

SCHEDA DI APPROFONDIMENTO TECNICO-SCIENTIFICA

Intelligenza artificiale e sicurezza sul lavoro

Quattro anni di impegno AIAS hanno contribuito al nuovo assetto normativo

Roberto Sammarchi — SETTEMBRE 2026 • CIRCA 13 MIN DI LETTURA



Un percorso costruito un passo alla volta: dalla fase preparatoria del 2022 all'ammissione di AIAS all'AI Act Advisory Forum.

L'introduzione dell'intelligenza artificiale nei cicli produttivi trasforma in profondità la prevenzione aziendale. Il passaggio da modelli fondati sull'analisi retrospettiva degli eventi a sistemi capaci di anticiparli impone di ripensare le categorie giuridiche poste a presidio dell'incolumità di chi lavora.

In questa prospettiva AIAS ha sviluppato, a partire dal 2022, un'attività tecnica volta a orientare lo sviluppo tecnologico verso la tutela effettiva della persona. Il percorso si è articolato in contributi formali, audizioni e interlocuzioni con le

istituzioni nazionali ed europee, fino alla partecipazione alle consultazioni promosse dalla Commissione europea. Ha trovato riconoscimento nell'ammissione di AIAS all'AI Act Advisory Forum previsto dall'art. 67 del Regolamento (UE) 2024/1689, quale unica associazione professionale accreditata specificamente in materia di salute e sicurezza sul lavoro tra i 173 membri del Forum.

IN SINTESI

2022-2026

quattro anni di attività tecnica continuativa di AIAS su IA e prevenzione

Art. 67

Reg. (UE) 2024/1689 — base dell'ammissione all'AI Act Advisory Forum

1 su 173

unica associazione professionale accreditata su salute e sicurezza sul lavoro nel Forum



Dall'analisi retrospettiva degli infortuni alla capacità predittiva dei sistemi di IA: un cambio di paradigma per la prevenzione aziendale.

CRONOLOGIA 2023 - 2026

Le proposte di AIAS: le tappe di un percorso

2023

Le asimmetrie tra innovazione e norme vigenti

Dopo una fase preparatoria avviata nel 2022, nel 2023 AIAS ha istituito il Gruppo Tecnico Specialistico 5.0 (GTS 5.0), con il compito di esaminare le asimmetrie tra innovazione tecnologica e disciplina vigente.

Sul piano lavoristico, l'Associazione ha rilevato le incertezze applicative dell'art. 4 della Legge 300/1970. Pur riformulata dall'art. 23 del D.Lgs. 151/2015, la norma non traccia con nettezza il confine tra gli strumenti utilizzati per rendere la prestazione (comma 2) e le soluzioni algoritmiche di monitoraggio ambientale continuo dalle quali può derivare la possibilità di controllo a distanza, che restano soggette all'accordo sindacale o all'autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro (comma 1). A tale quadro si sono aggiunti gli obblighi informativi sui sistemi decisionali o di monitoraggio automatizzati introdotti dall'art. 1-bis del D.Lgs. 152/1997, inserito dal D.Lgs. 104/2022 (cosiddetto Decreto Trasparenza). Il loro ambito è stato poi circoscritto dal D.L. 48/2023, convertito dalla Legge 85/2023, ai sistemi «integralmente automatizzati».

Quanto al trattamento dei dati personali, AIAS ha chiarito che il problema non risiedeva nella mancanza di basi giuridiche. Queste sono individuabili nell'art. 6, par. 1, lett. c) e nell'art. 9, par. 2, lett. b) del GDPR, in raccordo con il D.Lgs. 81/2008 e con gli artt. 113 e 114 del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018). La vera difficoltà stava nel rispetto del principio di minimizzazione (art. 5, par. 1, lett. c) del GDPR) quando sensori fisiologici o biometrici vengono integrati nei dispositivi di protezione.

