai ruoli, almeno la conoscenza dei seguenti elementi essenziali:

1. funzionamento e limiti dell'AI, la differenza tra dato, inferenza e generazione e la necessità di supervisione umana;
2. rischi principali, errori, *bias*, allucinazioni, uso improprio di dati, *cybersecurity*, dipendenza dai fornitori, *decision capture*;
3. AI Act, principi fondamentali:
   - pratiche vietate (art. 5);
   - classificazione dei sistemi ad alto rischio (art. 6-7);
   - obbligo per il management di svolgere AI Risk Assessment e mantenerne evidenza;
   - obbligo di informare i preposti apicali alla gestione, il consiglio di amministrazione e il collegio sindacale in caso di utilizzo o introduzione di sistemi di AI classificabili ad alto rischio.

3.2.6. La vigilanza del collegio sindacale

Il collegio sindacale vigila che:

- i sistemi di IA siano integrati nella governance aziendale con criteri di sicurezza, affidabilità ed efficacia;
- l'organo amministrativo mantenga la titolarità del processo decisionale, acquisendo evidenza della valutazione critica degli *output* algoritmici;

- siano tracciati i dati utilizzati, le assunzioni di base e, ove rilevante, il contributo fornito dall'AI al processo deliberativo;
- i sistemi di AI impiegati nei processi decisionali, di controllo o di monitoraggio siano oggetto di validazione, monitoraggio continuo e documentazione;
- la società utilizzi metodologie riconosciute (es. framework previsti dall'AI Act, NIST, OECD) per classificare il grado di autonomia dei sistemi di AI e il livello di intervento umano (*human-in-the-loop*, *human-on-the-loop*, *full automation*), ai fini della comprensione dell'impatto potenziale sui processi decisionali e di controllo;
- le decisioni legate all'IA rispettino la normativa vigente e supportino gli obiettivi strategici dell'organizzazione;
- vengano adottati controlli adeguati a minimizzare rischi operativi, strategici e di sicurezza legati ai sistemi di IA;
- esista un flusso informativo trasparente tra gli organi decisionali aziendali e gli stakeholder responsabili, al fine di garantire la supervisione sui rischi associati all'IA;
- il piano di alfabetizzazione e formazione venga definito e implementato come sopra indicato.

In generale la sua vigilanza ha come finalità quella di valutare se le decisioni della gestione legate all'IA rispettino le leggi e supportino gli obiettivi aziendali, se i rischi siano identificati e mitigati anche grazie ad una governance societaria efficace e se i dipendenti ricevano una adeguata formazione. Qualora la società utilizzi sistemi di monitoraggio continuo, controllo automatico o soluzioni di AI a supporto del sistema di controllo interno, il collegio sindacale verifica che tali strumenti siano adeguati, proporzionati rispetto alla natura dell'impresa e ai rischi cui essa è esposta, e non sostituiscano le responsabilità e il giudizio critico delle funzioni umane di controllo.

GLI USE CASE DEL PARAGRAFO

Use Case 6: Charter del comitato controllo e rischi (o Comitato endoconsiliare equivalente dell'organo di amministrazione, se costituito)

Contesto

Il consiglio di amministrazione ha nominato un comitato controllo e rischi ma non ha formalizzato le responsabilità sull'IA né assegnato ad altri comitati consiliari tali responsabilità.

Azioni dei preposti alla gestione aziendale

- Formalizzare nel charter del comitato controllo e rischi i compiti in materia di IA, con ruoli e limiti chiari.
- Nominare un referente manageriale dedicato (es. CIO, Chief Data/AI Officer) con *reporting* periodico al consiglio di amministrazione.
- Aggiornare le policy aziendali su IA in coerenza con AI Act (*provider/deployer*) e, tenendo conto entro i limiti ritenuti opportuni ed applicabili alla circostanza, ISO/IEC 42001 (ambito e responsabilità).

Azioni dell'Organo di controllo

Il collegio sindacale sollecita il consiglio di amministrazione ad assegnare le responsabilità a un comitato consiliare e analizza criticamente delibere e verbali per verificare se esista una delega chiara sulla supervisione dell'IA, con ruoli definiti anche manageriali (es. CIO, Chief AI Officer). Verifica se le policy aziendali sono approvate, aggiornate e in linea con AI Act (ruoli: *provider*, *deployer*, etc.) e ISO/IEC 42001 (scope e responsabilità).

Risultato Atteso

Implementazione di una governance dell'AI che coinvolga adeguatamente l'organo di gestione.

Use Case 7: Bias da Machine Learning

Contesto

Un sistema di *scoring* clienti restituisce risultati discriminatori delle società petrolifere in base ai dati di addestramento discriminatori rispetto al settore desumibili dalle tendenze rilevabili digitalmente.

Azioni dei preposti alla gestione aziendale

- Documentare i *dataset* di *training***,** con tracciabilità delle fonti e giustificazione della loro affidabilità.
- Implementare procedure di validazione per identificare e mitigare *bias* (metriche di *fairness*, test di robustezza).
- Istituire una revisione periodica dei modelli con audit interni e, se necessario, terze parti indipendenti.
- Integrare nei processi di governance aziendale la gestione dei rischi legali e reputazionali legati a *bias*.

Azione dell'organo di controllo

Il collegio sindacale richiede informazioni sui dati di *training*, valuta se esistano procedure di validazione delle fonti metriche per identificare *bias* e processi di revisione periodica.

Risultato atteso

Garantire che l'azienda prevenga rischi di discriminazione o inefficacia, riducendo impatti legali e reputazionali.

Use Case 8: Sicurezza e resilienza dei sistemi di IA

Contesto

Una società quotata del settore industriale utilizza un sistema di IA per il controllo di impianti produttivi. Un attacco informatico mirato tenta di manipolare i dati di *input* per alterare le previsioni di manutenzione e causare blocchi della linea. I sistemi rilevano un'anomalia ma la segnalazione viene

gestita con ritardo perché mancano procedure integrate di *incident response* e ruoli ben definiti per la gestione di emergenze IA.

Azioni dei preposti alla gestione aziendale

- Redigere e aggiornare un piano di sicurezza IA integrato con la *cyber policy* aziendale.
- Effettuare test periodici di resilienza (*penetration test*, *red teaming* specifico su IA).
- Definire ruoli, flussi e procedure documentate di *incident response* e *reporting* (incluso registro anomalie).
- Attivare un programma di *audit* interno e *follow-up* per verificare l'efficacia delle azioni correttive.
- Allineare le pratiche alle prescrizioni dell'AI Act per sistemi ad alto rischio.

Azioni dell'organo di controllo

Alla luce dell'accaduto, il collegio sindacale chiede alla struttura aziendale preposta, previa valutazione delle circostanze:

- evidenza di un piano di sicurezza IA aggiornato e coerente con la *cyber policy* aziendale;
- le risultanze dei test di resilienza effettuati periodicamente (*penetration test*, *red teaming* specifico su modelli IA);
- evidenza dell'esistenza di:
  - ruoli e flussi informativi chiari in caso di attacco informatico (chi segnala, chi decide, chi interviene);
  - registri delle anomalie e delle azioni correttive intraprese;
  - procedure documentate di *incident reporting*, come richiesto dall'AI Act per i sistemi ad alto rischio.
- audit interni e *follow-up* per monitorare l'implementazione delle azioni correttive.

Risultato Atteso

L'azienda integra nella propria governance IA un sistema strutturato di sicurezza e risposta agli incidenti, riducendo il rischio operativo e reputazionale.

Use Case 9: Coinvolgimento degli stakeholders responsabili

Contesto

Una società quotata del settore assicurativo sta implementando un modello di IA per la gestione dei sinistri e la personalizzazione delle polizze. Le decisioni operative sul modello, inclusi criteri di valutazione e fonti dati, vengono prese quasi esclusivamente dalla funzione IT, senza un confronto strutturato con i responsabili di compliance ed il consiglio di amministrazione. Di conseguenza, rischi legati a *bias*, impatti sui clienti e responsabilità legali non sono pienamente considerati a livello strategico.

Azioni dei preposti alla gestione aziendale

- Coinvolgere formalmente il consiglio di amministrazione e le funzioni chiave (Compliance, Risk Management, Business) nelle decisioni sull'IA.
- Creare un meccanismo strutturato di coordinamento interfunzionale per la gestione di rischi, impatti e opportunità.
- Organizzare programmi di formazione dedicati per dirigenti e consiglieri sul governo dell'IA.
- Produrre report integrati che dimostrino l'allineamento delle scelte IA con gli obiettivi aziendali, l'AI Act e la ISO/IEC 42001.
- Evitare che le decisioni operative restino confinate alla sola funzione IT.

