

**Roberto Sammarchi**

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



L'impatto dell'intelligenza artificiale sui dispositivi di protezione individuale: convergenze e distanze regolatorie con il settore medico

L'introduzione di sistemi avanzati nei contesti industriali sta mutando profondamente il concetto classico di tutela della salute dei lavoratori.

I dispositivi di protezione individuale (DPI), storicamente concepiti come barriere passive adibite alla difesa dell'integrità fisica contro agenti esterni, si stanno rapidamente trasformando in strumenti intelligenti e interconnessi.

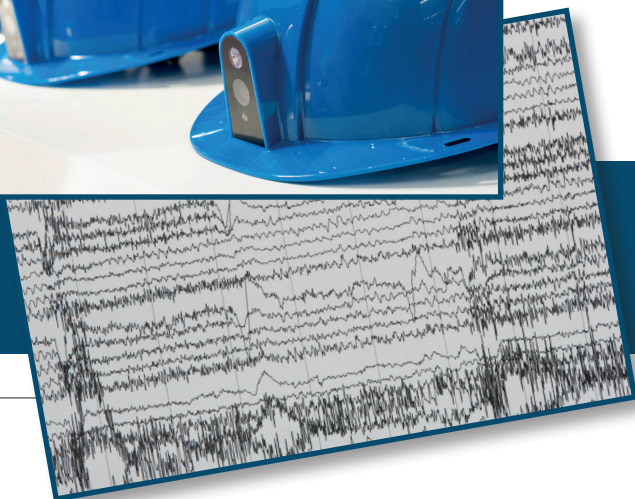
L'adozione di sensori biometrici e ambientali, unita ad algoritmi di apprendimento automatico, permette oggi di raccogliere ed elaborare flussi informativi complessi in tempo reale.

Il Regolamento (UE) 2023/1230 relativo alle macchine ha già formalizzato l'ingresso di queste tecnologie nell'ambiente manifatturiero, riconoscendo esplicitamente come i software che svolgono funzioni di sicurezza e mostrano comportamenti evolutivi debbano essere qualificati come veri e propri componenti di sicurezza autonomi.

L'evoluzione tecnologica evidenzia scenari complessi sotto il profilo giuridico, dove i confini tradizionali tra la protezione antinfortunistica e il monitoraggio biomedico tendono a dissolversi, sollevando delicate questioni di conformità per i fabbricanti e di responsabilità per le direzioni aziendali.

LA CONVERGENZA TECNOLOGICA TRA SMART DPI E TECNOLOGIE CLINICHE

Un DPI di nuova generazione, quale un casco dotato di elettrodi per l'elettroencefalografia finalizzato a prevenire i colpi di sonno nei conducenti, o una giacca da lavoro sensorizzata capace di monitorare costantemente la frequenza cardiaca e la temperatura corporea dell'operatore in ambienti confinati, condivide la medesima infrastruttura di base di un comune dispositivo medico. Entrambe le tipologie



di hardware poggiano su pilastri tecnici identici, che possono ricalcare la definizione di sistema di intelligenza artificiale nell'ordinamento europeo (AI Act, Art. 3, punto 1): l'autonomia operativa adattabile, la capacità di inferenza su base probabilistica e l'idoneità dell'output a influenzare contesti fisici o digitali.

La raccolta e l'analisi di parametri vitali per prevenire un malore termico in cantiere può sfruttare logiche predittive analoghe a quelle utilizzate dai software clinici destinati alla previsione del deterioramento clinico dei pazienti nei reparti di terapia intensiva. L'infrastruttura algoritmica non opera secondo schemi deterministici rigidi, ma agisce come un agente predittivo autonomo in grado di interpretare variazioni fisiologiche anche minime, modificando in modo sostanziale l'approccio alla prevenzione aziendale.

IL NODO DELLA PARZIALE CONVERGENZA E LA DOPPIA CERTIFICAZIONE

L'inquadramento normativo coordinato richiede un'attenta disamina della destinazione d'uso impressa dal fabbricante al prodotto. L'esame dell'architettura regolatoria generale mostra come l'evoluzione della tecnologia generi una sovrapposizione tra corpi normativi differenti. Qualora uno smart DPI sia progettato non solo per proteggere da un rischio professionale specifico, ma incorpori funzioni destinate esplicitamente alla diagnosi precoce o alla prevenzione di patologie cliniche individuali, il fabbricante si troverà obbligato a seguire un percorso di doppia certificazione. Sarà necessario soddisfare contemporaneamente i requisiti essenziali previsti dal Regolamento (UE) 2016/425 sui DPI e i parametri di prestazione e sicurezza clinica imposti dal Regolamento (UE) 2017/745 (MDR).

L'intersezione con l'AI Act (Regolamento UE 2024/1689) aumenta questa complessità. I sistemi di intelligenza artificiale utilizzati come componenti di sicurezza all'interno di prodotti soggetti a valutazione della conformità da parte di terzi sono oggi catalogati ex lege come sistemi ad alto rischio. Di conseguenza, sia i dispositivi medici digitali sia gli smart DPI

avanzati che integrano funzioni di sicurezza ricadono nell'applicazione del Capo III dell'AI Act.

I produttori sono tenuti a implementare un sistema di gestione dei rischi specifico per l'IA, a garantire una rigorosa governance dei dati priva di bias legati a etnia o età, e ad assicurare la tracciabilità mediante logging automatico.

Il pacchetto legislativo di semplificazione denominato Digital Omnibus, approvato a maggio 2026, ha esteso i termini di applicazione per i sistemi integrati nei prodotti regolati dalle normative dell'Allegato I, posticipando la scadenza definitiva al 2 agosto 2028. La dilazione temporale rappresenta un'opportunità di rilievo per il comparto industriale, consentendo la reingegnerizzazione dei fascicoli tecnici in coordinamento con gli standard europei armonizzati.

