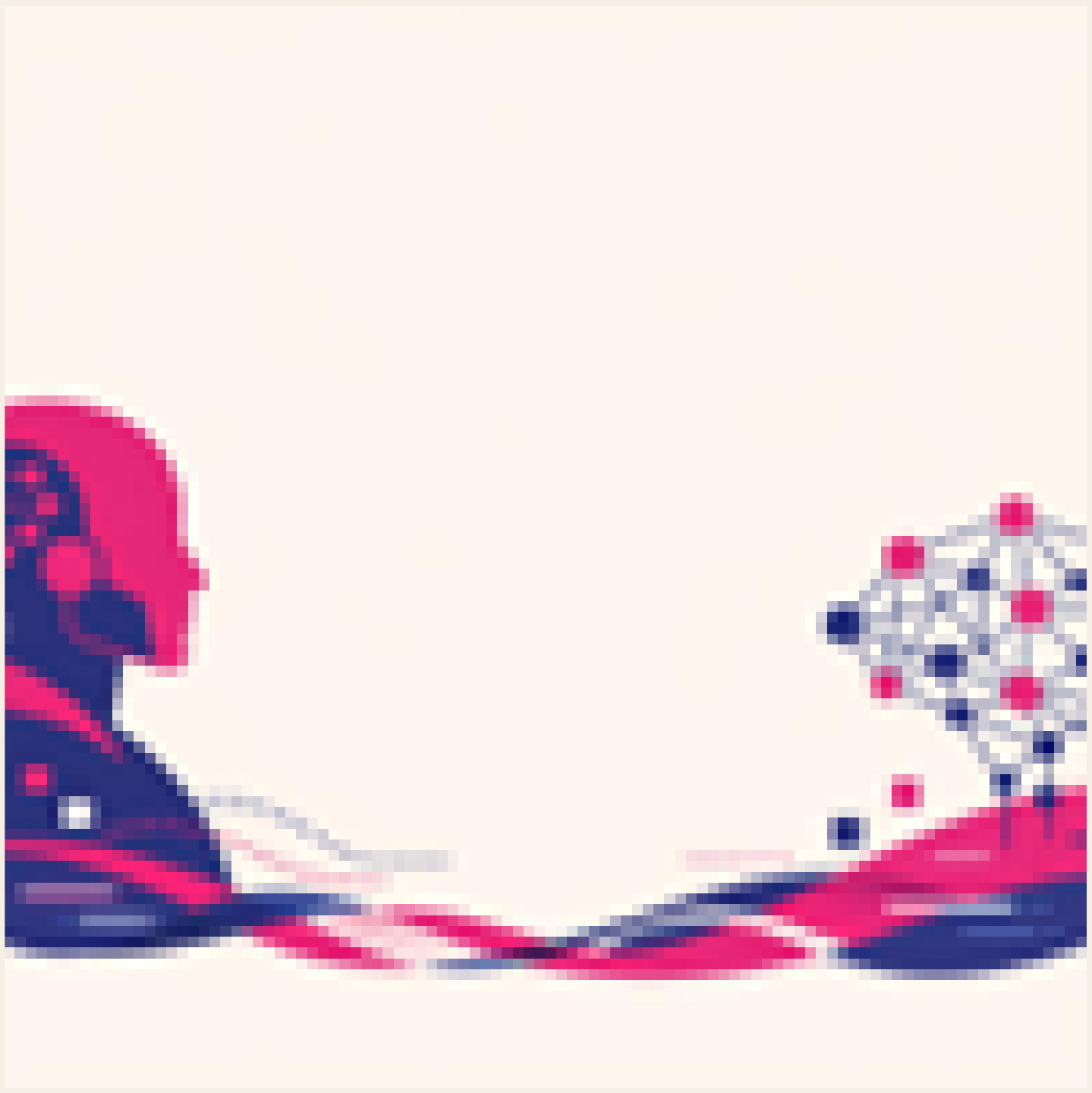


**AI PER L'IMPRESA
RISCHI E RESPONSABILITA'
DERIVANTI DALL'UTILIZZO
DELL'AI**

**GOVERNO
DELL'IMPRESA
COMMERCIALE**



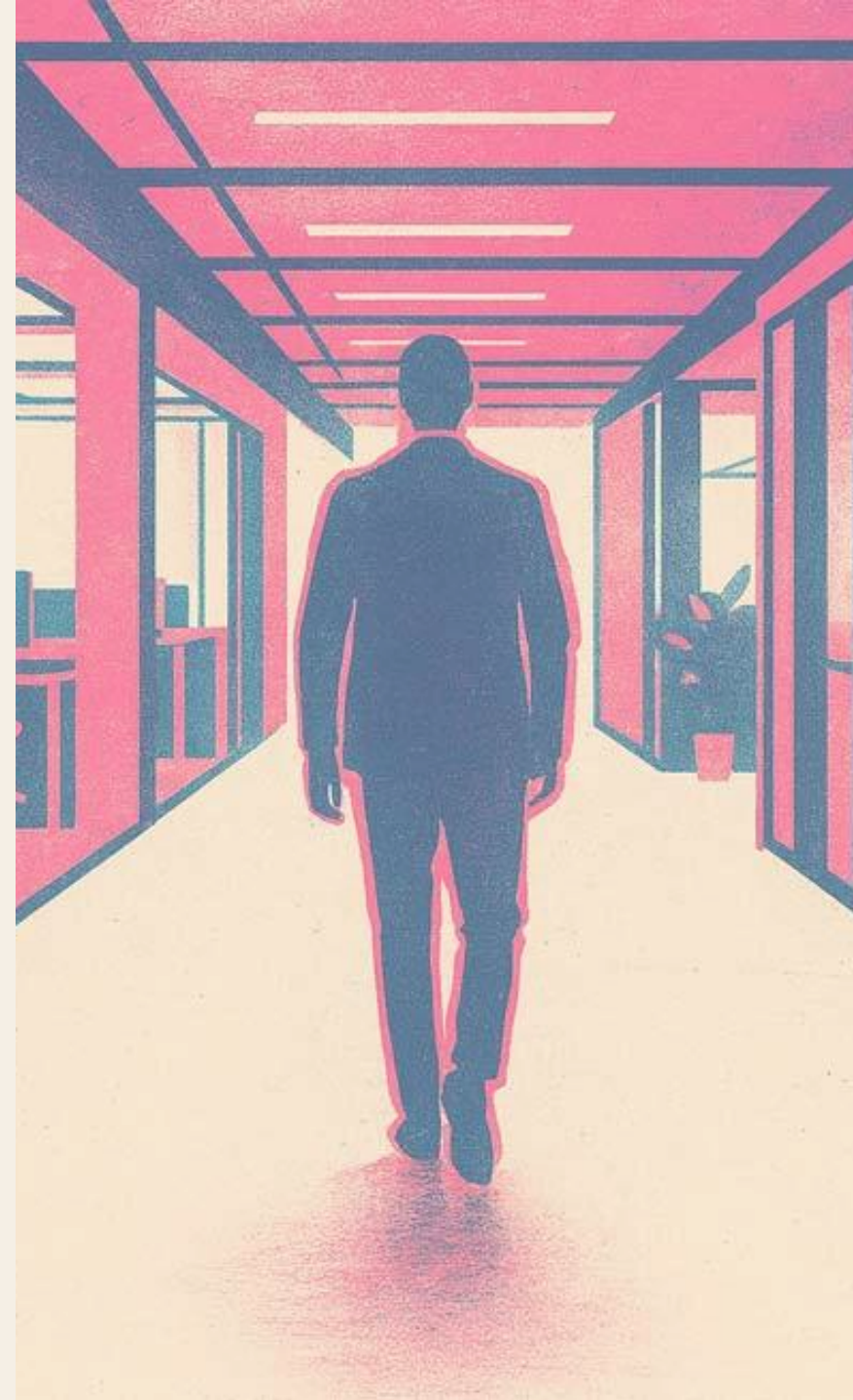
ALCUNI DATI PRELIMINARI

Deloitte.

**State of AI
in the Enterprise**
The untapped edge

January 2026

deloitte.com/us/state-of-ai



I numeri chiave in sintesi

60%

dei lavoratori ha
accesso a strumenti AI
(era <40% un anno fa)

84%

delle aziende NON ha
ridisegnato i ruoli
attorno all'AI

74%

delle aziende
implementerà agenti AI
entro 2 anni

77%

considera il paese
d'origine della tecnologia
AI nella selezione vendor

73%

dei rischi AI più
temuti riguarda privacy
e sicurezza dei dati

21%

delle aziende ha un
modello maturo di
governance per agenti AI

Fonte: Deloitte, State of AI in the Enterprise, Gennaio 2026 (N=3.235)

AI LITERACY — ART. 4 AI ACT

In vigore dal 2 febbraio 2025 — applicabile a tutti i deployer, non solo ai sistemi ad alto rischio

