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

IA e sicurezza sul lavoro: la rivoluzione strategica dei professionisti SSL

L'uso dell'intelligenza artificiale nei luoghi di lavoro è una realtà operativa che sta ridisegnando processi, gerarchie e profili di rischio. In questo contesto, l'entrata in vigore della legge italiana sull'IA (L. 132/2025), in stretto rapporto con il Regolamento UE (AI Act, Reg. 2024/1689), segna un punto di svolta irreversibile, in particolare per i professionisti della Sicurezza e Salute nei Luoghi di Lavoro (SSL).

Il nuovo quadro giuridico impone un radicale cambio di paradigma: si transita da una gestione della sicurezza basata sulla conformità normativa a un'analisi strategica attiva, che deve governare nuovi rischi e cogliere opportunità inedite. Per figure chiave come il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e i consulenti specializzati, ciò significa una profonda ridefinizione del proprio ruolo.
Non più solo controllori a valle, ma governatori a monte dell'innovazione, chiamati ad acquisire nuove competenze per integrare la prevenzione nelle strategie di sviluppo tecnologico delle imprese.

IL NUOVO PERIMETRO GIURIDICO: DAL D.LGS. 81/08 ALL'AI ACT

Il fulcro della nuova disciplina si trova nell'articolo 11 della L. 132/2025. La norma stabilisce un nuovo principio fondamentale: l'IA è impiegata per "migliorare le condizioni di lavoro" e "tutelare l'integrità psicofisica" dei lavoratori. La previsione crea un collegamento giuridico diretto con gli obiettivi di salute e sicurezza già sanciti dal D.Lgs. 81/2008. L'innovazione tecnologica non è vista come un'area separata, ma come uno strumento orientato alla tutela delle persone.

L'AI Act europeo classifica inoltre come sistemi ad "alto rischio" (High-Risk AI Systems) la maggior parte delle applicazioni in ambito lavorativo. Rientrano in questa categoria i sistemi per l'assunzione, la selezione, le decisioni su promozioni o cessazione del

rapporto, l'assegnazione di compiti e, con impatto notevole sulla sicurezza, i sistemi destinati al monitoraggio o alla valutazione delle prestazioni e del comportamento dei lavoratori.

La classificazione impone al datore di lavoro, in qualità di *deployer* (utilizzatore), obblighi specifici. Tra questi, la garanzia di un'adeguata "sorveglianza umana" (art. 14 AI Act) e l'obbligo di utilizzare i sistemi conformemente alle istruzioni d'uso (art. 26 AI Act). È qui che il ruolo del professionista SSL si espande: da "valutatore" a "garante" della corretta implementazione e gestione dei nuovi obblighi tecnologici.

L'EVOLUZIONE DEL RISCHIO

Il D.Lgs. 81/2008 impone la valutazione di "tutti i rischi".
L'integrazione dell'IA nei processi aziendali introduce nuove tipologie di rischio, spesso immateriali ma non per questo meno impattanti, che i professionisti SSL devono ora mappare e gestire.

Il Documento di Valutazione dei Rischi (DVR) deve ora obbligatoriamente evolversi per includere una sezione dedicata al "rischio algoritmico".

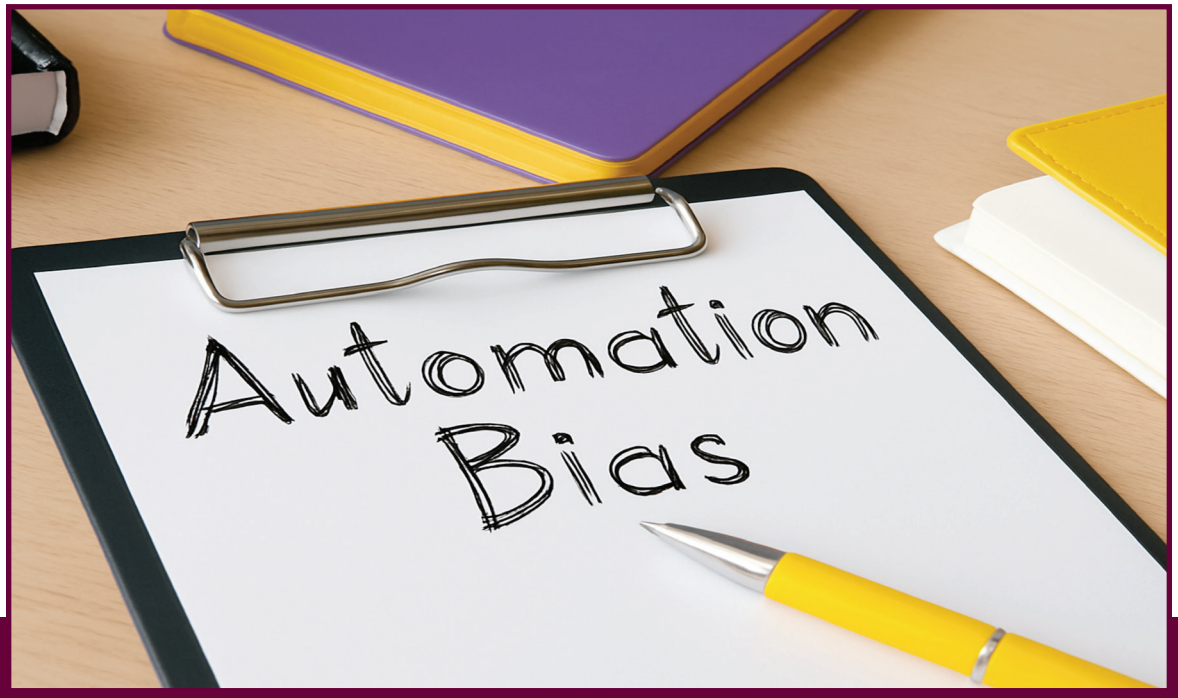
La nuova valutazione si articola su tre fronti principali.

