Roberto Sammarchi
Avvocato specialista in diritto dell'informazione, della comunicazione digitale e della protezione dei dati personali, componente della Rete Giuridica AIAS, Coordinatore GTS Mare e GTS Gestione dei cambiamenti e dell'innovazione di AIAS, Socio AIAS

Intelligenza artificiale e sicurezza sul lavoro: un equilibrio tra innovazione e regole

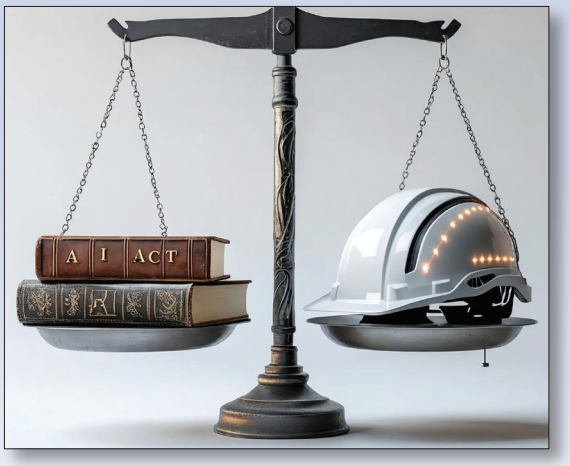
L'intelligenza artificiale (IA) ha il potenziale per trasformare la sicurezza e la salute nei luoghi di lavoro (SSL), spostando l'approccio da reattivo a predittivo. Il suo potenziale si confronta tuttavia con il nuovo regolamento europeo sull'IA, che a causa dei pesi burocratici rischia di ostacolare l'adozione di tecnologie salvavita. L'analisi di questo complesso rapporto è al centro di un contributo di Roberto Sammarchi, rappresentante di AIAS in ENSHPO, presentato il 20.5.2025 a Bruxelles nel corso del Good Practice Exchange organizzato da EU-OSHA (European Agency for Safety and Health at Work).

Di seguito una sintesi dell'intervento; il testo completo inglese e la relativa scheda sono presenti fra i documenti della Rete Giuridica[1].

Il regolamento (UE) 2024/1689[2], noto come AI Act, è la prima norma organica al mondo sull'intelligenza artificiale. Adotta un approccio basato sul rischio, classificando i sistemi di IA in diverse categorie. Molte applicazioni pensate per la SSL ricadono in base al regolamento nella categoria ad "alto rischio". La classificazione presuntiva scatta, ad esempio, quando un sistema di IA è destinato a essere impiegato per la gestione dei lavoratori, per l'assegnazione di compiti o per il monitoraggio delle loro prestazioni e comportamenti, tutte aree operative e funzioni che possono rientrare nella dimensione propria della SSL. La qualifica di "alto rischio" impone ai produttori e agli utilizzatori obblighi estremamente gravosi: sistemi di gestione del rischio, stringenti requisiti di governance dei dati, documentazione tecnica, sorveglianza umana effettiva, notifiche alle autorità di controllo e procedure di valutazione della conformità.

L'imposizione di oneri così complessi, costosi e con elevato rischio giuridico a causa di sanzioni che appaiono sproporzionate soprattutto per le piccole e medie imprese può generare un paradosso. Strumenti progettati specificamente per ridurre i rischi sul lavoro vengono sottoposti a un regime normativo che ne rende complessa e costosa l'adozione. Il risultato potrebbe essere un "effetto congelante" sull'innovazione, scoraggiando lo sviluppo di soluzioni capaci di salvare vite umane a causa di barriere normative il cui scopo è del tutto diverso: evitare che la nuova tecnologia intelligente consenta in modo subdolo e difficilmente tracciabile violazioni dei diritti umani. Il regolamento, infatti, inquadra l'IA solo come un rischio da gestire, non rilevandone le potenzialità come strumento in grado in alcune circostanze di eliminare o ridurre rischi negli ambienti di lavoro.

La portata della norma dipende da definizioni tecniche precise che ne fissano l'ambito oggettivo. L'articolo 3(1) dell'AI Act definisce "sistema di IA" una macchina che, tra le altre cose, "inferisce" (*infers*) come generare



un output. L'analisi linguistica delle diverse versioni ufficiali del testo rivela delle sfumature molto diverse. Se la versione inglese usa "inferiree" (*to infer*), quelle italiana e francese usano "dedurre" (*deduce* / *déduit*), mentre quella tedesca "derivare" (*ableitet*).