I dati raccolti restano inoltre soggetti alle garanzie dell'art. 2-septies del Codice e alla valutazione d'impatto prevista dall'art. 35 del GDPR.

L'Associazione ha perciò sollecitato un coordinamento tra Ministero del Lavoro, Ispettorato Nazionale del Lavoro e Garante per la protezione dei dati personali, così da pervenire a indirizzi applicativi uniformi. Il profilo sarebbe

poi divenuto ancora più stringente con l'AI Act: dal 2 febbraio 2025 l'art. 5, par. 1, lett. f) vieta i sistemi di IA destinati a inferire le emozioni delle persone nel luogo di lavoro, salvo che per motivi medici o di sicurezza.

2024

Le intersezioni tra AI Act e D.Lgs. 81/2008

Con l'adozione del Regolamento (UE) 2024/1689 (AI Act), AIAS ha approfondito le intersezioni con il D.Lgs. 81/2008. Nei contesti produttivi il deployer (art. 3, punto 4, del Regolamento) coincide di regola con il datore di lavoro. Su di lui grava l'obbligo, non delegabile ai sensi dell'art. 17 del D.Lgs. 81/2008, di valutare tutti i rischi, compresi quelli generati dall'impiego dei sistemi di IA.



Il datore di lavoro come *deployer*: sul piano produttivo, la valutazione dei rischi generati dai sistemi di IA resta un obbligo non delegabile.

L'Associazione ha inoltre segnalato un'anomalia nella versione italiana dell'art. 3, punto 1: la formulazione della definizione di «sistema di IA» rischiava di generare incertezze applicative rispetto alle altre versioni linguistiche dell'Unione. In collaborazione con Confcommercio Professioni, AIAS ha poi portato in sede di audizione parlamentare due priorità: la formazione continua e il ruolo dei professionisti della sicurezza operanti ai sensi della Legge 4/2013.

Il contributo alla legge quadro e il piano europeo

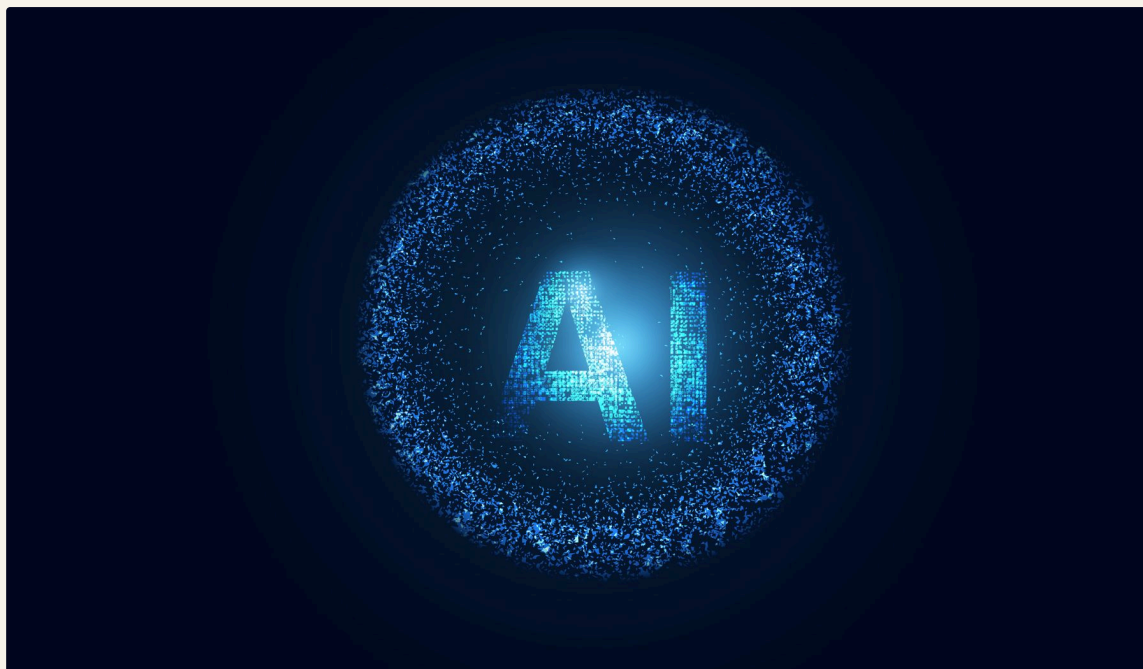
Nel 2025 l'apporto fornito in sede parlamentare insieme a Confcommercio Professioni si è mosso nella direzione poi accolta dall'art. 11 della Legge 23 settembre 2025, n. 132. La norma stabilisce che l'impiego dell'IA nel lavoro deve migliorare le condizioni di lavoro, tutelare l'integrità psicofisica dei lavoratori e accrescere la qualità delle prestazioni.