1. Rischi Psico-sociali

Sistemi di monitoraggio costante o di valutazione delle prestazioni possono generare stress lavoro-correlato.
Se l'algoritmo è percepito come opaco (scarsa "spiegabilità"), invasivo o ingiusto (per via di bias), l'impatto sul benessere mentale del lavoratore è diretto.

2. Rischio Discriminatorio (Bias)

L'IA impara dai dati.
Se usata per assegnare compiti o valutare performance, e viene addestrata su dati storici vi-



ziati, l'IA non solo replicherà, ma amplificherà le discriminazioni passate.
Questo, come specificato dall'art. 11 della legge italiana, impatta direttamente l'integrità psicofisica e il benessere organizzativo.

3. Rischio Cognitivo (Automation Bias)

L'AI Act avverte del rischio da "eccessivo affidamento".
Si tratta della tendenza umana a fidarsi acriticamente dell'output della macchina, riducendo la propria vigilanza critica così da individuare eventuali errori.
Questo bias cognitivo può portare l'operatore a ignorare segnali di pericolo reali o a seguire indicazioni errate dell'algoritmo, con conseguenze potenzialmente gravi.

La mappatura di questi rischi richiede una collaborazione rinnovata e più stretta tra RSPP, Medico Competente, Risorse Umane e Rappresentanti dei Lavoratori (RLS).

IL PROFESSIONISTA SSL COME "GOVERNATORE" DELLA TECNOLOGIA

Di fronte a questi scenari, il ruolo del professionista SSL evolve in una figura strategica. La normativa non sminuisce la competenza umana, al contrario la rende indispensabile per governare la tecnologia.

La "sorveglianza umana", imposta sia dalla legge italiana (principio antropocentrico) sia dall'AI Act, non è una passiva supervisione.

L'articolo 14 dell'AI Act è chiaro: il sistema deve essere progettato per consentire all'operatore umano di "ignorare, annullare o ribaltare" l'output dell'al-

goritmo. Inoltre, l'articolo 26 impone che questa sorveglianza sia affidata a persone con "competenza, formazione e autorità" necessarie.

Il professionista SSL diventa la figura determinante per *disegnare* questo processo.
Il suo compito non si limita a definire le procedure di sorveglianza, ma si estende alla progettazione della formazione specifica (richiesta anche dall'art. 12 della legge italiana) e alla validazione, a monte, della scelta di sistemi che siano "sicuri, affidabili e trasparenti".

Anche la formazione (ex art. 37 D.Lgs. 81/08) deve evolvere.
Non basta un addestramento generico; dovrà essere specifica per i sistemi in uso.
I supervisori designati devono comprendere i limiti prestazionali del sistema, le procedure di sorveglianza e, soprattutto, come e quando esercitare il potere/dovere di "ignorare, annullare o ribaltare" la decisione dell'IA.

NUOVE OPPORTUNITÀ: L'IA COMPLIANT COME STRUMENTO DI PREVENZIONE

L'IA offre ai professionisti SSL strumenti di prevenzione potentissimi.
L'IA conforme alla legge può essere impiegata per analisi predittive, elaborando modelli per prevedere guasti di macchinari (manutenzione predittiva) o situazioni di pericolo prima che si manifestino, intervenendo così sulla probabilità di accadimento.

Sistemi di visione artificiale possono analizzare in tempo reale posture e movimenti ripetitivi per prevenire disturbi muscolo-scheletrici, in modo non invasivo e oggettivo. Inoltre, l'IA permette di analizzare enormi volumi di dati sui *near miss* (mancati infortuni), identificando pattern di rischio nascosti e correlazioni complesse che l'analisi umana tradizionale faticherebbe a cogliere, migliorando esponenzialmente l'efficacia delle misure di prevenzione.

Il problema principale non è oggi la tecnologia disponibile, ma – per quanto ciò possa apparire un paradosso – il suo utilizzo conforme alle norme; esattamente il ruolo in cui gli esperti di compliance SSL possono esprimere un contributo determinante.

Le nuove norme impongono un approccio sistemico.
Un aspetto cruciale è il rafforzamento del ruolo del Rappresentante dei Lavoratori per la Sicurezza (RLS).
L'articolo 26 dell'AI Act impone al datore di lavoro di informare i rappresentanti prima di mettere in servizio un sistema AI ad alto rischio.
Non si tratta di una informativa a valle, ma di un coinvolgimento preventivo che si salda con l'articolo 50 del D.Lgs. 81/08, implicando la consultazione sulla valutazione dei nuovi rischi e sulle relative misure di prevenzione.

L'intelligenza artificiale non è solo un nuovo rischio da normare.

È un'opportunità per rendere la gestione della sicurezza più efficace, predittiva e basata sui dati.

Per i professionisti SSL, la nuova opportunità è trasformarsi da gestori della conformità a architetti della governance tecnologica, garantendo che l'innovazione rimanga sempre al servizio della persona e della sua integrità psicofisica.