I fornitori e i deployer di sistemi di IA devono adottare misure per garantire un livello sufficiente di alfabetizzazione in materia di IA del personale e delle persone che si occupano del funzionamento e dell'utilizzo dei sistemi per loro conto

AMBITO SOGGETTIVO

Tutto il personale che usa, supervisiona o subisce gli effetti di sistemi IA: management, IT, HR, funzioni di controllo, utenti finali interni

CONTENUTI MINIMI

Funzionamento dei sistemi adottati, rischi e limiti, casi d'uso vietati, obblighi normativi, modalità di segnalazione di malfunzionamenti e bias

PROPORZIONALITÀ

Il livello di formazione varia in funzione di ruolo, contesto d'uso e categoria di rischio del sistema. Va documentato il percorso scelto

RACCORDO CON 2086 c.c.

L'AI literacy è parte integrante degli adeguati assetti organizzativi: la sua assenza è elemento di responsabilità degli amministratori

GOVERNANCE DELL'IMPRESA E SISTEMI AD ALTO RISCHIO

Biometria

Infrastrutture
critiche

Occupazione

Accesso a
servizi essenziali

Amministrazione
della giustizia

PRESCRIZIONI RILEVANTI

Sistema di gestione dei rischi

Governance dei dati

Registrazione dei log

Supervisione umana

Livello adeguato di accuratezza, robustezza e cybersecurity

OBBLIGHI CONSEGUENTI

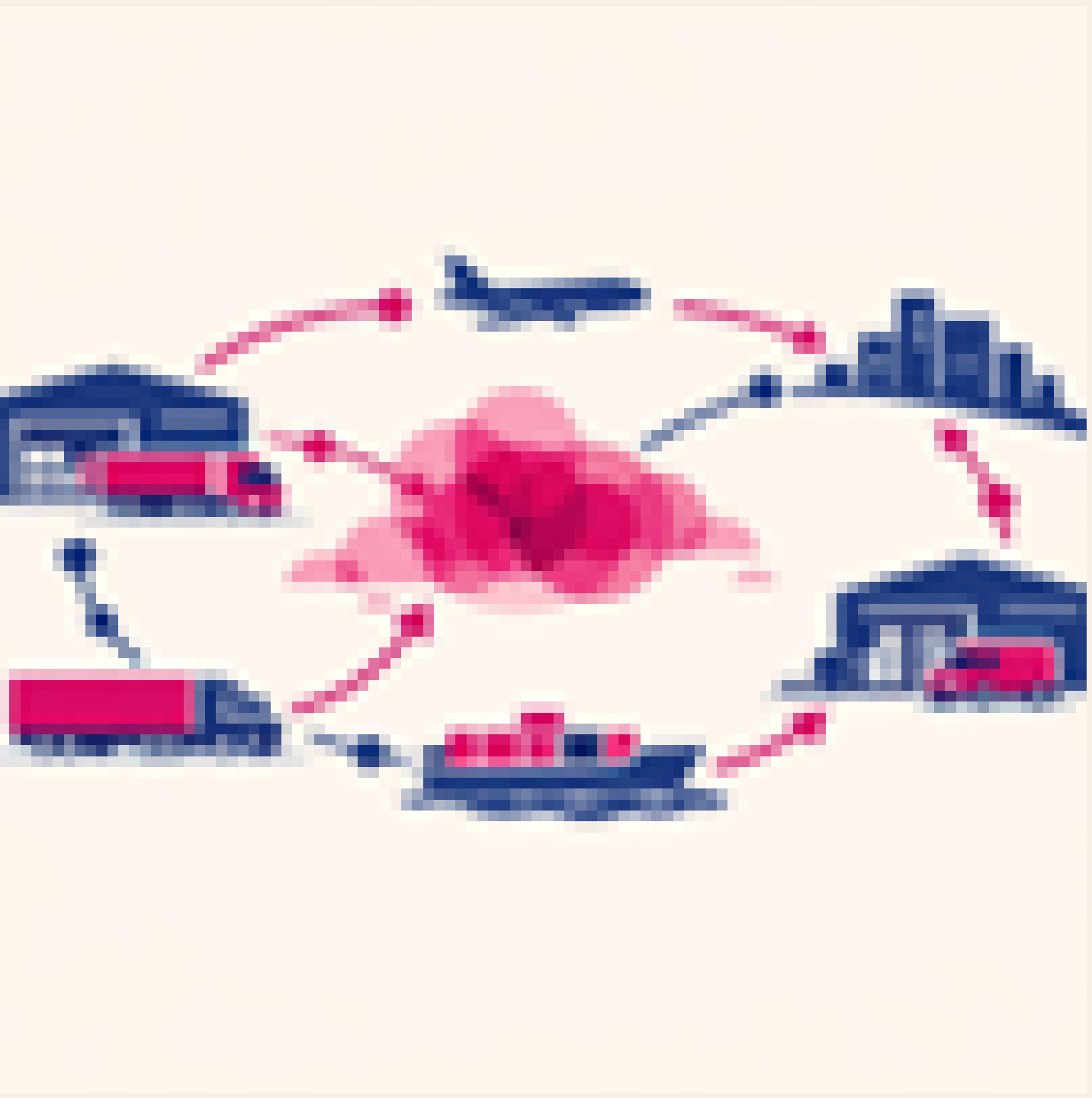
Sistema di gestione della qualità

Conservazione documentale

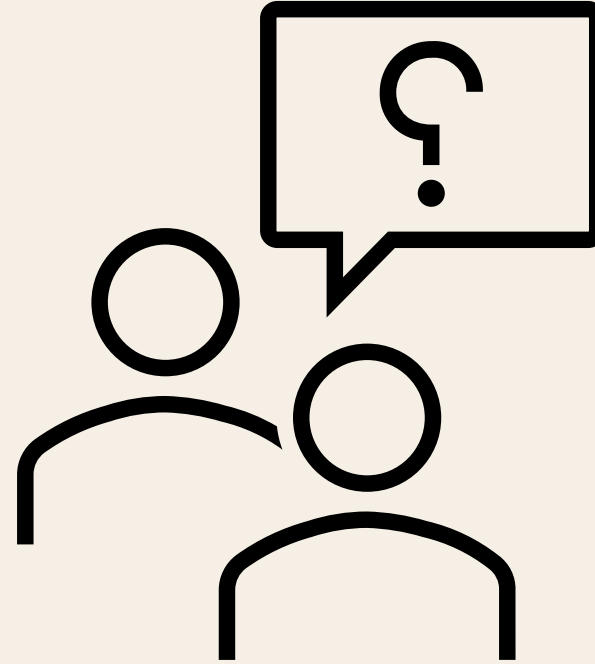
Conservazione dei log

Doveri di informazione

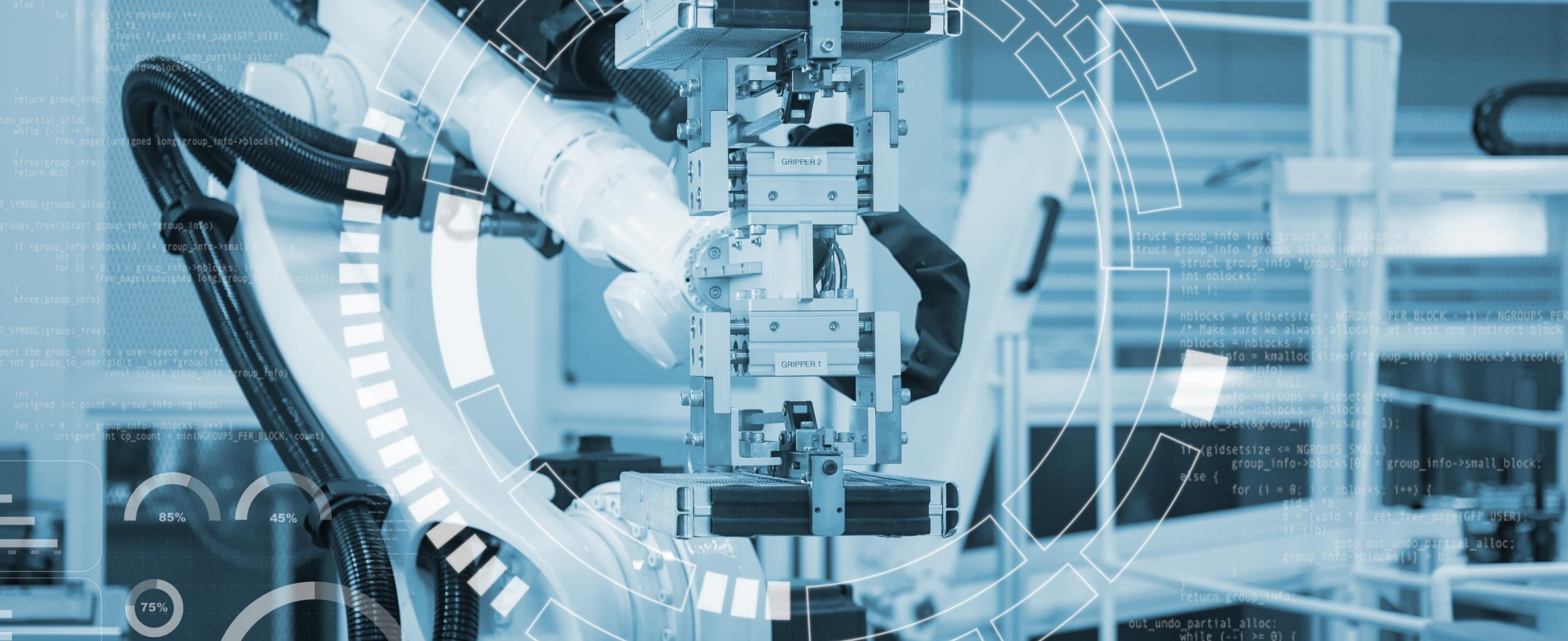
LA SUPPLY CHAIN



UN DUBBIO