Azioni dell'organo di controllo

Il collegio sindacale chiede:

- che il consiglio di amministrazione intervenga sul tema, con analisi di impatti, rischi e opportunità;
- la creazione di un meccanismo di coordinamento tra funzioni tecnologiche, legali, di business e risk management;
- programmi di formazione per dirigenti e componenti del consiglio di amministrazione, così che comprendano rischi e benefici dell'IA;
- report che dimostrino l'allineamento delle scelte IA agli obiettivi aziendali e ai requisiti di AI Act e ISO/IEC 42001.

Risultato Atteso

Le decisioni sull'IA diventano trasversali e consapevoli: il consiglio di amministrazione e le altre funzioni chiave partecipano attivamente, riducendo il rischio di implementazioni isolate e assicurando che l'IA sia trattata come leva strategica e conforme alle norme e agli standard di governance.

Use Case 10: AI che influenza le fasi preliminari del processo decisionale (pre-decision capture)

Scenario

La società utilizza sistemi di AI generativa o *general purpose* (es. assistenti virtuali, strumenti di analisi documentale, sistemi predittivi) a supporto di attività di analisi, preparazione report, sintesi dati o predisposizione di scenari decisionali. In alcuni casi, tali sistemi non si limitano a fornire dati, ma reinterpretano la richiesta dell'utente, selezionano quali informazioni includere o escludere, oppure propongono direttamente un'impostazione del problema, anticipando o condizionando l'istruttoria decisionale.

Azioni dei preposti alla gestione aziendale

- Documentare, con modalità sostenibili, se e quando l'AI modifica il prompt originario, sceglie le fonti, esclude variabili o genera contenuti non riconducibili a dati verificabili;

- Quando l'azienda utilizza agenti di AI sviluppati o configurati internamente, può essere previsto, già in fase di progettazione, l'inserimento di "istruzioni permanenti" (*system prompt* o filtri logici) che impongano al sistema di:
    1. non generare contenuti privi di fonte o basati su inferenze non dichiarate;
    2. non estendere autonomamente il perimetro dell'analisi oltre le informazioni disponibili;
    3. dichiarare esplicitamente quando un *output* è ipotetico, stimato o non fondato su dati verificabili.
- Introdurre criteri minimi di tracciabilità ("audit trail leggero"): storico delle richieste (prompt), indicazione dell'eventuale riformulazione algoritmica, distinzione tra dati reali e *output* generativo o predittivo;
- Integrare programmi di formazione sul "Prompt Engineering critico", insegnando agli utenti a:
    - chiedere fonti e logiche dell'*output*;
    - distinguere dato verificato da contenuto inferenziale;
    - interrogare l'AI con domande esplorative e non solo con richieste di risposta unica.
- Comunicare e rendere accessibili le procedure interne sull'uso dell'AI, incluse le regole minime per il prompting consapevole, a tutte le funzioni aziendali coinvolte.

<u>Azioni dell'organo di controllo</u>

Nell'ambito delle proprie funzioni *ex* art. 2403 c.c. e art. 149 TUF, il collegio sindacale può:

- verificare che il management abbia valutato il rischio che l'AI influenzi la fase istruttoria e non solo la decisione finale;
- validare che siano state definite e comunicate procedure interne sull'utilizzo dell'AI, incluse quelle relative alla formazione o al *prompting* consapevole;
- chiedere evidenza dell'esistenza di attività formative rivolte a dipendenti o funzioni critiche, finalizzate a evitare l'affidamento acritico agli *output* e a promuovere pensiero critico;
- laddove l'azienda sviluppi o personalizzi agenti AI per attività di analisi o supporto decisionale, vigila che siano previste istruzioni di sistema (*system prompt*) o filtri predefiniti che limitino la generazione di contenuti privi di fonte, impediscano omissioni istruttorie e assicurino che il contributo dell'AI resti supportivo e non sostitutivo della valutazione umana.

<u>Risultati attesi</u>

- Maggiore consapevolezza che il rischio di *decision capture* può originarsi prima della decisione, nella fase di preparazione delle informazioni.
- Presidio proporzionato del rischio, senza ostacolare l'uso dell'AI, ma garantendo tracciabilità, pensiero critico e autonomia del giudizio umano.
- Diffusione di competenze di *prompting* responsabile e pensiero critico sull'AI tra il personale aziendale.

- Maggior efficacia preventiva del sistema di controllo interno “by design” per eventuali anomalie nei processi decisionali.

4. Gestione dei rischi legati all’IA

Con riguardo all’adozione di sistemi di intelligenza artificiale, l’obiettivo del collegio sindacale è di vigilare non solo che i rischi siano stati formalmente censiti dal consiglio di amministrazione, ma che la loro gestione sia coerente e continuativa rispetto all’evoluzione dei modelli impiegati e che l’azienda disponga di presidi organizzativi e procedure in grado di monitorare la mitigazione di tali rischi.

4.1. Tassonomia dei rischi e campo di applicazione

In base a una preliminare macro-definizione dei rischi, il collegio sindacale vigila che il management abbia ricompreso nel proprio modello di gestione dei rischi almeno le seguenti tipologie:

- rischi tecnici: performance (accuratezza, robustezza, drift e obsolescenza), sicurezza del modello e dei dati (manipolazioni, avvelenamento dati, attacchi malevoli), disponibilità (*fault*, continuità operativa) e integrità (cambiamenti non autorizzati di modelli/dataset);
- rischi di *bias* e discriminazione: distorsioni nei dati e nei modelli (esiti sistematicamente sfavorevoli o favorevoli per gruppi specifici o categorie di clienti/dipendenti), *proxy bias* e *disparate impact*;
- rischi legali e di conformità: pratiche vietate, obblighi *high risk* per *provider/deployer*, trasparenza (chatbot, contenuti sintetici), gestione di modelli GPAI (General Purpose AI o AI di uso generale non progettati per un solo scopo), come ChatGPT o modelli fondazionali., requisiti privacy, proprietà intellettuale e responsabilità;
- rischi operativi e di terze parti: errori di processo, dipendenze da fornitori e API (Application Programming Interface, ossia interfaccia che consente a sistemi diversi di comunicare/scambiare dati o servizi) uso di modelli/fondazioni esterni, SLA e licenze;
- rischi reputazionali e di diritti fondamentali: opacità, *explainability* insufficiente, contenziosi, perdita di fiducia di clienti, investitori e dipendenti.

Il collegio sindacale vigila che l’azienda abbia definito una tassonomia di rischio IA coerente con il proprio perimetro (prodotti/processi/unità).

4.2. Identificazione, valutazione e *scoring* del rischio

Successivamente alla definizione della tassonomia, il collegio sindacale raccoglie informazioni sulle modalità con le quali il management ha attuato le seguenti azioni:

- inventario e classificazione: per ogni sistema IA, identificare finalità, dati in *input*/*output*, attori (*provider/deployer*), canali di decisione (automatica vs *human-in-the-loop*), e livello di rischio AI Act;
- metodologia di *scoring*: definire criteri e pesi (es. impatto su persone/mercato, probabilità di errore, esposizione regolatoria, dipendenza da terzi) con soglie di escalation;
- Valutazioni d'impatto: ove applicabile, privacy e valutazioni sui diritti fondamentali/etiche; per *high risk*, verifiche specifiche richieste dall'AI Act.

L'obiettivo è di mantenere un inventario aggiornato, schede sistema (*model card/data sheet* o strumenti equivalenti), matrice di *scoring*, verbali di classificazione, pareri legale/compliance.

4.3. Piani di trattamento e controlli

Per ogni rischio rilevante, è opportuno che la società predisponga un piano di trattamento con responsabilità, scadenze, KPI/KRI e controlli di efficacia.

Per i sistemi di intelligenza artificiale, i principali elementi da presidiare possono essere riassunti come segue:

- dati utilizzati dall'AI, controllo di origine, qualità e aggiornamento dei dati, verifica che eventuali errori o distorsioni nei dati siano corretti, tracciamento di chi modifica i dati e con quali autorizzazioni;
- modelli di AI, verifica che i modelli siano testati e validati anche da soggetti indipendenti, controllo periodico che funzionino come previsto (*backtest, stress test*), documentazione delle versioni utilizzate e ogni modifica effettuata;
- *bias* e imparzialità, monitoraggio per verificare se l'AI produca risultati discriminatori o distorti, analisi indicatori e soglie di allerta, verifica di soggetti indipendenti dei risultati su categorie o dati sensibili;
- sicurezza e protezione dei sistemi, progettazione dei sistemi in modo sicuro fin dall'inizio (*secure by design*), protezione degli accessi, credenziali e dati sensibili, *testing* dei sistemi simulando attacchi o usi impropri, monitoraggio di eventuali incidenti o minacce;
- supervisione umana, chiara individuazione dei momenti e delle circostanze nelle quali l'umano debba intervenire, garanzia di poteri di blocco o modifica delle decisioni dell'AI (*override/kill switch*), previsione di una doppia approvazione per decisioni rilevanti;
- controlli operativi in esercizio, monitoraggio nel tempo delle performance del sistema (es. accuratezza, deviazioni, tempi di risposta), conservazione dei log delle attività svolte, predisposizione di alert automatici e procedure di gestione degli incidenti.