Una lettura tassativa, legata al concetto logico di deduzione, potrebbe nel contesto italiano escludere molti sistemi moderni di *machine learning*, che operano su base probabilistica e inferenziale piuttosto che deduttiva. L'inferenza è un metodo logico di tipo bottom-up, che parte da indizi o elementi per generare una soluzione probabile; la deduzione è un metodo top-down che applica regole logiche di portata generale e genera risultati certi.

Se l'IA viene definita come "deduttiva" si ottiene l'effetto paradossale di vedere potenzialmente assoggettati al regolamento vecchi sistemi basati sull'applicazione deterministica di regole logiche, che con l'intelligenza artificiale moderna nulla hanno a che vedere. Portando il ragionamento all'estremo, il testo italiano potrebbe attirare nell'ambito oggettivo del regolamento una calcolatrice (che si basa sulla deduzione, cioè sull'applicazione deterministica di regole logiche e può "adattare" il risultato eseguendo ad esempio un arrotondamento in base al numero consentito di decimali). Una lettura nominalistica potrebbe addirittura portare a escludere un moderno modello generativo, che non deduce affatto l'output ma lo inferisce in modo indeterministico. Tale incertezza giuridica potrebbe portare a un'applicazione disomogenea del regolamento nei diversi Stati membri, considerando che in alcuni territori dell'Unione Europea l'inglese è ancora lingua ufficiale.

Proseguendo il nostro percorso e con riguardo alle applicazioni dell'IA alla SSL, se un sistema rientra nell'ambito oggettivo del regolamento esistono alcune possibilità interpretative per evitare la classificazione ad alto rischio e i rilevantissimi oneri connessi. L'articolo 6(3) dell'AI Act infatti prevede una deroga per i sistemi elencati nell'Allegato III, a condizione che il fornitore dimostri che il sistema non pone un "rischio significativo di danni" e non "influenza materialmente l'esito del processo decisionale". La deroga si applica se il sistema svolge compiti specifici, come l'esecuzione di una stretta attività procedurale, il miglioramento di un'attività umana già completata o un'attività preparatoria a una valutazione successiva.

Sulla base di questa deroga, potrebbero essere considerati non ad alto rischio alcuni sistemi di IA per la SSL. Tra questi, i sistemi per la formazione, purché non valutino le persone con conseguenze su assunzione o carriera, e i sistemi informativi di supporto alla decisione umana. In quest'ultimo caso, è fondamentale che il decisore umano mantenga una reale autonomia e capacità critica, evitando la fallacia dell'*human-in-the-loop*, che si determina quando la presenza umana è solo formale. Anche i sistemi concepiti per la pura riduzione del rischio, come un arresto di emergenza intelligente, potrebbero in teoria rientrare in questa categoria, sebbene la loro natura di "componente di sicurezza" di una macchina possa farli ricadere nell'ambito dell'alto rischio per altra via.

Per realizzare il potenziale dell'IA nella SSL è necessario un approccio normativo equilibrato che promuova l'innovazione responsabile. La strada da percorrere richiede un dialogo costante tra professionisti, sviluppatori, datori di lavoro, lavoratori e regolatori. Di particolare importanza è la partecipazione ai momenti di dialogo e alle consultazioni pubbliche promosse per il contributo degli stakeholder, fra i quali con riguardo ai temi SSL AIAS ed ENSHPO. L'obiettivo è sviluppare linee guida chiare, buone pratiche e standard tecnici che traducano i principi di trasparenza, responsabilità e sorveglianza umana in requisiti per soluzioni pratiche. Solo costruendo un ecosistema di fiducia sarà possibile garantire che l'IA diventi uno strumento per creare luoghi di lavoro più sicuri, garantendo il rispetto dei diritti fondamentali che costituisce lo scopo del regolamento.

1. Cfr: https://www.aias-sicurezza.it/documenti-rete-giuridica-aias/sec6643ca
2. Cfr: https://eur-lex.europa.eu/eli/reg/2024/1689/oj