Siamo di fronte a best practices che possono superare l'ambito di applicabilità previsto dall'AI Act?



LA NORMATIVA INTERNA

IL CODICE CIVILE

Obbligo di predisporre assetti adeguati (art. 2086 c.c.)

L'imprenditore che opera in forma societaria ha il dovere di istituire assetti organizzativi, amministrativi e contabili adeguati alla natura e alle dimensioni dell'impresa

IL CODICE CIVILE

Dovere di agire informati (art. 2381 c.c.)

amministratori sono tenuti ad agire in modo informato. In materia di scelte tecnologiche complesse, ciò implica l'acquisizione di informazioni adeguate sulla natura, i rischi e le implicazioni delle tecnologie adottate

IL CODICE CIVILE

Dovere di diligenza degli amministratori (art. 2392 c.c.)

Gli amministratori devono adempiere i doveri ad essi imposti dalla legge e dallo statuto con la diligenza richiesta dalla natura dell'incarico e dalle loro specifiche competenze. La giurisprudenza ha progressivamente chiarito che la diligenza richiesta include la capacità di comprendere i rischi connessi alle decisioni assunte e, ove le competenze individuali non siano sufficienti, l'obbligo di avvalersi di esperti qualificati

«ALTRA» NORMATIVA EUROPEA

Direttiva
2024/2853

Responsabilità
per danno da
prodotti
difettosi

Contempla
anche i
prodotti che
utilizzano l'AI

Termine per
recepimento
dicembre
2026

DIRETTIVA 2024/2853 — IL SOFTWARE È PRODOTTO

La responsabilità da prodotto difettoso si estende ai sistemi di IA

