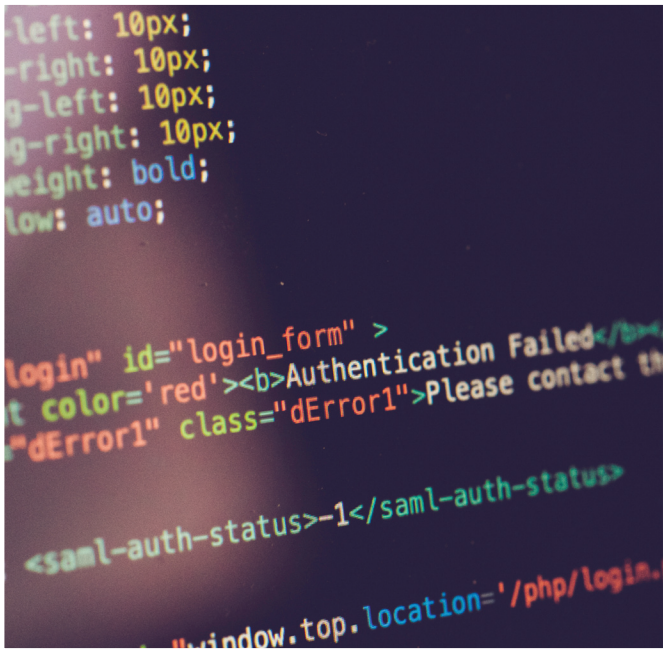
Roberto Sammarchi
Avvocato specialista in diritto dell'informazione, della comunicazione digitale e della protezione dei dati personali, Socio AIAS

L'intelligenza artificiale entra nei luoghi di lavoro: le sfide per la sicurezza integrata

Il presente articolo completa il percorso di approfondimento su IA e sicurezza sul lavoro a cura dell'Avv. Roberto Sammarchi, avviato su aiasmag nel quadro dell'impegno di AIAS, in Italia e nelle sedi europee tramite ENSHPO, per una regolazione che favorisca l'adozione della tecnologia a fini prevenzionali. Come documentato nello Speciale pubblicato sul n. 38, l'Associazione ha portato all'attenzione del legislatore, tramite Confcommercio Professioni e con il supporto della Senatrice Paola Mancini, le criticità interpretative della nuova normativa, incluso il disallineamento nelle traduzioni dell'AI Act nelle diverse lingue europee.



Il 2026 segna una nuova tappa per la prevenzione e la sicurezza sul lavoro in Italia. Con l'approvazione definitiva della Legge 23 settembre 2025, n. 132 e del D.L. 31 ottobre 2025, n. 159 (convertito a fine anno nella Legge n. 198/2025), il legislatore ha consegnato a imprese e professionisti un quadro normativo che fa dell'IA un asse centrale delle nuove strategie di tutela della salute e sicurezza.

Per i professionisti del settore HSE, comprendere queste norme è ormai una necessità operativa.

1 Un quadro normativo completo e graduale

Il primo punto da chiarire è che non ci muoviamo più in una zona grigia. Il quadro normativo italiano ed europeo è oggi sostanzialmente completo. La Legge 132/2025 opera come raccordo nazionale con il Regolamento (UE) 2024/1689 (AI Act), ne anticipa alcuni effetti e ne specifica l'applicazione nel nostro ordinamento. Non si tratta di un "big bang" normativo che stravolge tutto da un giorno all'altro, ma di un processo graduale di attuazione che permette alle aziende di adeguarsi. La legge italiana definisce i principi cardine (antropocentrismo, trasparenza, sicurezza), individua le autorità di controllo e stabilisce le sanzioni, ma lascia spazio a decreti attuativi e norme tecniche per i dettagli operativi. Questa struttura offre almeno un primo nucleo di certezza del diritto: benché non manchino in termini pratici problemi (notevoli) di attuazione delle norme, sappiamo almeno con grande dettaglio quali sono i requisiti fondamentali che un sistema di IA deve rispettare per entrare in azienda, soprattutto in un'area critica come la gestione del lavoro e la sua sicurezza. Viene anche dettagliata la "conformità" dell'IA come processo continuo di analisi, valutazione e gestione del rischio.

2 Sicurezza 4.0: DPI intelligenti e ruolo dell'INAIL

La novità più tangibile per chi opera sul campo arriva probabilmente dall'Articolo 5 del D.L. 159/2025. La norma attribuisce all'INAIL un mandato forte per promuovere e incentivare l'adozione di "DPI intelligenti" (smart PPE). Se attuata progressivamente a livello generale, si tratta di una rivoluzione copernicana: il dispositivo di protezione cessa di essere uno scudo passivo (come il classico elmetto o la scarpa antinfortunistica) e diventa un nodo attivo di una rete IoT (Internet of Things). Caschi che rilevano urti e malori, gilet che segnalano la presenza di gas o la vicinanza pericolosa a un muletto, scarpe che allertano in caso di "uomo a terra". L'introduzione di questi strumenti porta ovviamente con sé nuove complessità. Per funzionare, i DPI intelligenti devono essere interconnessi, trasmettere dati in tempo reale e spesso geolocalizzare il lavoratore. Si aprono quindi due fronti critici: la cybersicurezza e la privacy. Un DPI connesso è un potenziale punto di ingresso per attacchi informatici che potrebbero paralizzare l'azienda o, peggio, manipolare i dati di sicurezza. Inoltre, la raccolta massiva di dati sui movimenti del lavoratore rischia di violare l'Articolo 4 dello Statuto dei Lavoratori se non rigo-