DIVERGENZE NORMATIVE E FILOSOFIE REGOLATORIE A CONFRONTO

Nonostante la forte prossimità sul piano ingegneristico, i due sistemi normativi rispondono anche a logiche divergenti.

La normativa sulla sicurezza nei luoghi di lavoro si impernia sulla riduzione del rischio occupazionale nell'ambiente d'impresa, ponendo in capo al datore di lavoro un dovere di tutela collettiva dei dipendenti.

La disciplina dei dispositivi medici è invece focalizzata sul beneficio clinico diretto per il paziente, bilanciato rispetto ai rischi clinici intrinseci.

Una marcata divergenza emerge nell'approccio alla gestione del rischio algoritmico.

Il Regolamento Macchine 2023/1230 richiede che la valutazione dei rischi operata dal fabbricante consideri le variazioni del comportamento del sistema durante l'intero ciclo di vita, focalizzandosi sulle interazioni dinamiche all'interno di un insieme di macchine e sulle possibili azioni autonome in ambienti non strutturati.

L'AI Act, di contro, pone l'accento sulla tutela dei diritti fondamentali e richiede protezioni avanzate

contro vulnerabilità informatiche peculiari dell'intelligenza artificiale, quali il *data poisoning* e gli *adversarial examples*. Nel settore medico, un malfunzionamento del software può condurre a dosaggi farmacologici tossici; nel settore della sicurezza sul lavoro, un difetto inferenziale di uno smart DPI o di un componente software integrato può tradursi in una lesione traumatica causata dal mancato arresto di un elemento meccanico in movimento.

PROFILI DI RESPONSABILITÀ PER IL DATORE DI LAVORO E TUTELA DEI DATI

L'adozione di strumenti di protezione basati su modelli predittivi introduce elementi di novità circa l'accertamento della responsabilità in caso di infortunio. L'affidamento acritico nei confronti dell'output dell'intelligenza artificiale (il noto fenomeno dell'*automation bias*) configura una condotta colposa per negligenza o imprudenza sia in capo al medico che si adegua passivamente al suggerimento della macchina, sia in capo al datore di lavoro che omette l'attivazione di controlli tradizionali confidando ciecamente nella vigilanza algoritmica.

Se uno smart DPI non segnala una situazione di pericolo a causa di un difetto intrinseco del software o di un disallineamento dei dati (*data drift*), la responsabilità contrattuale ed extracontrattuale coinvolgerà il fabbricante per il difetto del prodotto, ma lambirà l'organizzazione aziendale qualora sia dimostrata una carente manutenzione dei sistemi locali o una mancata implementazione degli aggiornamenti necessari.

La gestione continua di dati biometrici dei lavoratori solleva inoltre problematiche in tema di protezione dei dati personali. L'applicazione del Regolamento



(UE) 2016/679 (GDPR) deve coordinarsi, nell'ordinamento nazionale, con i divieti tassativi sanciti dall'articolo 4 dello Statuto dei Lavoratori in materia di controllo a distanza.

La raccolta dei parametri vitali deve essere rigorosamente finalizzata alla prevenzione dei rischi e i dati devono essere trattati in forma pseudonimizzata o anonimizzata, garantendo l'accesso esclusivo al medico competente ed escludendo qualsiasi monitoraggio disciplinare da parte della direzione aziendale.

La robustezza informatica del sistema diventa così un vincolo di sicurezza antinfortunistica: un attacco alla riservatezza potrebbe alterare le soglie di allarme del dispositivo, esponendo i lavoratori a rischi non più gestiti.

LINEE GUIDA OPERATIVE PER UNA COMPLIANCE INTEGRATA

La complessità dello scenario regolatorio descritto richiede alle aziende l'adozione di un approccio strutturato, volto a incorporare la conformità normativa sin dalle fasi preliminari di acquisto dei sistemi (*compliance by design*).



Per le direzioni aziendali e i responsabili dei servizi di prevenzione e protezione si suggeriscono le seguenti linee d'azione:

— Analisi dei sistemi

Sottoporre a una approfondita analisi preliminare ogni nuovo dispositivo di protezione o componente software intelligente, verificando le dichiarazioni di conformità del produttore, la documentazione tecnica e l'effettiva presenza di interfacce chiare destinate a garantire il controllo umano.

— Integrazione dei sistemi di gestione

Transitare verso un sistema di gestione integrato che armonizzi le procedure della ISO 45001 sulla salute e sicurezza sul lavoro con i requisiti gestionali della ISO/IEC 42001 (specifica per l'IA) e della ISO/IEC 27001 sulla cybersicurezza, applicando laddove opportuno le metodologie della ISO 14971 per estendere la valutazione dei rischi alle criticità tipiche del machine learning.

— Vigilanza e comitati interni

Istituire comitati di valutazione multidisciplinari, sul modello dei Board ospedalieri, al fine di vigilare sulle introduzioni tecnologiche ed evitare che accordi contrattuali opachi trasferiscano la responsabilità legale sull'utilizzatore finale.

— Piani di alfabetizzazione informatica

Investire in programmi organici di formazione tecnica e critica rivolti ai lavoratori, fornendo loro gli strumenti conoscitivi necessari per comprendere i limiti intrinseci, i margini di errore statistico e le metriche di funzionamento dei dispositivi indossati, riaffermando il primato della decisione umana e della prudenza operativa rispetto all'automatismo digitale.

L'orizzonte europeo della sicurezza sul lavoro richiede uno sforzo di riorganizzazione dei processi che, se adeguatamente governato, consente di trasformare la conformità in un fattore di sviluppo per imprese sane, protette ed eticamente sostenibili.