Contestualmente AIAS ha delineato un modello di revisione del Documento di Valutazione dei Rischi (DVR) fondato su due elementi. Il primo è una sorveglianza umana effettiva ai sensi dell'art. 14 dell'AI Act. Il secondo è il coinvolgimento preventivo delle rappresentanze: l'informazione dei rappresentanti dei lavoratori prima della messa in servizio di un sistema ad alto rischio, prevista dall'art. 26, par. 7, dell'AI Act, va raccordata con la consultazione del Rappresentante dei Lavoratori per la Sicurezza (RLS) ai sensi dell'art. 50 del D.Lgs. 81/2008.

Indirizzi convergenti con le proposte associative si ritrovano nel D.L. 31 ottobre 2025, n. 159, convertito con modificazioni dalla Legge 29 dicembre 2025, n. 198. Il provvedimento autorizza l'INAIL a sostenere, in particolare nelle micro, piccole e medie imprese, l'acquisto di dispositivi di protezione individuale dotati di tecnologie innovative e sistemi intelligenti. Prevede inoltre linee guida per il tracciamento e l'analisi dei mancati infortuni (near miss) nelle imprese con più di quindici dipendenti.

Sul piano europeo AIAS, tramite ENSHPO, è intervenuta con una relazione nella sessione plenaria di apertura dell'evento EU-OSHA di Bruxelles (20-21 maggio 2025). Ha poi rappresentato alla Commissione europea l'esigenza di non attrarre automaticamente nel regime dell'alto rischio i sistemi destinati alla sicurezza fisica e ambientale, quali i sensori di gas, di parametri termici e di polveri. La soluzione proposta passava per la deroga dell'art. 6, par. 3, per i sistemi dell'Allegato III e, più in generale, per una corretta delimitazione della nozione di componente di sicurezza. L'Associazione ha sollecitato al tempo stesso spazi di sperimentazione normativa (sandbox) per la gestione algoritmica del lavoro tramite piattaforma, ambito oggi oggetto anche della Direttiva (UE) 2024/2831, in corso di recepimento (AIAS ha contribuito alla consultazione parlamentare).

All'inizio del 2026 AIAS ha elaborato un position paper sulla norma ISO/IEC 42001:2023. Il documento qualifica il sistema di gestione per l'IA come modello integrabile con le norme ISO 45001:2018 e ISO 45003:2021, al fine di presidiare il tecnostress e i rischi psicosociali.



Il position paper AIAS sulla ISO/IEC 42001:2023 propone un sistema di gestione per l'IA integrabile con ISO 45001 e ISO 45003.

L'ammissione all'AI Act Advisory Forum ha consolidato questo percorso. Nel Memorandum del 16 giugno 2026, predisposto per la riunione inaugurale del Forum, AIAS ha descritto l'AI Act come connettore di sistema tra le discipline di prodotto, di prevenzione e di protezione dei dati. Ha inoltre proposto la costituzione di un gruppo di lavoro sulla sicurezza e sulla trasparenza algoritmica, secondo la linea programmatica *Safe AI – AI for Safety*.