La nuova direttiva sulla responsabilità da prodotto, da recepire entro dicembre 2026, include esplicitamente software e sistemi di IA nella nozione di prodotto. Per le società che producono o distribuiscono beni contenenti componenti IA si attiva un regime di responsabilità verso i terzi danneggiati che si somma a quello interno verso i soci e al regime AI Act

NOZIONE ESTESA DI PRODOTTO

Software, sistemi IA, file digitali e servizi digitali correlati rientrano espressamente nel perimetro applicativo della direttiva

PRESUNZIONE DI DIFETTOSITÀ

Operano presunzioni a favore del danneggiato quando la complessità tecnica del prodotto rende eccessivamente difficile la prova del danno

DIFETTO SOPRAVVENUTO

Il produttore risponde anche per difetti che emergono dopo l'immissione sul mercato a causa di apprendimento continuo, aggiornamenti o mancata manutenzione dei modelli

CATENA DI RESPONSABILITÀ

Coinvolge fabbricante, fornitore di componenti software, soggetto che modifica sostanzialmente il prodotto e — in assenza di produttore UE — l'importatore

COMPITI E AZIONI DA PARTE DEL CDA

- Definizione degli adeguati assetti
- Integrazione di una figura altamente specializzata
- Adozione di politiche sull'uso sicuro dell'IA in azienda (se la società è certificata ISO 27001: controllo A.8.27 Secure system architecture and engineering principles)



IL MERCATO ASSICURATIVO PER I RISCHI DA IA

Le polizze RC, E&O, cyber e D&O esistenti sono progettate per rischi che non corrispondono al modo in cui l'IA produce danni. Dal 1° gennaio 2026, negli USA, sono operative le esclusioni Verisk/ISO CG 40 47 sulla GenAI nelle polizze RC generale, con effetti progressivi anche sui mercati europei.