Il collegio sindacale acquisisce la documentazione a supporto della esistenza ed efficacia del *risk register* IA con i relativi piani di trattamento, verificando l'individuazione di ruoli chiari e la tracciabilità delle decisioni.

4.4. Terze parti, fornitori e catena di fornitura

La gestione delle terze parti è un elemento essenziale per garantire affidabilità, sicurezza e qualità dei sistemi di IA, anche quando l'organizzazione non sviluppa internamente tutti i componenti. Il collegio sindacale vigila tramite discussione con il management che:

- sia stato predisposto un processo di due diligence sui fornitori e sui modelli esterni, per valutare solidità, affidabilità e qualità dei dati o degli algoritmi utilizzati. Questo include verifiche sulle licenze, sulla governance dei dati e sulla disponibilità di supporto tecnico e operativo;
- nei contratti con fornitori o partner siano previste clausole chiare di qualità, sicurezza e tracciabilità, in linea con quanto indicato da ISO/IEC 42001 per i sistemi di gestione dell'IA;
- siano presenti procedure interne per il monitoraggio continuo dei rischi di filiera, incluse verifiche periodiche delle prestazioni e della conformità dei sistemi forniti da terzi;
- venga gestito il fenomeno della "shadow AI" (utilizzo di strumenti IA non autorizzati): l'organizzazione dovrebbe prevedere un processo di "intake".

4.5. Monitoraggio, KPI/KRI e *reporting*

Il monitoraggio dei sistemi di IA non può limitarsi a verifiche episodiche, ma deve prevedere un processo strutturato e continuo, capace di fornire al management informazioni tempestive e affidabili sul funzionamento, sui rischi e sulle performance.

Indicatori di performance e di rischio

KPI (Key Performance Indicators): devono misurare l'efficacia e l'efficienza dei sistemi di IA, includendo metriche come accuratezza dei modelli, copertura delle previsioni, tempo medio di decisione, produttività e riduzione degli errori.

KRI (Key Risk Indicators): devono intercettare segnali di rischio, come tassi di override da parte degli operatori umani, scostamenti significativi per gruppi o segmenti, numero e gravità degli incidenti, model drift (deriva delle prestazioni), violazioni SLA o anomalie di sicurezza.

Reporting e trasparenza informativa

I risultati del monitoraggio devono essere consolidati in cruscotti periodici e comunicati al consiglio di amministrazione, al comitato controllo e rischi.

Devono essere previsti report di eccezione (*exception reporting*) per evidenziare eventi critici scostamenti dai target, accompagnati da piani di rientro, date obiettivo e responsabilità assegnate.

Ogni incidente rilevante deve produrre un'analisi delle cause (*lessons learned*) e aggiornare procedure e controlli, alimentando un ciclo di miglioramento continuo.

Responsabilità del consiglio di amministrazione

Il collegio sindacale vigila che il consiglio di amministrazione fornisca le linee di indirizzo per:

- la gestione degli incidenti vale a dire fornire le linee di indirizzo per la predisposizione di procedure per la classificazione (tecnica, etica, legale), la notifica tempestiva interna ed esterna, l'analisi *post mortem* e la *root cause analysis*, (cioè l'analisi per identificare la causa a monte primaria di una anomali o di un problema) con registrazione sistematica degli eventi;
- le azioni correttive e preventive (CAPA - Corrective and Preventive Actions): definire responsabili, scadenze e verifiche di efficacia per ogni azione, assicurando che le problematiche non si ripetano;
- i riesami e lo svolgimento di audit, vale a dire eseguire audit periodici su modelli, fornitori e processi; condurre riesami di direzione per aggiornare strategie e controlli;
- non conformità, incidenti e miglioramento continuo.

La gestione di non conformità e incidenti è parte integrante del ciclo di *risk management* e del miglioramento continuo. L'obiettivo è garantire che ogni evento anomalo diventi occasione di apprendimento e rafforzamento dei controlli.

Vigilanza del collegio sindacale

È opportuno che il collegio sindacale acquisisca periodicamente la reportistica nonché le evidenze della verifica di qualità e affidabilità dei dati riportati; in caso di ritardi o rischi non mitigati, sarà opportuno coinvolgere il consiglio di amministrazione ovvero il comitato rischi o altro comitato con funzioni equivalenti al fine di accertarsi che siano intraprese azioni correttive ovvero le stesse siano state effettivamente implementate e chiuse.

In sintesi, l'attività del collegio sindacale deve essere orientata, al di là delle singole modalità adottate dalla società, a vigilare che l'impianto istituito dal management su indirizzo del consiglio di amministrazione fornisca una ragionevole evidenza che i rischi IA siano identificati, valutati e trattati in modo coerente con una efficace gestione dell'AI e che misure di contenimento efficaci e verificabili attraverso un sistema di governance contraddistinto da una attitudine al miglioramento continuo e alla tutela degli stakeholder e del valore aziendale siano adottate.

GLI USE CASE DEL PARAGRAFO

Use Case 11: Non conformità, incidenti e miglioramento continuo

Contesto

Dopo il rilascio di un sistema di pricing dinamico, il management ha predisposto cruscotti mensili: accuratezza, tempo di decisione, produttività, tassi di intervento umano, scostamenti per segmento e incidenti registrati. Alcuni indicatori mostrano oscillazioni inattese in una regione.

Azioni dei preposti alla gestione aziendale

- Predisporre cruscotti periodici con indicatori chiave (accuratezza, tempi, produttività, incidenti).
- Analizzare le oscillazioni anomale e documentare cause e azioni correttive con tempi di rientro.
- Fornire report chiari al consiglio di amministrazione con evidenza delle priorità e responsabilità.
- Aggiornare la reportistica con coerenza rispetto agli impegni presi.

Azioni dell'organo di controllo

Il collegio sindacale prende visione della reportistica periodica e chiede informazioni in ordine alle cause delle oscillazioni, alle azioni in corso e i tempi di rientro. Invita a mantenere evidenza di eventuali problematiche e dei piani di rimedio associati per risolverle, così che il consiglio di amministrazione abbia una lettura ordinata di priorità e responsabilità. Successivamente verifica che il racconto dei numeri sia coerente con gli impegni presi.

Risultato atteso

Un monitoraggio continuo che consente di individuare precocemente deviazioni, con piani di rientro chiari e una comunicazione al consiglio di amministrazione tempestiva.

Use Case 12: "Shadow AI"

Contesto

La funzione clienti intende integrare un modello linguistico esterno per automatizzare parte delle risposte. Il fornitore è internazionale; alcune funzionalità richiedono invio di porzioni di testo contenenti dati sensibili.

Azioni dei preposti alla gestione aziendale

- Condurre due diligence sui fornitori esterni di IA (qualità, sicurezza, gestione dei dati).
- Definire clausole contrattuali chiare su tracciabilità ai fini dell'audit, continuità e supporto.
- Attivare un processo interno di autorizzazione per strumenti di IA esterni, con controlli contro usi non autorizzati.
- Monitorare periodicamente le prestazioni dei fornitori e comunicare gli esiti al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale chiede informazioni in ordine alle modalità con cui la direzione ha condotto la due diligence sul fornitore (qualità del servizio, sicurezza, gestione dei dati), le clausole contrattuali su qualità, tracciabilità, supporto e continuità e il processo interno di autorizzazione per strumenti esterni, compresi i presìdi contro usi non autorizzati. Successivamente chiede di essere aggiornato sugli esiti del monitoraggio periodico delle prestazioni e sui controlli applicati ai flussi di dati.

Risultato atteso

Gestione dei fornitori nell'ambito di un quadro di responsabilità definite in modo chiaro, individuazione di modalità contrattuali adeguate e di un processo interno che previene "shadow AI" e fuoriuscite di informazioni critiche.

Use Case 13: Monitoraggio tramite indicatori

Contesto

L'azienda ha avviato un algoritmo predittivo per la manutenzione, ma non ha definito indicatori chiave.

Azioni dei preposti alla gestione aziendale.

- Definire indicatori chiave di performance (accuratezza, tasso di errore, tempi di intervento).
- Implementare procedure di *logging* e sorveglianza umana per i sistemi classificati ad alto rischio.
- Mantenere documentazione tecnica aggiornata dei modelli e dei processi di validazione.
- Fornire report periodici al consiglio di amministrazione sull'andamento dei sistemi.