Nel luglio 2026, infine, il protocollo d'intesa triennale sottoscritto con l'INAIL ha incluso tra gli ambiti di collaborazione lo studio delle applicazioni dell'IA per il monitoraggio delle condizioni di lavoro e l'analisi del rischio.

La coerenza del quadro normativo attuale con le proposte di AIAS

Le riforme perfezionatesi tra il 2025 e il 2026 mostrano una chiara convergenza con le linee sostenute dall'Associazione e segnano il passaggio verso una gestione integrata della tecnologia nei luoghi di lavoro.

01 Semplificazione e raccordo con la disciplina delle macchine nell'Omnibus digitale

REGOLAMENTO (UE) 2026/1744

Il Regolamento (UE) 2026/1744 dell'8 luglio 2026 (Omnibus digitale sull'IA), pubblicato nella Gazzetta ufficiale dell'Unione europea il 24 luglio e in vigore dal 27 luglio 2026, ha rimodulato il calendario applicativo dell'AI Act. Le disposizioni sui sistemi ad alto rischio (sezioni 1, 2 e 3 del capo III) si applicheranno dal 2 dicembre 2027 per i sistemi autonomi di cui all'Allegato III e dal 2 agosto 2028 per i sistemi che sono componenti di sicurezza di prodotti di cui all'Allegato I, o sono essi stessi tali prodotti. Si tratta di date fisse, non più condizionate alla disponibilità delle norme armonizzate.



L'Omnibus digitale ridefinisce il calendario applicativo dell'AI Act con date fisse, non più legate alla disponibilità delle norme armonizzate.

Quanto alle macchine, l'Omnibus ha soppresso dalla Sezione A dell'Allegato I il rinvio alla direttiva 2006/42/CE e ha inserito nella Sezione B il Regolamento (UE) 2023/1230, applicabile dal 20 gennaio 2027. I requisiti dell'AI Act non si applicheranno quindi più direttamente alle macchine, ma saranno integrati nell'Allegato III del Regolamento macchine mediante atti delegati della Commissione, che dovranno applicarsi entro il 2 agosto 2028. Resta ferma, invece, la classificazione ad alto rischio dei sistemi che ne costituiscono componenti di sicurezza, ai sensi dell'art. 6, par. 1. La scelta è coerente con l'indirizzo associativo di considerare parti meccaniche e logiche algoritmiche come un insieme unitario. Evita la duplicazione delle procedure di valutazione e riconduce la verifica di conformità al percorso già previsto per la marcatura CE, scongiurando oneri che avrebbero rallentato la diffusione di apparati salvavita.

Nella stessa direzione va la ridefinizione della nozione di «componente di sicurezza» (art. 3, punto 14, e nuovi paragrafi dell'art. 6). La nozione è ora ancorata alla funzione di sicurezza, intesa come finalità prevista determinata dal fornitore, e non comprende i sistemi utilizzati esclusivamente per finalità diverse, quali l'assistenza all'utente, l'ottimizzazione delle prestazioni o il controllo qualità. La mera integrazione dell'IA in un prodotto regolato non comporta quindi, di per sé, la classificazione ad alto rischio. I dispositivi la cui funzione è proprio quella di proteggere restano invece componenti di sicurezza: per essi la richiesta associativa trova risposta soprattutto nel raccordo procedurale con la disciplina di prodotto e nella clausola di equivalenza del nuovo art. 2, par. 13, che consentirà di limitare taluni requisiti dell'AI Act quando la normativa di settore dell'Allegato I, Sezione A, assicura un livello di protezione equivalente o superiore. La nuova definizione opera dal 27 luglio 2026, mentre i nuovi paragrafi dell'art. 6 si applicheranno secondo il calendario differito degli obblighi per l'alto rischio.