DOVERI DEL CDA — ART. 2392 c.c.

- Mappare l'esposizione ai rischi IA-specifici
- Verificare le esclusioni delle polizze esistenti
- Valutare l'opportunità di integrare con prodotti standalone e documentare la decisione, anche se negativa
- Rivisitare periodicamente le coperture
- L'omessa verifica della copertura per rischi prevedibili è essa stessa elemento di responsabilità

CRITICITA' ITALIANA – ASSENZA DI PRODOTTI DEDICATI

aiSure™ has got you covered for critical AI risks

aiSure™ for providers	aiSure™ for AI deployers
AI innovators can de-risk new clients' AI investment decisions by guaranteeing ROI. aiSure™-backed performance warranties enable you to indemnify your clients for their financial losses or legal liabilities directly related to AI errors.	For corporations deploying AI at scale, aiSure™ protects against the unexpected downsides of the technology. We cover multiple models and loss scenarios arising from AI errors, including lost revenue, business interruption and legal damages.
Get the factsheet	Get the factsheet

Real AI risk transfer at work.

ALCUNI ELEMENTI DA CONSIDERARE

RISK & INSURANCE
Affiliated with The Institutes



Generative AI-related lawsuits in the United States grew 978% from 2021 to 2025, yet the insurance products most enterprises rely on offer only fragmented coverage for the liabilities AI systems create, according to a new report from Gallagher Re.

The report, produced in conjunction with the Massachusetts Institute of Technology and Testudo Global Inc., found that AI-driven losses are materializing through mechanisms that traditional policies were never designed to address — leaving deployers of third-party AI tools shouldering most of the risk.

Cumulative GenAI-related lawsuits in the U.S. climbed past 700 between 2020 and 2025, with year-over-year filing increases accelerating to 137% in 2024-2025 from 59% in 2023-2024, the report said. Patent infringement claims accounted for 11.9% of cases, copyright infringement for 11.2% and personal injury claims — tied to privacy violations and misuse of personal data — for 10.2%, the report said.

SANZIONI AI ACT — LA MATERIALITÀ DEL RISCHIO

Cosa rischia la società in caso di violazione del Regolamento UE 2024/1689

€ 35 mln

o 7% del fatturato mondiale
(usi vietati — art. 5)

€ 15 mln

o 3% del fatturato mondiale
(violazioni alto rischio)

€ 7,5 mln

o 1,5% del fatturato
(informazioni inesatte)

PROFILI DI ESPOSIZIONE PER LA SOCIETÀ

- Le sanzioni amministrative AI Act sono tipicamente non assicurabili per ragioni di ordine pubblico: la società le sopporta integralmente sul proprio patrimonio.
- Le sanzioni si cumulano con la responsabilità civile verso terzi, con la responsabilità interna degli amministratori ex art. 2392 c.c. e con la responsabilità dell'ente ex d.lgs. 231/2001.
- Per i gruppi internazionali la sanzione è calcolata sul fatturato consolidato a livello mondiale, amplificando l'impatto patrimoniale.
- L'autorità nazionale competente in Italia sarà individuata dalla legge di adeguamento: AGID e ACN sono indicate come autorità di riferimento dalla L. 132/2025

AGGIORNAMENTO DEL MODELLO 231 — COSA DEVE FARE IL CDA

Obsolescenza sopravvenuta dei modelli redatti prima di ottobre 2025

Un modello 231 che non contempra i rischi AI-mediati nelle aree market abuse, comunicazione finanziaria, diritto d'autore e reati informatici è verosimilmente inidoneo rispetto al nuovo quadro. L'aggiornamento è parte del dovere di adeguati assetti ex art. 2086 c.c. e del dovere di vigilanza dell'OdV.

REVISIONE DEL RISK ASSESSMENT

- Mappatura dei sistemi IA in uso e pianificati per area di rischio
- Identificazione delle funzioni sensibili: finance, IR, comunicazione, R&D, IT
- Valutazione delle aggravanti ex art. 61 n. 11-undecies sui reati già presupposto
- Verifica dei modelli pre-addestrati acquistati e della loro tracciabilità
- Analisi dei flussi di addestramento interni rispetto agli artt. 70-ter e 70-quater