Azioni dell'organo di controllo

Il collegio sindacale chiede al management di presentare le metriche di performance (accuratezza, tasso di errore), le procedure di *logging* e sorveglianza umana per sistemi ad alto rischio, e la documentazione tecnica dei modelli.

Risultato Atteso

Adozione dei sistemi IA governata, misurata e conforme alle politiche interne e all'AI Act.

Use Case 14: Risk Management

Contesto

Un produttore industriale utilizza l'IA per manutenzione predittiva e per visione artificiale su linea. Test iniziali hanno evidenziato drift del modello e alcune segnalazioni di falsi positivi. Il management ha predisposto un piano di trattamento che tocca dati, modelli, supervisione umana e sicurezza.

Azioni dei preposti alla gestione aziendale

- Predisporre un registro dei rischi relativo ai sistemi di IA con interventi programmati, responsabilità e scadenze.
- Aggiornare periodicamente il registro, indicando avanzamenti e azioni chiuse.
- Monitorare in particolare i casi ripetitivi di *drift* e falsi positivi, con piani specifici di trattamento.
- Comunicare in modo strutturato gli stati di avanzamento al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale, all'inizio del mandato, acquisisce il registro dei rischi riferito ai sistemi di IA con gli interventi programmati, responsabilità e scadenze. Nei trimestri successivi segue lo stato di avanzamento e la chiusura delle azioni pianificate per ridurre al minimo i falsi postivi, ponendo particolare attenzione ai casi ripetitivi che, se non adeguatamente monitorati, potrebbero produrre conseguenze significative sulla efficacia ed efficienza dei costi di manutenzioni.

Risultato atteso

Individuazione di un piano di trattamento credibile e tracciato, controlli operativi misurabili e un ciclo di miglioramento che riduce progressivamente gli eventi ricorrenti.

Use Case 15: Piani di trattamento e controlli

Contesto

Una società finanziaria introduce un modello che pre-valuta le pratiche di credito. Il management ha predisposto schede di sistema, classificazione del livello di automazione, matrici di *scoring* del rischio e una valutazione d'impatto sui dati personali.

Azioni dei preposti alla gestione aziendale

- Mantenere inventario aggiornato dei sistemi con schede descrittive (finalità, *input*/*output*, canale decisionale, ruoli).
- Definire matrici di *scoring* del rischio e scale di priorità con soglie di escalation.
- Predisporre valutazioni d'impatto sui dati personali e aggiornarle in caso di variazioni.
- Documentare variazioni di *scoring*, nuove evidenze e impatti organizzativi e riferirne al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale prende visione dell'inventario aggiornato, delle schede descrittive (finalità, *input*/*output*, canale decisionale, ruoli aziendali coinvolti), della metodologia di *scoring* con criteri e soglie di escalation e delle valutazioni d'impatto svolte. Chiede informazioni circa la graduazione delle priorità dei rischi, le tempistiche dei controlli e le modalità con cui vengono registrate le decisioni di classificazione. Nel prosieguo chiede aggiornamenti su variazioni di *scoring*, nuove evidenze e impatti organizzativi.

Risultato atteso

Un sistema di valutazione trasparente e ripetibile, documenti coerenti (schede, matrici, verbali) e un legame evidente tra livello di rischio e profondità dei controlli programmati.

Use Case 15: Tassonomia dei rischi e campo di applicazione

Contesto

Un gruppo retail opera con più sistemi di IA: motore di raccomandazione in e-commerce, chatbot per l'assistenza, analisi antifrode nei resi e una soluzione per l'assegnazione turni del personale. I progetti sono nati in momenti diversi e non esiste ancora una tassonomia unica dei rischi né una mappatura completa.

Azioni dei preposti alla gestione aziendale

- Redigere e mantenere aggiornata la mappatura completa dei sistemi di IA in uso e in sviluppo.
- Classificare ciascun sistema secondo categorie di rischio (tecnico, legale, reputazionale, ecc.) e livello (alto, limitato, vietato).
- Assegnare un responsabile chiaro per ogni sistema.
- Integrare la tassonomia dei rischi nei processi decisionali e nei piani di progetto, comunicando regolarmente gli aggiornamenti al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale acquisisce dal management l'elenco dei sistemi in uso e in sviluppo, come questi ultimi siano stati ricondotti a categorie di rischio omogenee (tecnici, *bias*, legali, operativi, reputazionali) e quale etichetta di rischio è stata attribuita a ciascuno (vietato, alto, limitato, altro). Chiede informazioni circa la funzione responsabile per ogni sistema e circa le modalità tramite cui la tassonomia si riflette nei processi decisionali e nei piani di progetto. Il collegio sindacale pianifica quindi in occasione delle successive riunioni di ottenere informazioni sugli aggiornamenti alla mappa e delle eventuali variazioni di perimetro.

Risultato atteso

Mappatura dei rischi chiara e mantenuta tale nel tempo, con tassonomia applicata in modo coerente e con identificazione di un responsabile per ogni sistema: base necessaria per le fasi successive di analisi e controllo.

Use Case 16: AI per assunzione di personale

Contesto

Una società quotata nel settore tecnologico introduce un sistema di IA per la selezione del personale che utilizza algoritmi di screening automatico dei CV e di valutazione dei candidati tramite interviste video e test cognitivi. Questa applicazione, rientrando tra i sistemi ad alto rischio ai sensi dell'AI Act (Allegato III, n. 4 "Occupazione, gestione dei lavoratori e accesso al lavoro autonomo"), incide direttamente su decisioni con impatti significativi sui diritti della persona, potendo generare rischi di discriminazione, *bias* algoritmici e contenziosi legali.

Azioni dei preposti alla gestione aziendale

- Classificare correttamente il sistema come ad alto rischio ai sensi dell'AI Act.

- Effettuare audit sui dati di training per verificarne diversità delle fonti e assenza di *bias*.
- Implementare protocolli di sorveglianza umana e possibilità di revisione delle decisioni automatizzate.
- Fornire informative chiare a candidati e dipendenti sui diritti e sull'uso dell'IA.
- Tenere un registro aggiornato delle decisioni e delle anomalie, con azioni correttive tracciate.
- Coordinare le funzioni HR, legale, compliance e IT, riferendo al consiglio di amministrazione.

Azioni dell'organo di controllo

Il collegio sindacale raccoglie informazioni e vigila che:

- il sistema sia stato correttamente classificato come ad alto rischio e che siano rispettati i requisiti dell'AI Act;
- esistano procedure di audit sui dati di training per garantire diversità, qualità e assenza di *bias*;
- siano stati predisposti protocolli di sorveglianza umana sulle decisioni automatizzate e possibilità di revisione delle scelte;
- le informative a candidati e dipendenti siano chiare, con indicazione delle modalità di utilizzo dell'IA e dei diritti di reclamo;
- sia presente un registro aggiornato delle decisioni e delle anomalie, con piani di miglioramento e vi sia un coordinamento tra le funzioni HR, legale, compliance e IT per garantire la robustezza del processo.

Il collegio sindacale inoltre chiede evidenze sulle azioni correttive adottate in caso di anomalie.

Risultato atteso

Dimostrare che l'uso dell'IA nelle decisioni HR è conforme all'AI Act, si basa su criteri di trasparenza ed è monitorato, riducendo rischi di contenzioso, danni reputazionali e sanzioni. L'attività di vigilanza tutela i diritti della persona e rafforza la fiducia di stakeholder e autorità, garantendo un approccio responsabile all'innovazione in ambito risorse umane.

Use Case 17: Continuità operativa e dipendenza da un fornitore di modelli nel customer care

Contesto

Una società del settore utility decide di introdurre un sistema conversazionale per il servizio clienti basato su un modello linguistico fornito da un operatore estero. Il business case prevede riduzione dei tempi di risposta del 30% e migliore qualità delle soluzioni. Il progetto è critico: un malfunzionamento avrebbe impatto reputazionale e operativo; la dipendenza dal fornitore introduce rischio di continuità. Il consiglio di amministrazione fornisce al management le linee di indirizzo per la redazione di un piano che unisca obiettivi economici e presìdi di affidabilità e lo approva. Il management presenta un assetto a tre livelli: primo, integrazione dell'assistente virtuale con chiari punti di passaggio all'operatore umano; secondo, misure di qualità e sicurezza dei dati; terzo, continuità operativa con piani di *fallback*

(riduzione del perimetro automatizzato, instradamento a operatori, messaggistica al cliente). Il rapporto con il fornitore è regolato da impegni su qualità del servizio, supporto e possibilità di audit; è prevista una sessione di pre-audit interna prima della messa in esercizio e un audit indipendente a sei mesi dal go-live. La reportistica verso il consiglio di amministrazione comprende indicatori su tempi di risposta, escalation all'operatore, reclami e incidenti, insieme allo stato delle azioni correttive.