02

La centralità dell'integrità psicofisica nella Legge n. 132/2025

LEGGE 23 SETTEMBRE 2025, N. 132

L'art. 11 della Legge 132/2025, in vigore dal 10 ottobre 2025, accoglie un'impostazione coerente con quella di AIAS. L'impiego dei sistemi intelligenti deve migliorare le condizioni di lavoro e tutelare l'integrità psicofisica dei lavoratori. Il datore di lavoro è tenuto a informare il lavoratore nei casi e con le modalità dell'art. 1-bis del D.Lgs. 152/1997.

Letta in combinato disposto con l'art. 28 del D.Lgs. 81/2008, la disposizione impone di includere nella valutazione aziendale anche i rischi psicosociali, il tecnostress e il sovraccarico cognitivo derivanti dall'interazione con l'organizzazione algoritmica. L'istituzione, ai sensi dell'art. 12, dell'Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro presso il Ministero del Lavoro rafforza la consapevolezza necessaria a un governo controllato degli strumenti digitali. Nello stesso senso operano le misure di alfabetizzazione previste dalla legge.

03 Responsabilità d'impresa e presidi penali nel Decreto Legislativo n. 160/2026

D.LGS. 9 SETTEMBRE 2026, N. 160

In attuazione delle deleghe dell'art. 24 della Legge 132/2025 è stato emanato il D.Lgs. 9 settembre 2026, n. 160, pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026 e in vigore dal 30 settembre 2026. Il decreto introduce nel codice penale l'art. 437-bis, rubricato «Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi».



Reclusione da uno a cinque anni per l'omessa adozione delle misure di sicurezza o di sorveglianza umana sui sistemi di IA ad alto rischio.

La norma punisce con la reclusione da uno a cinque anni l'omessa adozione delle misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione o l'immissione sul mercato di sistemi di IA ad alto rischio, idonee a prevenirne malfunzionamenti o alterazioni. Punisce allo stesso modo l'omessa adozione delle necessarie misure di sorveglianza umana. In entrambi i casi occorre che dall'omissione derivi un pericolo per la vita o per l'incolumità pubblica o individuale; la pena è più elevata se il pericolo riguarda la sicurezza dello Stato. La norma sanziona inoltre, con pena più severa, l'alterazione dei sistemi, prevede una pena ridotta per le omissioni del primo comma commesse con colpa grave e detta una specifica disciplina per l'utilizzatore professionale che ometta intenzionalmente la sorveglianza umana.

La fattispecie ha portata generale, ma la sua rilevanza per la prevenzione negli ambienti di lavoro è immediata. Il datore di lavoro che impiega sistemi ad alto rischio in veste di utilizzatore professionale può rispondere penalmente quando omette intenzionalmente la sorveglianza umana e ne deriva un pericolo per l'incolumità dei lavoratori. Sul piano prevenzionistico resta comunque ferma la rilevanza di ogni carenza di sorveglianza ai sensi

del D.Lgs. 81/2008. Ciò vale per i sistemi dell'Allegato III destinati alla gestione del lavoro come per i componenti di sicurezza dei dispositivi di protezione e, secondo la disciplina di settore, delle macchine.

L'ipotesi di alterazione colpisce, a sua volta, la manomissione dei sistemi di IA ad alto rischio, compresi quelli con funzione di sicurezza. Si colloca così accanto all'art. 437 c.p., che da tempo sanziona la rimozione e l'omissione dolosa di cautele contro gli infortuni, e ne estende la logica alla dimensione algoritmica della prevenzione. La concreta operatività della norma andrà peraltro letta in raccordo con il calendario applicativo degli obblighi dell'AI Act, come ridefinito dal Regolamento (UE) 2026/1744.