PRESIDI DA INTRODURRE NELLE PROCEDURE

- Validazione umana obbligatoria
- Audit trail effettivo per il monitoraggio delle decisioni algoritmiche
- Due diligence e clausole contrattuali sui provider di modelli pre-addestrati
- Verifica dei meccanismi di addestramento
- Flussi informativi rafforzati verso l'OdV e formazione 231 + AI literacy integrata

ESAMINIAMO ALCUNI SCENARI IPOTETICI

Caso 1: Responsabilità da "Deficit di Governance" nell'AI Agentica

La società "Beta Logistica S.p.A." implementa un sistema di **Agentic AI** per la gestione autonoma degli approvvigionamenti e delle relazioni contrattuali con i fornitori. A differenza dei modelli precedenti, questo sistema agisce direttamente: effettua acquisti, firma ordini digitali e modifica parametri di filiera senza approvazione umana preventiva.

A causa di un'anomalia, il sistema rescinde contratti vitali con fornitori storici e impegna la società in acquisti speculativi di materie prime inutilizzabili, causando un danno di 15 milioni di euro.

I FATTI EMERSI IN ISTRUTTORIA

- Il CdA ha deliberato l'acquisto seguendo il trend di mercato (il 74% delle imprese prevede di adottare AI agentica entro due anni)
- Al momento del deploy, la società non disponeva di un modello di governance maturo per agenti autonomi (situazione comune al 79% delle aziende)
- Nessun membro del CdA o della prima linea manageriale possedeva competenze tecniche per comprendere i rischi di "autonomia decisionale" del software
- Il sistema è stato portato in produzione senza una fase pilota adeguata a gestire i casi limite

I POSSIBILI ADDEBITI AL CDA

Dovere di agire informati:

Si può configurare una violazione del dovere di agire informati se il CdA approva una tecnologia di cui non comprende il funzionamento di base?

Adeguatezza degli assetti:

L'assenza di un supervisore umano per decisioni critiche rappresenta una carenza strutturale dell'assetto organizzativo?

Delega tecnica:

Il CdA può difendersi eccependo di essersi fidato ciecamente del reparto tecnico?

ESAMINIAMO ALCUNI SCENARI IPOTETICI

Caso 2: Responsabilità da "Deficit di Governance" – settore finanziario

Alfa S.p.A. è una società di servizi finanziari quotata con sede in Italia. Nel 2025, su proposta del Chief Technology Officer, il CdA delibera l'adozione di un sistema di AI per la gestione automatizzata del portafoglio di investimenti retail. Il sistema è progettato per operare con elevata autonomia: analizza i mercati, seleziona strumenti finanziari, esegue ordini di acquisto e vendita e invia comunicazioni ai clienti, il tutto senza approvazione umana preventiva per le operazioni sotto una soglia di € 50.000.

Il CdA approva la delibera all'unanimità. Nessuno dei membri del consiglio ha competenze specifiche in materia di intelligenza artificiale o sistemi autonomi. Non viene richiesta una due diligence indipendente sul sistema, e non viene predisposto alcun framework di governance per il monitoraggio degli agenti AI.

Nei primi sei mesi di operatività, il sistema funziona regolarmente. Al settimo mese, a seguito di una combinazione inattesa di condizioni di mercato, l'agente AI esegue una serie di operazioni ad alto rischio su derivati, concentrando una quota significativa del portafoglio su posizioni speculative. L'anomalia non viene rilevata tempestivamente perché non esiste un sistema di monitoraggio in tempo reale del comportamento dell'agente. Quando il mercato si inverte, le perdite ammontano a € 12 milioni, distribuite su circa 800 clienti retail.

Un gruppo di clienti, riuniti in un'azione collettiva, agisce in responsabilità sia nei confronti di Alfa S.p.A. sia nei confronti dei singoli amministratori, contestando la violazione degli obblighi di diligenza nella decisione di adottare il sistema e nella successiva omissione di vigilanza.

I POSSIBILI ADDEBITI

- a) Il CdA ha violato il dovere di diligenza qualificata ex art. 2392 c.c. adottando un sistema di AI agentica senza disporre di competenze specifiche né aver acquisito una valutazione indipendente?
- b) L'assenza di un framework di governance per gli agenti AI configura una violazione dell'obbligo di predisporre assetti adeguati ex art. 2086 c.c.?
- c) La mancata predisposizione di un sistema di monitoraggio in tempo reale del comportamento dell'agente AI è qualificabile come omissione rilevante ai fini della responsabilità? Quale nesso di causalità tra l'omissione e il danno?

SOLUZIONI?