Azioni dei preposti alla gestione aziendale

- Redigere un piano che unisca obiettivi economici con presìdi di affidabilità e continuità, da sottoporre al consiglio di amministrazione per l'approvazione.
- Implementare misure di qualità e sicurezza dei dati, con chiari punti di passaggio all'operatore umano.
- Definire piani di *fallback* in caso di degrado del servizio.
- Stabilire impegni contrattuali con il fornitore su qualità, supporto e auditabilità.
- Svolgere pre-audit interno e audit indipendente a sei mesi dal go-live.
- Fornire report periodici al consiglio di amministrazione con indicatori su tempi di risposta, escalation, reclami e incidenti.

Azioni dell'organo di controllo

Il collegio sindacale prende visione del dossier che ha sostenuto la deliberazione: valutazione dei benefici, analisi dei rischi connessi alla dipendenza dal fornitore, misure di continuità e calendario degli audit. Durante l'esercizio chiede informazioni circa l'andamento degli indicatori, con particolare attenzione a reclami e interruzioni del servizio; quando il pre-audit interno evidenzia aree deboli (ad esempio qualità dei dati di addestramento o tempi di escalation all'operatore), sollecita che le priorità siano portate all'attenzione del consiglio di amministrazione e segue l'evoluzione delle correzioni. Nei verbali documenta i passaggi principali e le motivazioni delle scelte.

Risultato atteso

Il customer care raggiunge gli obiettivi di qualità e velocità senza incidenti rilevanti. In caso di degrado del servizio, i meccanismi di *fallback* entrano in funzione in modo ordinato; gli audit confermano la robustezza dell'impianto e offrono spunti di miglioramento che vengono incorporati nel ciclo successivo. La dipendenza dal fornitore è governata e resa compatibile con gli obiettivi di continuità e reputazione.

5. Compliance normativa e regolamentare

Per quanto attiene al quadro normativo di riferimento, sono da richiamare principalmente l'AI Act, e, con specifico riferimento alla protezione dei dati personali il Regolamento (UE) 2016/679, c.d. GDPR (General Data Protection Regulation).

Con riferimento all'AI Act gli obblighi chiave per *deployer* e (ove rilevante) *provider* sono strutturati rispetto alle seguenti modalità:

- pratiche vietate: gate di ammissibilità e attestazione al consiglio di amministrazione che nessun sistema rientra nell'art. pratiche vietate;
- sistemi ad alto rischio (*deployer*): uso conforme alle istruzioni, sorveglianza umana, qualità dei dati, *logging* e conservazione, informative ai lavoratori/clienti, canali di *incident reporting* e cooperazione con il *provider*/autorità;
- trasparenza (rischio limitato): disclosure per chatbot/contenuti sintetici/*emotion/biometric*;
- GPAI: requisiti di documentazione e (per rischi sistemici) *red teaming*, sicurezza rafforzata e segnalazioni;
- registrazioni: dove previsto, iscrizioni nella banca dati UE e uso solo di sistemi correttamente registrati.

L'entrata in vigore scaglionata del provvedimento rappresenta un punto di attenzione per l'attività di vigilanza del collegio sindacale, in particolare con riferimento all'operatività già dal 2 febbraio 2025 dei divieti riguardanti le applicazioni di intelligenza artificiale non consentite, rispetto agli ulteriori obblighi, come quelli di inventariazione e classificazione delle categorie di rischio delle applicazioni utilizzate in azienda, che troveranno applicazione in una fase successiva, a partire dal 2 agosto 2026. La presenza di eventuali applicazioni proibite dovrà essere accertata dalla società in via preventiva, anticipando quindi l'attività di ricognizione e inventariazione delle applicazioni esistenti, oppure, in alternativa, o a integrazione, ricorrendo a tecnologie di analisi dei dati destrutturati già disponibili in azienda. A titolo esemplificativo, si potrà utilizzare tali tecnologie per analizzare automaticamente tali dati (es. e-mail, documentazione tecnica, conversazioni su piattaforme collaborative, log applicativi, report non strutturati, scambi informali su chat interne) e individuare indicatori o segnali della presenza di casi potenzialmente rientranti nelle fattispecie vietate da sottoporre a verifica con le funzioni di business e con l'ufficio legale, al fine di accertarne la conformità normativa.

5.1. Quadro generale e responsabilità del management/consiglio di amministrazione

La responsabilità primaria dell'adeguamento normativo ricade sul management, sotto l'indirizzo e la supervisione del consiglio di amministrazione. In un assetto integrato AI Act - GDPR la società predispone e mantiene:

a) Inventario e classificazione dei sistemi di IA:

- mappatura dei sistemi/progetti IA, dei relativi processi decisionali e dei flussi di dati personali;
- classificazione del rischio ai fini dell'AI Act (pratiche vietate, alto rischio, rischio limitato, GPAI) e inquadramento del ruolo aziendale (*deployer* e, ove applicabile, *provider*);
- collegamento dell'inventario al Registro dei trattamenti (RoPA) GDPR, con finalità, basi giuridiche, categorie di dati e tempi di conservazione.

b) Data governance e basi privacy:

- definizione di basi giuridiche e informativa trasparente (*privacy notice*) per i trattamenti connessi ai sistemi IA;
- valutazioni d'impatto quando richiesto (profilazione/ADM significative, trattamenti su larga scala, categorie particolari);
- politiche di minimizzazione, qualità e accuratezza dei dati, *retention* e cancellazione; misure di sicurezza (art. 32 GDPR) su dati e modelli.

c) Requisiti tecnici e organizzativi AI Act:

- per i sistemi ad alto rischio (*deployer*): uso conforme alle istruzioni, sorveglianza umana definita, *logging* e conservazione dei log, qualità degli *input*, informative a lavoratori e utenti, canali di gestione/seguito degli incidenti, cooperazione con *provider*/autorità;
- per casi di trasparenza (rischio limitato): regole di *disclosure* (chatbot, contenuti sintetici, *emotion/biometric*);
- per GPAI (se integrati o forniti): documentazione tecnica, informazioni sui dati di addestramento; misure rafforzate ove "a rischio sistemico";
- per i "provider": adottare un sistema di gestione della qualità, tenere un fascicolo tecnico del sistema di IA, svolgere la valutazione di conformità per la marcatura CE (quando prevista) e fare monitoraggio post-commercializzazione del sistema.

d) Ciclo di vita dei modelli e controlli operativi:

- procedure di sviluppo/validazione/rilascio, *explainability* adeguata al rischio, gestione versioni e *change control*;
- metriche KPI/KRI (accuratezza, tassi di *override*, drift, SLA, anomalie per gruppi), cruscotti periodici per consiglio di amministrazione e funzioni di controllo;
- politiche di *incident response integrate* (AI e privacy), con registri, *root cause analysis* (analisi delle cause a monte primarie) e azioni correttive/preventive (CAPA).

e) Terze parti e uso non autorizzato:

- due diligence e requisiti contrattuali per fornitori/modelli (qualità, sicurezza, tracciabilità, supporto), in linea con buone prassi e ISO/IEC 42001;
- processo di "intake" per strumenti esterni e presidi contro shadow AI, inclusi controlli di *egress* dei dati, cioè misure che servono a impedire che dati aziendali escano in modo non autorizzato dall'organizzazione o dai sistemi informativi, soprattutto verso l'esterno (fornitori cloud, piattaforme AI, e-mail personali, dispositivi USB, ecc.).

f) Ruoli, formazione, cultura e *reporting*:

- ruoli e responsabilità formalizzati (*business owner, model owner, data owner*, DPO, compliance, IT), piani formativi mirati e campagne di consapevolezza;

- calendario di *reporting* verso consiglio di amministrazione e comitati, integrazione dei temi IA nei riesami di direzione e nelle pianificazioni annuali.

Alcuni obblighi previsti dall'AI Act "dialogano" direttamente con il disegno e la applicazione di modelli di gestione e di governance così come in precedenza descritti nel documento nonché con analoghe disposizioni che riguardano il GDPR. Una visione integrata di tali aspetti costituisce oltre che un elemento di efficienza nel disegno e nell'attuazione del sistema di gestione e di quelli di compliance una caratteristica fondamentale per assicurare la efficacia dei modello unico.

5.2. Monitoraggio normativo e interlocuzione con le Autorità

L'AI Act prevede sanzioni molto elevate: per le violazioni più gravi (es. pratiche vietate) fino a €35 milioni o il 7% del fatturato mondiale annuo; per altre violazioni fino a €15 milioni o il 3%; per informazioni inesatte fornite alle autorità fino a €7,5 milioni o l'1%. A queste si sommano i rischi GDPR (sino al 4% del fatturato o €20 milioni) e gli impatti reputazionali. Per una società quotata, la conformità e la prontezza documentale sono presidi di valore per investitori, mercato e autorità.