Il decreto inserisce inoltre nel D.Lgs. 231/2001 l'art. 25-vicies, rubricato «Reati commessi con l'uso di sistemi di intelligenza artificiale». La norma annovera tra i reati presupposto della responsabilità degli enti l'art. 437-bis, con una sanzione pecuniaria da seicento a mille quote, nonché il delitto di illecita diffusione di contenuti generati o alterati con sistemi di IA (art. 612-quater c.p.), con una sanzione pecuniaria da duecento a settecento quote; per entrambi i reati si applicano le sanzioni interdittive diverse dall'interdizione all'esercizio dell'attività. I modelli di organizzazione e gestione dovranno quindi presidiare il rischio da IA in modo coordinato con quello da reati in materia di salute e sicurezza sul lavoro (art. 25-septies). A tal fine assume rilievo la modifica dell'art. 30, comma 5, del D.Lgs. 81/2008, operata dal D.L. 159/2025, convertito dalla Legge 198/2025, che ha sostituito il riferimento alla BS OHSAS 18001 con la norma UNI EN ISO 45001:2023+A1:2024. I modelli definiti in conformità a essa si presumono conformi ai requisiti dell'art. 30 per le parti corrispondenti, e ciò agevola l'integrazione con la ISO/IEC 42001.

Sul versante civilistico il decreto si muove in una direzione coerente con l'impostazione associativa, che fa leva sull'effettività delle misure più che sulla conformità formale. L'art. 19 stabilisce che la conformità di un sistema agli obblighi dell'AI Act, anche se certificata, non esclude di per sé la responsabilità del convenuto. L'art. 18 presume, salvo prova contraria, il nesso di causalità tra la violazione di tali obblighi e il danno. L'art. 17

consente al giudice di ordinare l'esibizione dei registri previsti dall'art. 12 dell'AI Act, della documentazione sulla gestione dei rischi e delle informazioni sulle modalità di sorveglianza umana.

In ambito lavorativo queste regole si saldano con l'obbligo generale di sicurezza dell'art. 2087 c.c. La prevenzione deve dunque fondarsi su una gestione sostanziale, documentata e verificabile, per la quale lo standard ISO/IEC 42001 offre un modello idoneo, e su una sorveglianza umana autentica ai sensi dell'art. 14 dell'AI Act.

04 Governance coordinata e formazione qualificata nel decreto attuativo sulle Autorità nazionali

ATTO DEL GOVERNO N. 421

Il secondo decreto legislativo attuativo dell'art. 24 della Legge 132/2025, relativo ai poteri delle Autorità nazionali e all'utilizzo dell'intelligenza artificiale nella formazione (Atto del Governo n. 421), è stato approvato in via definitiva dal Consiglio dei Ministri il 4 agosto 2026 ed è, al momento in cui scriviamo, in attesa di pubblicazione; il termine della delega scade il 10 ottobre 2026. Il testo traduce in norme due costanti priorità associative. AIAS ha partecipato alla consultazione parlamentare tramite Confcommercio Professioni.

Sul piano della governance, il testo definisce i ruoli e i canali di raccordo tra AgID (autorità di notifica), ACN (autorità di vigilanza del mercato e punto di contatto unico), Banca d'Italia, CONSOB e IVASS per il settore finanziario e Garante per la protezione dei dati personali. Restano ferme le competenze delle autorità di settore per i prodotti dell'Allegato I. Il testo risponde così all'esigenza, più volte rappresentata da AIAS, di evitare duplicazioni e attriti tra sicurezza informatica, protezione dei dati e prevenzione infortunistica.

Di particolare rilievo per il lavoro è la previsione secondo cui le decisioni relative alla costituzione, alla modifica e alla cessazione del rapporto non possono fondarsi esclusivamente su un trattamento automatizzato. Il divieto

si estende ai provvedimenti disciplinari e il licenziamento adottato in violazione è nullo. Il testo precisa peraltro che non rientrano tra le decisioni finali relative alla costituzione del rapporto le attività di ricerca e selezione delle candidature, anche quando comportino la mancata ammissione alle fasi successive.