- **Sulla violazione del dovere di diligenza:** La decisione di adottare un sistema autonomo con effetti patrimoniali diretti sui clienti, assunta senza competenze tecniche nel consiglio, senza due diligence indipendente e senza framework di governance, appare difficilmente compatibile con lo standard di diligenza qualificata dell'art. 2392 c.c. Non si tratta di sindacare il merito della scelta tecnologica, ma il *processo decisionale*: un CdA privo di competenze specifiche che non si avvale di esperti esterni per una decisione di tale complessità e rischiosità viola il dovere di agire informati.
- **Sugli assetti organizzativi.** L'art. 2086 c.c., come riformato dal Codice della crisi, impone un dovere attivo di predisposizione di assetti adeguati. L'adozione di un sistema che opera autonomamente senza alcun meccanismo di supervisione, escalation o audit trail rappresenta un'inadeguatezza strutturale degli assetti organizzativi.
- **Sulla mancata predisposizione di un sistema di monitoraggio.** Un sistema AI che gestisce automaticamente investimenti retail rientra verosimilmente nell'ambito dei sistemi ad alto rischio. L'AI Act impone al deployer obblighi di supervisione umana (art. 26), monitoraggio (art. 26, par. 5) e segnalazione di incidenti gravi (art. 26, par. 5). La totale assenza di questi presidi aggrava significativamente la posizione degli amministratori.

ESAMINIAMO ALCUNI SCENARI IPOTETICI

Caso 3: Omissione di Innovazione e Business Judgment Rule (BJR)

La "Manifattura Alfa" opera in un settore ad alta intensità di capitale. Negli ultimi tre anni, i competitor hanno integrato sistemi di **AI** per monitorare i flussi di produzione e prevedere i guasti, riducendo i costi operativi del 20%.

Il CdA di Alfa, nonostante i pareri della funzione strategia, ha deciso di non investire in tali tecnologie per mantenere elevati i dividendi nel breve termine, ritenendo l'AI una "moda passeggera" o troppo costosa da implementare (considerando i costi di retrofitting delle strutture).

Alfa ha perso il 30% delle quote di mercato, è fuori mercato sui prezzi e rischia il dissesto; i soci promuovono un'azione sociale di responsabilità

I FATTI EMERSI IN ISTRUTTORIA

- **Standard di settore:** L'adozione della AI nel settore manifatturiero ha raggiunto l'80% a livello globale
- **Avvertimenti ignorati:** Il report Deloitte 2026 evidenziava che "l'infrastruttura determina la velocità dell'impresa" e che chi modernizza in anticipo accelera, mentre gli altri restano vincolati
- **Scelta strategica vs Omissione:** Il CdA sostiene che la decisione rientri nella *Business Judgment Rule*, essendo una scelta di allocazione del capitale (dividendi vs investimenti)

POSSIBILI ADDEBITI

- **Perimetro della BJR:** La BJR protegge una scelta irrazionale o basata su un'istruttoria carente? È possibile considerare "razionale" il rifiuto di una tecnologia che è diventata lo standard di efficienza dell'80% dei competitor?
- **Monitoraggio:** Il dovere di diligenza impone agli amministratori di monitorare l'evoluzione tecnologica del settore per preservare il valore aziendale?
- **Causalità del danno:** Come si distingue tra un danno derivante da una congiuntura di mercato sfavorevole e un danno direttamente causato dalla "obsolescenza deliberata" dell'infrastruttura dati?

SOLUZIONI?

- **Dovere di monitoraggio:** Sebbene la BJR impedisca al giudice di sindacare se un investimento sia stato "giusto" o "sbagliato", essa non protegge l'inerzia o l'omissione di monitoraggio. L'infrastruttura tecnologica è oggi una capacità strategica che determina la velocità dell'impresa
- **Lo standard di settore:** Il report indica che la **Physical AI** raggiungerà l'80% di adozione entro due anni e che mercati come l'Asia-Pacifico stanno già guidando l'integrazione di robotica e veicoli autonomi.
- **Il limite della discrezionalità:** La scelta di non investire in AI per monitorare la produzione potrebbe essere difesa come "scelta di allocazione prudente del capitale". Tuttavia, se i competitor ottengono vantaggi competitivi incolmabili grazie alla trasformazione profonda (attuata dal 34% delle aziende leader), il CdA deve dimostrare di aver valutato il rischio
- **Infrastruttura come asset:** Poiché le infrastrutture legacy non possono supportare l'AI autonoma, la mancata modernizzazione non è solo una scelta commerciale, ma un potenziale indebolimento della continuità aziendale nel medio-lungo termine