L'art. 20 della legge 23 settembre 2025, n. 132 ha designato l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) quali Autorità nazionali competenti per l'intelligenza artificiale, con funzioni rispettivamente orientate alla regolazione, al coordinamento e alla promozione delle iniziative in materia (AgID) e alla vigilanza sugli aspetti di sicurezza, integrità e resilienza dei sistemi (ACN).

È opportuno che il consiglio di amministrazione abbia:

- individuato un referente unico verso le Autorità AI con delega formale, sostituto, recapiti dedicati e mandato a coordinare Legal/Compliance, DPO, IT/Data, Risk, HR e funzioni di business che abbia il compito di tenere il quadro normativo, raccordare le funzioni, curare le interlocuzioni e lo "stato di prontezza" dell'azienda;
- stabilito un canale formale e una routine di contatto;
- sviluppato una Audit strategy integrata nel piano annuale di Internal Audit che preveda:
  - pre-audit interni periodici sui sistemi IA critici (alto rischio, HR, credito, sicurezza): controllo di contenuti ed evidenze per arrivare agli audit esterni delle Autorità senza sorprese;
  - piano di azioni correttive/preventive con responsabile e data di chiusura, condiviso con consiglio di amministrazione;
- la tenuta in un unico spazio dell'inventario dei sistemi IA con evidenza della classificazione AI Act, collegamento al Registro trattamenti GDPR, DPIA (Data Protection Impact Assessment).
- la valutazione d'impatto privacy per trattamenti dati rischiosi./valutazioni, policy e procedure, istruzioni d'uso/sorveglianza umana, log essenziali e *retention*, registro incidenti, esiti test/red-team, contratti fornitori critici, formazione erogata, cruscotti KPI/KRI e stato CAPA;
- sviluppato un *reporting* al consiglio di amministrazione, ovvero ai comitati consiliari.

- elaborato modalità di preparazione alle ispezioni del personale.

5.3. *Oversight* dell'organo di controllo

Nel rispetto delle prerogative che gli sono riconosciute dall'ordinamento e dei limiti che connotano la funzione di vigilanza, il collegio sindacale in particolare:

- prende visione dei piani di conformità AI Act predisposti dal management e dei relativi avanzamenti, con attenzione a ruoli, scadenze e priorità;
- considera la completezza delle informazioni ricevute avuto riguardo all'inventario dei sistemi di AI utilizzati, classificazione del loro livello di rischio, valutazioni di impatto (DPIA), policy adottate, cruscotti con indicatori di performance/rischio (KPI/KRI) e registri degli incidenti o malfunzionamenti e segnala eventuali aree che richiedono chiarimenti, integrazioni o presìdi più robusti;
- sollecita aggiornamenti sui temi critici (p. es. sistemi ad alto rischio in esercizio, incidenti significativi, interazioni con le Autorità, gestione fornitori strategici).
- promuove il coordinamento tra consiglio di amministrazione, funzioni di controllo e compliance/DPO (Data Protection Officer), responsabile della protezione dati ai sensi del GDPR. Vigila sul rispetto delle norme privacy, quando utili a una migliore integrazione dei presidi;
- prende visione della strategia adottata dalla società finalizzata a favorire canali di interlocuzione con le Autorità AI, delle pianificazioni di audit (interni/terze parti) e dei report periodici;
- acquisisce informazioni sui principali rischi/incidenti gestiti e l'avanzamento delle CAPA;
- formula osservazioni sulle aree che richiedono priorità o risorse, segnala al consiglio di amministrazione eventuali criticità rilevanti e sollecita aggiornamenti su impegni già assunti.

È doveroso evidenziare come il collegio sindacale non sostituisca il management né assuma responsabilità specifiche con riferimento alla compliance della società rispetto a tali normative. La sua azione si colloca infatti unicamente nell'alveo della vigilanza generale sulla conformità dei processi aziendali a quanto previsto nella normativa, con riguardo alla corretta integrazione tra AI Act, GDPR e sistemi di controllo interno.

5.4. *Deliverable* attesi dal management (a supporto dell'*oversight*)

- Inventario dei sistemi di AI, integrato con il registro GDPR (RoPA), indicando per ciascun sistema: finalità, categoria AI Act, responsabile, base giuridica, dati trattati e tempi di conservazione.
- Classificazione del rischio AI Act per ciascun sistema (incluse esclusioni delle pratiche vietate) e, se applicabile, pacchetto "alto rischio" (sorveglianza umana, *logging*, informative).
- Valutazione degli impatti e policy operative su:
  - data governance e sicurezza informatica;

- ADM (Automated Decision-Making e profilazione automatizzata), ossia i processi decisionali basati in tutto o in parte su algoritmi che producono effetti significativi sulle persone o sull'organizzazione;
- *explainability* dell'algoritmo, intesa come la capacità di comprendere, documentare e rendere spiegabili i criteri, i dati e le logiche attraverso cui il sistema di AI genera i propri *output*;
- *change control* dei modelli e dei dati, cioè le procedure che assicurano che ogni modifica ai modelli di AI, agli algoritmi o ai dataset sia tracciata, autorizzata e verificabile, mantenendo coerenza e qualità delle versioni utilizzate.

- Cruscotti KPI/KRI e piani CAPA; registro incidenti.
- Schema fornitori (due diligence, clausole, report periodici) e presidio *shadow* AI.
- Piano formativo e calendario *reporting* a consiglio di amministrazione/comitati.

GLI USE CASE DEL PARAGRAFO

Use Case 18: Trasparenza e gestione di contenuti sintetici

Contesto

Un retailer online integra un chatbot generativo per rispondere ai clienti. Alcuni utenti segnalano risposte fuorvianti (es. informazioni inesatte su termini contrattuali) e contenuti non appropriati. Il rischio riguarda sia la reputazione, sia la responsabilità legale per pubblicità ingannevole.

Azioni dei preposti alla gestione aziendale

- Applicare sistemi di *watermarking* o etichettatura per rendere chiaro che la risposta proviene da un'IA.
- Definire policy interne per la validazione dei contenuti critici (es. clausole legali, prezzi).
- Formare il team di customer care per identificare e segnalare comportamenti anomali del chatbot.
- Implementare un canale rapido di revisione e correzione dei contenuti segnalati.

Azioni dell'organo di controllo

Il collegio sindacale:

- verifica che esista un processo strutturato di monitoraggio dei contenuti generati dall'IA e di gestione dei reclami;
- analizza periodicamente i report di incidenti e valuta se le misure di mitigazione poste in atto dalla società sono state efficaci;
- chiede aggiornamenti al consiglio di amministrazione sui rischi reputazionali e sulle azioni intraprese.

Risultati attesi

Maggiore fiducia dei clienti, riduzione del rischio di reclami o sanzioni per informazioni scorrette, allineamento alle regole di trasparenza previste dall'AI Act.

Use case 19: Interlocuzione con autorità e gestione delle segnalazioni

Contesto

Un gruppo industriale utilizza IA per manutenzione predittiva su impianti critici. Un fornitore segnala una possibile anomalia nei dati raccolti, temendo che i sensori stiano memorizzando informazioni non autorizzate su terzi. L'Autorità competente invia una richiesta formale di chiarimenti.

Azioni dei preposti alla gestione aziendale

- Attivare un Single Point of Contact (SPOC) per interfacciarsi con l'Autorità.
- Avviare un pre-audit interno sul sistema IA per individuare eventuali problemi di raccolta dati.
- Documentare le azioni correttive (CAPA) e predisporre un rapporto da inviare all'autorità.
- Coinvolgere la funzione legale e di compliance per la revisione della risposta ufficiale.

Azioni dell'organo di controllo

Il collegio sindacale vigila che il processo di interlocuzione con l'Autorità competente sia rapido e trasparente. Il collegio sindacale vigila in ordine alla qualità della documentazione prodotta e all'adeguatezza delle misure correttive e informa il consiglio di amministrazione su eventuali rischi residui o impatti economico-reputazionali.

Risultati attesi

Risposta tempestiva e documentata alle richieste ispettive, minimizzazione di sanzioni e danni reputazionali, rafforzamento della governance complessiva sull'uso dell'IA.