La sorveglianza umana resta il perno del sistema: prevenire la «distorsione dell'automazione» richiede formazione continua, non solo regole.

Sotto il profilo formativo, le disposizioni mirano a qualificare le competenze degli operatori lungo l'intero arco professionale, in coerenza con il sistema della Legge 4/2013. Il Regolamento (UE) 2026/1744 ha configurato l'obbligo di alfabetizzazione dell'art. 4 dell'AI Act come obbligo di mezzi.

L'attenuazione non riguarda però chi esercita la sorveglianza umana sui sistemi ad alto rischio: l'art. 26, par. 2, dell'AI Act impone al deployer di affidarla a persone fisiche dotate della competenza, della formazione e dell'autorità necessarie. L'addestramento continuo di queste persone diventa così la condizione concreta dell'effettività della sorveglianza. Occorre prevenire la dipendenza passiva dall'output e l'eccessivo affidamento sul sistema, cioè quella «distorsione dell'automazione» (automation bias) di cui, ai sensi dell'art. 14, par. 4, lett. b) dell'AI Act, le persone preposte alla sorveglianza devono poter restare consapevoli.

«L'intelligenza artificiale acquista piena legittimità nel lavoro quando è diretta a liberare la persona dal pericolo fisico e cognitivo e preserva il controllo umano al vertice dei processi decisionali.»

DALLE CONSIDERAZIONI CONCLUSIVE

SINTESI

Considerazioni conclusive

L'evoluzione dell'ordinamento conferma la linea sostenuta da AIAS: l'intelligenza artificiale acquista piena legittimità nel lavoro quando è diretta a liberare la persona dal pericolo fisico e cognitivo e preserva il controllo umano al vertice dei processi decisionali.

Il quadro che ne emerge è coerente. Le regole di prodotto semplificate dall'Omnibus, i principi della Legge 132/2025, i presidi penali e risarcitori del D.Lgs. 160/2026 e la governance delineata dal decreto sulle Autorità nazionali chiedono alle imprese non la mera conformità formale, ma l'effettività delle misure.

La partecipazione dell'Associazione all'AI Act Advisory Forum offrirà un presidio qualificato affinché l'attuazione degli spazi di sperimentazione normativa previsti dall'art. 57, che gli Stati membri dovranno istituire entro il 2 agosto 2027, e le future linee guida europee consolidino questi principi in tutele stabili negli ambienti di lavoro.

Riferimenti normativi essenziali

Regolamento (UE) 2024/1689

AI Act — disciplina generale sui sistemi di intelligenza artificiale

Regolamento (UE) 2026/1744

Omnibus digitale sull'IA — rimodula il calendario applicativo dell'AI Act

D.Lgs. 81/2008 Testo Unico in materia di salute e sicurezza sul lavoro	Legge 23 settembre 2025, n. 132 Legge quadro sull'intelligenza artificiale
D.Lgs. 9 settembre 2026, n. 160 Presidi penali, responsabilità degli enti e regole civilistiche sull'IA	D.Lgs. 231/2001 Responsabilità amministrativa degli enti — nuovo art. 25-vicies
Regolamento (UE) 2016/679 (GDPR) Protezione dei dati personali, inclusi i dati biometrici e fisiologici	D.Lgs. 196/2003 Codice in materia di protezione dei dati personali
D.L. 159/2025, conv. Legge 198/2025 Sostegno INAIL a DPI intelligenti e tracciamento dei near miss	Direttiva (UE) 2024/2831 Lavoro tramite piattaforme digitali, in corso di recepimento
ISO/IEC 42001:2023 Sistema di gestione per l'intelligenza artificiale	Atto del Governo n. 421 Decreto attuativo su Autorità nazionali e formazione IA

Autore: Roberto Sammarchi

Scheda di approfondimento tecnico-scientifica pubblicata a cura di AIAS. I contenuti hanno finalità informativa e non costituiscono consulenza legale.