rosamente perimetrata alle sole finalità di sicurezza. La sfida per i Responsabili del Servizio di Prevenzione e Protezione e per tutti i ruoli tecnici e organizzativi del sistema prevenzionale sarà gestire questa integrazione, collaborando con i responsabili IT e Privacy per garantire che la tecnologia protegga la vita senza comprimere i diritti. Se il sistema che interconnette e gestisce i DPI intelligenti utilizza l'IA, si apre un altro scenario: si tratta di un sistema di IA che le norme europee e nazionali qualificano come "ad alto rischio", con rilevanti problemi di compliance e oneri a carico dei datori di lavoro in gran parte ancora inesplorati. Essenziale, per potere sperimentare le nuove tecnologie e la loro compliance, è l'attivazione delle *sandbox* previste dall'AI Act. Si tratta di spazi tecnologici protetti e incentivati nei quali i nuovi sistemi possono essere sviluppati in vista della certificazione e al riparo da sanzioni, creando un motore dell'innovazione nel settore IA e un passaggio fondamentale a sostegno della sovranità tecnologica europea.

3 La nuova frontiera: salute mentale, benessere, gestione algoritmica

Se sui rischi fisici la tecnologia offre soluzioni, sui rischi per la salute psicologica può crearne di nuovi. L'Articolo 10 della Legge 132/2025 è esplicito: l'IA deve migliorare le condizioni di lavoro, non peggiorarle. Eppure, l'introduzione di algoritmi per l'organizzazione e la gestione delle attività (c.d. *Algorithmic Management*) nasconde insidie. Un algoritmo che pianifica turni, percorsi logistici o carichi di lavoro puntando alla massima efficienza teorica può generare ritmi insostenibili, portando a stress lavoro-correlato, ansia da prestazione e burnout.
La Valutazione dei Rischi deve evolvere.
Ormai è un obbligo normato anche valutare l'impatto dell'algoritmo sulla psiche del lavoratore. La mancanza di autonomia, la sensazione di essere controllati da una "scatola nera" e l'impossibilità di prevedere i carichi di lavoro nel confronto con interlocutori umani sono fattori di rischio psicosociale che devono essere mitigati, garantendo sempre la supervisione umana e la possibilità di "staccare" (diritto alla disconnessione).
L'intelligenza artificiale deve essere un supporto, non un caporale digitale.

4 Competenze manageriali: governare la transizione

La tecnologia, da sola, non genera sicurezza; è il modo in cui viene gestita a fare la differenza. Si pone dunque un problema urgente di competenze. Il management aziendale e i professionisti della sicurezza devono sviluppare nuove capacità per accompagnare questa transizione. Non servono solo competenze tecniche, ma manageriali ed etiche.
La finalità è duplice. Da un lato, assicurare la tutela e il benessere delle persone e dei loro diritti: il manager deve saper spiegare al lavoratore come funziona l'algoritmo, deve saper intervenire se l'IA prende decisioni ingiuste o pericolose e deve garantire che la dignità umana prevalga sempre sul processo computazionale. Dall'altro, nel rispetto del quadro normativo, assicurare che l'IA sia una leva per migliorare la sicurezza. Saper leggere i dati predittivi forniti dai sistemi intelligenti permette di passare da una prevenzione reattiva (analisi degli infortuni accaduti) a una proattiva (analisi dei *near-miss* e dei trend di rischio), prevenendo l'incidente prima che accada.
In questo scenario di profonda trasformazione, AIAS - Associazione Italiana Ambiente e Sicurezza conferma il suo impegno centrale. L'Associazione sta lavorando per sviluppare ed estendere alleanze strategiche su questi temi con tutti i soggetti istituzionali (Ministeri, INAIL, Autorità garanti e di controllo), con le imprese e le loro organizzazioni, le organizzazioni dei lavoratori, università ed enti di ricerca. L'obiettivo è fornire ai propri iscritti e al sistema Paese gli strumenti culturali e operativi per vincere questa sfida, facendo dell'Italia un laboratorio d'eccellenza per un'Intelligenza Artificiale sicura, etica e produttiva.

Sintesi degli Adempimenti nel nuovo quadro normativo 2026 per la "Sicurezza Tecnologica"

Area di intervento	Azione richiesta
Recruiting & HR	Verifica assenza bias discriminatori negli algoritmi di selezione.
Trasparenza	Informativa ai lavoratori sull'uso di sistemi decisionali automatizzati.
Sicurezza fisica	Adozione DPI intelligenti (facoltativa ma incentivata) e aggiornamento DVR.
Salute mentale	Valutazione rischio stress da gestione algoritmica e carichi di lavoro.
Supervisione	Nomina supervisori umani per sistemi IA ad alto rischio e definizione procedure di "stop" efficaci.
Cybersicurezza	Verifica requisiti di sicurezza dei sistemi IA e dispositivi connessi.