6. Utilizzo dei sistemi di AI da parte degli organi di governance

6.1. Ambiti in cui l'AI può supportare le funzioni degli organi societari

L'utilizzo dell'AI nella corporate governance può svilupparsi su tre livelli progressivi: (i) supporto a compiti istruttori e di analisi di dati o documenti; (ii) strumenti che ampliano la capacità informativa del board mediante analisi predittive o scenari alternativi; (iii) sistemi che incidono sulle valutazioni strategiche e sulle decisioni d'investimento. Le cautele e i presidi dell'organo di controllo devono tener conto del livello di impatto del sistema sul processo deliberativo. A titolo esemplificativo, l'adozione di sistemi di intelligenza artificiale può fornire un contributo concreto alle attività del consiglio di amministrazione, dei comitati endoconsiliari e del collegio sindacale, nei seguenti ambiti:

- supporto informativo e documentale, attraverso analisi di bilancio, *benchmarking* settoriale, estrazione di informazioni da documentazione complessa (es. contratti, report industriali);
- analisi predittiva e simulazioni, a supporto della pianificazione strategica, della valutazione di scenari di investimento, dell'analisi dei rischi industriali, finanziari e di continuità aziendale;
- monitoraggio esterno (OSINT), tramite strumenti di raccolta e analisi automatica di informazioni pubbliche su mercati, competitor, fornitori, variazioni normative o reputazionali;
- attività di vigilanza e controllo, in cui l'AI può agevolare l'identificazione di anomalie, trend contabili, scostamenti gestionali o rischi emergenti;
- sorveglianza su *cyber risk* e sicurezza delle informazioni, con sistemi predittivi o di allerta automatica su incidenti o comportamenti anomali.

6.2. Rischi associati all'utilizzo dell'AI nella governance

L'utilizzo di sistemi di AI da parte degli organi di vertice e di controllo richiede adeguata consapevolezza dei rischi connessi, tra cui:

- *decision capture* e *automation bias*: rischio che l'organo accetti in modo acritico gli *output* algoritmici o che la decisione venga, di fatto, anticipata o sostituita dal sistema (*decision proxying*), con perdita di autonomia valutativa, motivazione e responsabilità;
- opacità del processo decisionale: in assenza di tracciabilità delle fonti, dei dati e delle logiche di AI, l'organo potrebbe non essere in grado di ricostruire o giustificare la decisione assunta;
- scelta e dipendenza dagli strumenti: nel caso del collegio sindacale, va evitato che l'adozione di strumenti di AI di supporto alla vigilanza sia decisa dal management o da soggetti sottoposti al controllo;
- rischi di protezione e riservatezza dei dati: utilizzo di piattaforme AI non adeguatamente presidiate sotto il profilo GDPR, segreto aziendale e sicurezza informatica;
- *cybersecurity* e integrità dell'*output*: rischio che dati o modelli siano alterati, manipolati o soggetti a attacchi di tipo malevolo.

6.3. Presidi e condizioni per un uso corretto dell'AI da parte degli organi gestionali di governance

Per garantire che l'utilizzo dell'AI rafforzi le responsabilità degli organi societari, è opportuno che:

- siano adottate policy interne sull'uso dell'AI da parte del consiglio di amministrazione e dei suoi comitati, definendo ambiti consentiti, limiti, requisiti di qualità dei dati, modalità di supervisione e responsabilità;
- sia garantita la tracciabilità del processo decisionale, documentando quando e come l'AI ha supportato l'analisi, distinguendo dati verificabili da elaborazioni inferenziali o predittive;

- venga sviluppata un'adeguata alfabetizzazione in materia di AI (AI *literacy*) anche per i componenti degli organi societari, in coerenza con l'art. 3, n. 56 e l'art. 4 dell'AI Act;
- i sistemi di AI vengano utilizzati come strumento di supporto, e non come metodi di sostituzione della volontà umana, mantenendo l'assunzione di responsabilità individuale e collegiale;
- siano verificati i requisiti di protezione dei dati e resilienza tecnologica dei sistemi di AI utilizzati dal consiglio di amministrazione e dai suoi comitati.

Nell'ambito dei processi di autovalutazione periodica del proprio funzionamento, il consiglio di amministrazione dovrebbe includere una verifica della maturità e dell'efficacia nell'utilizzo di strumenti di AI a supporto delle decisioni, valutando la loro incidenza sulla qualità del processo deliberativo e sull'equilibrio dei flussi informativi interni con particolare riferimento:

- al livello di consapevolezza e comprensione (AI *literacy*) dei componenti del consiglio di amministrazione;
- alla capacità dell'organo di utilizzare sistemi di AI a supporto delle decisioni, mantenendo autonomia critica e tracciabilità del processo deliberativo;
- all'effettiva esistenza di policy interne che disciplinano l'uso dell'AI nei processi informativi e decisionali del board;
- al grado di presidio dei rischi connessi (*automation bias*, *decision capture*, opacità dell'algoritmo, uso improprio di strumenti suggeriti o forniti dal management);
- all'integrazione dell'AI nei flussi informativi al consiglio di amministrazione (*decision support sistem*, *dashboard*, monitoraggi automatici).

6.4. Utilizzo di sistemi di AI da parte del collegio sindacale

L'adozione di strumenti di intelligenza artificiale da parte del collegio sindacale (es. per l'analisi documentale, l'individuazione di anomalie contabili, il monitoraggio di informazioni pubbliche o di flussi informativi) può rappresentare un supporto significativo all'attività di vigilanza.

Tuttavia, tale utilizzo genera, oltre ai rischi già analizzati in precedenza di portata generale, anche specifici profili di rischio, che il collegio sindacale deve considerare in modo consapevole, i più rilevanti dei quali sono:

- *automation bias* del controllore: rischio che il collegio sindacale accetti acriticamente gli esiti forniti dal sistema di AI senza un vaglio autonomo;
- informazioni filtrate o incomplete: l'AI potrebbe selezionare o sintetizzare dati omettendo elementi rilevanti ai fini della vigilanza;
- protezione delle informazioni riservate: l'uso di AI esterne o *cloud-based* deve rispettare segreto d'ufficio, riservatezza delle informazioni societarie e normativa privacy.

Da tale prospettiva è opportuno che il collegio sindacale:

- valuti preventivamente le funzionalità, i limiti e le fonti informative utilizzate dal sistema;
- si assicuri che il sistema consenta, ove tecnicamente possibile, la tracciabilità del contributo dell'AI rispetto alle valutazioni svolte;
- mantenga sempre un controllo umano critico sugli esiti prodotti.

L'utilizzo di sistemi di AI da parte del collegio sindacale, anche mediante l'immissione di documenti e informazioni aziendali, è incoraggiato a condizione che sia rispettata la tutela della riservatezza, del segreto d'ufficio e dell'indipendenza della funzione di controllo. In particolare, il collegio sindacale, nell'avvalersi di sistemi di AI, si assicura che:

- il fornitore della piattaforma o del modello AI rilasci dichiarazioni contrattuali che garantiscano la non utilizzazione dei dati caricati per finalità di addestramento, profilazione o divulgazione a terzi o siano inibite eventuali opzioni previste dalla piattaforma utilizzata. In particolare, prima di utilizzare piattaforme o modelli di AI per l'analisi di documenti aziendali, il collegio sindacale verifica che il contratto di fornitura preveda clausole espresse di riservatezza e non divulgazione dei dati, in modo da assicurare la piena tutela delle informazioni riservate e il rispetto del segreto d'ufficio;
- siano adottate le usuali misure tecniche minime per evitare l'accesso non autorizzato ai documenti trasmessi (es. canali cifrati, accesso autenticato, account aziendali dedicati);
- l'utilizzo dell'AI non determini diffusione, archiviazione esterna non autorizzata o indicizzazione dei documenti in ambienti non controllati;
- permanga la piena responsabilità dell'organo nella valutazione critica degli *output* generati e nella verifica della loro attendibilità.

L'utilizzo dell'AI persegue una maggiore qualità ed efficacia dell'azione di vigilanza del collegio sindacale e quindi qualsiasi limitazione al suo operato in tal senso potrebbe rappresentare un ostacolo alla vigilanza stessa. La società non può introdurre limitazioni o misure tecniche (es. blocchi, decriptazione selettiva dei documenti etc.) che ostacolino una maggiore efficacia dell'attività del collegio sindacale conseguente all'uso di strumenti AI conformi ai suddetti requisiti, fermo restando l'obbligo da parte dei suoi componenti a rispettare le policy aziendali se si utilizzano strumenti di proprietà della società e salvaguardare in qualsiasi caso dati personali, informazioni price sensitive e segreti aziendali.

7. Possibili evoluzioni del quadro regolatorio, annuncio modifiche Omnibus 19 novembre 2025: considerazioni conclusive

Queste Linee Guida riflettono il quadro regolatorio attualmente vigente.

La Commissione europea ha annunciato il pacchetto "Digital Omnibus", che introduce proposte di modifica al GDPR orientate alla semplificazione del trattamento dei dati e a una maggiore compatibilità con l'adozione dei sistemi di intelligenza artificiale. L'annuncio diffuso il 19 novembre 2025 estende l'intervento regolatorio anche all'AI Act, includendo l'ipotesi di una revisione delle tempistiche

applicative e degli obblighi relativi ai sistemi ad alto rischio con la conseguenza che l'attività di vigilanza del Collegio sindacale dovrà considerare scenari applicativi differenziati a seconda dell'esito del processo legislativo e delle eventuali proroghe adottate.

Le informazioni al momento disponibili non consentono di delineare quello che sarà il testo definitivo che a seguito dell'iter legislativo europeo potrebbe conoscere modifiche nei contenuti e nella portata applicativa. Infatti, poiché anche le modifiche ai regolamenti vigenti richiedono la procedura legislativa ordinaria, non è possibile attribuire effetti immediati all'annuncio, né considerare definitive le ipotesi di rinvio dell'AI Act, finché non saranno approvate dal Parlamento europeo e dal Consiglio. È tuttavia possibile delineare, in termini generali, alcune aree nelle quali l'attività di vigilanza del collegio sindacale potrebbe assumere un'impostazione diversa rispetto a quella prevista dal quadro attuale:

1. un primo effetto riguarderebbe la minore complessità nella valutazione della natura dei dati trattati, poiché il perimetro dei dati soggetti a tutela rafforzata risulterebbe più lineare. È quindi possibile che le società possano trovarsi ad affrontare un numero inferiore di casi borderline;
2. la ridefinizione del rapporto tra dati e inferenze alleggerirebbe inoltre la necessità di controlli diffusi sui dataset da parte della società, orientando la vigilanza verso la qualità e l'impatto degli *output* dei modelli più che sulla distinzione tra dato verificato e contenuto inferenziale;
3. l'introduzione di una base giuridica specifica per l'utilizzo di alcune tipologie di dati nei modelli ridurrebbe le verifiche da parte della società basate su divieti assoluti o su presupposti non più necessari. Il collegio sindacale sarebbe chiamato a concentrarsi sui processi aziendali che garantiscono la correttezza della documentazione interna, più che l'imposizione di vincoli totali per finalità di addestramento;
4. l'attenuazione degli obblighi di minimizzazione e la possibilità di mantenere residui di dati all'interno dei modelli comporterebbero per il collegio sindacale una revisione delle modalità di vigilanza sul controllo tecnico sulle attività di rimozione preventiva e di cancellazione totale poste in essere dalla società, dovendosi la vigilanza stessa concentrare maggiormente sui criteri di proporzionalità dichiarati dalla Società stessa;
5. una maggiore flessibilità negli obblighi di trasparenza e di risposta alle richieste di accesso comporterebbe un'attività di vigilanza sulla motivazione e sulla ragionevolezza delle eventuali limitazioni;
6. l'attenzione sui dataset forniti da terzi sarebbe verosimilmente meno stringente rispetto alle logiche attuali e il collegio sindacale si concentrerebbe maggiormente sulla qualità della due diligence e sulla coerenza delle scelte contrattuali da parte della società;
7. per quanto riguarda il tema dei *bias*, l'attività di vigilanza sarebbe più orientata all'analisi degli effetti concreti dei modelli che alla mera rilevazione della natura dei dati in *input* da parte della società;
8. il rapporto tra normativa sulla protezione dei dati e AI Act potrebbe richiedere un intervento di vigilanza diverso nella parte dedicata alla conciliazione dei due regimi, potendo permanere zone di incoerenza laddove l'AI Act non fosse aggiornato in parallelo;

9. la semplificazione del dettaglio richiesto nella tracciatura delle fonti dei dati ridurrebbe il livello di granularità documentale che la società dovrebbe esaminare, orientando la vigilanza verso la coerenza complessiva dei processi istituiti dal management anziché verso la ricostruzione analitica delle categorie di dati da parte della società;
10. la maggiore centralità attribuita all'*accountability* interna porterebbe il collegio sindacale a vigilare principalmente sulla consistenza, la qualità e la verificabilità della documentazione detenuta dalla società, aspetti che assumerebbero un ruolo ancora più centrale nella valutazione dell'adeguatezza dei controlli.

Gli adeguamenti eventualmente necessari saranno introdotti alle presenti linee guida una volta approvato il testo definitivo del regolamento da parte del Parlamento europeo e del Consiglio.

Le modifiche annunciate nel Digital Omnibus non incidono sulla definizione né sull'ambito applicativo delle pratiche vietate dall'AI Act. Le applicazioni vietate rimangono integralmente proibite e non sono soggette ad alcun rinvio o revisione. Il collegio sindacale deve vigilare quindi che la società abbia istituito un processo efficace ad assicurare che nessun sistema IA a essa riferibile ricada in tali categorie, che restano immediatamente e pienamente applicabili alla data di pubblicazione del presente documento. In attesa di chiarimenti sulla possibile revisione delle categorie ad alto rischio dell'AI Act, è opportuno che la Società non interrompa le attività in corso e prosegua la classificazione dei sistemi di IA in base al proprio processo di *risk assessment* interno con l'obiettivo di: *i*) mantenere una mappatura pienamente allineata allo stato dell'arte regolatorio; *ii*) identificare i sistemi per i quali è opportuno posticipare l'implementazione degli adempimenti più complessi, pur preservando la capacità di attivarli tempestivamente; e *iii*) evitare decisioni strutturali basate su anticipazioni non ancora confermate, mantenendo una configurazione aperta che potrà essere ridimensionata qualora il legislatore circoscriva il perimetro degli obblighi assicurando comunque la propria capacità di adeguarsi tempestivamente ed evitando scelte strutturali basate su anticipazioni non definitive.

Appendice

Glossario Terminologico

1. AI Act – *Provider* vs *Deployer*

- *Provider*: il soggetto che sviluppa e immette sul mercato un sistema di AI.
- *Deployer*: l'impresa che utilizza il sistema di AI nei propri processi aziendali.

2. AI di alto rischio

Sistemi di AI che, secondo l'AI Act, incidono in modo significativo su diritti fondamentali, sicurezza o decisioni economiche. Richiedono:

- valutazione del rischio;
- governance dei dati;
- sorveglianza umana;
- registri e tracciabilità.

3. RoPA (Record of Processing Activities) – Registro dei Trattamenti GDPR

Documento obbligatorio per il GDPR che elenca:

- quali dati personali sono trattati;
- per quali finalità;
- da chi (responsabile);
- per quanto tempo.

4. DPIA (Data Protection Impact Assessment)

Valutazione d'impatto sulla protezione dei dati personali richiesta quando un trattamento presenta rischi elevati (es. utilizzo di AI per profilazione, decisioni automatizzate, analisi su larga scala).

5. ADM – Automated Decision-Making / Profilazione automatizzata

Processi in cui una decisione viene presa in tutto o in parte da un algoritmo, senza intervento umano significativo.

6. Explainability (spiegabilità dell'algoritmo)

Capacità di spiegare in modo comprensibile:

- quali dati ha utilizzato il sistema di AI;
- quali passaggi logici ha seguito.

7. Change Control (modelli e dati)

Insieme di procedure per documentare e approvare ogni modifica a:

- algoritmi o modelli di AI;
- dataset utilizzati.

8. KPI / KRI (Key Performance / Risk Indicators)

- KPI: indicatori di performance del sistema AI (accuratezza, tempi, costi).
- KRI: indicatori di rischio (errori, falsi positivi, incidenti, deviazioni dai risultati attesi).

9. Shadow AI

Uso spontaneo e non autorizzato di sistemi di AI da parte di dipendenti (es. ChatGPT gratuito per dati aziendali), al di fuori delle regole aziendali, con rischio di fuga dati.

10. Decision Capture / Automation Bias

Situazione in cui chi decide si affida eccessivamente o automaticamente al risultato fornito da un algoritmo, riducendo il proprio spazio critico o deliberativo.

11. Incident Register / Registro degli incidenti AI

Documento aziendale dove si annotano malfunzionamenti, errori di AI, usi impropri, violazioni o casi in cui l'algoritmo ha fornito risultati errati o distorsivi.

12. Risk Assessment AI

Valutazione sistematica dei rischi derivanti dall'uso dell'AI (operativi, legali, reputazionali, etici) prima di adottarla o modificarla.

13. AI Literacy (alfabetizzazione AI)

Livello minimo di competenze che amministratori, management, sindaci e dipendenti devono possedere su:

- cosa fa e non fa l'AI;
- limiti, rischi e responsabilità;
- impatti sui processi decisionali e dati.

14. Safe Prompting / Prompt Governance

Regole interne che definiscono come utilizzare i sistemi di AI generativa, cosa può o non può essere inserito nei prompt (es. evitare dati riservati), come documentare i risultati usati nei processi aziendali.

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
Piazza della Repubblica, 59 00185 Roma