



L'Intelligenza Artificiale per la Salute e Sicurezza sul Lavoro

Alcuni contributi sulle opportunità e sulle criticità della applicazione dell'IA nel mondo del lavoro

Alcune immagini sono concesse dal **Museo virtuale per la sicurezza** della Fondazione Aifos

Presentazione

Gilberto Boschioli
Presidente CIIP

L'IA è la capacità dei sistemi informatici di apprendere, ragionare e fornire soluzioni e può essere un potente alleato in diversi ambiti lavorativi e di vita, analizzando enormi volumi di dati per fornire raccomandazioni proattive.

Il tema è di grande attualità, non c'è giorno che non compaia qualche articolo o documento che parli dell'IA e anche in ambito Salute e Sicurezza sul Lavoro non c'è convegno, seminario o corso di formazione che non vi dedichi almeno una relazione, senza contare gli innumerevoli articoli sulle pubblicazioni di settore e no.

In questo fiume di parole, più a carattere torrentizio che non il calmo fluire dei grandi e consolidati corsi d'acqua, regna tuttavia una grande confusione, dove non è facile distinguere gli interventi seri e documentati dal chiacchiericcio di moda senza o quasi fondamenti scientifici.

Da una parte sembrano schierarsi gli entusiasti, che attribuiscono all'AI poteri e potenzialità incredibili, in grado di stravolgere il ruolo degli umani, dall'altra i catastrofisti che vedono prevalere i rischi per gli utilizzatori e gli utenti, sino ad arrivare a ipotesi fantascientifiche di un mondo dominato dalle macchine e con un ruolo ormai marginale per le persone.

È indubbio, tuttavia, che l'IA avrà un'importanza rilevante anche nell'ambito della prevenzione e, proprio per questo, la Consulta ha ritenuto doveroso cercare di fare un po' di chiarezza in tutto questo gran parlare, raccogliendo pareri scientificamente documentati e le esperienze serie già sperimentate.

Lo ha fatto con il suo consueto stile e metodo: si è costituito un Gruppo di Lavoro ad hoc, con membri di diversa estrazione e competenze professionali. Dopo il primo periodo di discussione generale per delimitare il campo e focalizzare i temi da trattare, a ciascuno è stato assegnato un argomento da approfondire, secondo le proprie competenze ed esperienze professionali. Ciascun argomento è stato poi presentato e ampiamente discusso in tutto il GdL sino ad arrivare a condividerne le linee generali che poi ciascun autore ha sviluppato.

Il metodo è peculiare e specifico di CIIP, unico nel panorama associativo italiano, ed è il suo punto di forza: riunire attorno a un tavolo su temi controversi professionalità molto diverse, per arrivare a documenti finali condivisi.

Antonio Grieco, il fondatore mai dimenticato della Consulta, nel lontano 2002 già affermava:

“Sicurezza e Prevenzione non sono l'acuto di un tenore ma il risultato finale di un percorso sistemico integrato, un concerto di voci diverse sapientemente orchestrato”

L'E-Book affronta un'ampia serie di argomenti che delineano lo “stato dell'arte” sul ruolo dell'IA nella prevenzione:

- Evoluzione del lavoro nell'era dell'intelligenza artificiale
- Valutazione dei rischi e responsabilità
- Partecipazione dei lavoratori
- Formazione e gestione del cambiamento
- Benessere psico-fisico e ruolo del medico competente
- Aspetti giuridici, etici e sostenibilità.

Il documento è inoltre corredato da una ricchissima bibliografia con le linee guida e di indirizzo più recenti pubblicate da Enti Istituzionali e altri autorevoli organismi.

Non posso che rinnovare i miei personali ringraziamenti a Rocco Vitale e Susanna Cantoni, che hanno coordinato i lavori del gruppo e a tutti i componenti per la loro consueta disponibilità.

Grazie anche a Lalla Bodini e a Enrico Cigada per la consulenza editoriale e agli autori dei manifesti che illustrano questo e-Book e realizzati dagli studenti dell'Accademia di Belle Arti Santa Giulia per conto della Fondazione Aifos.

Concludo ricordando che la serie di pubblicazioni della Consulta è sempre più ricca e ormai costituisce uno “strumentario” indispensabile per gli operatori della prevenzione:

- La promozione della salute in azienda
- Oltre la rete: Salute e sicurezza nella pesca professionale
- Alleggeriamo il carico
- Agenti chimici e cancerogeni
- Aging is art
- Rischi psicosociali
- Il D.Lgs 81/08 dieci anni dopo
- 1989-2019 CIIP La storia
- Salute e Lavoro oggi: le nuove sfide della Medicina del Lavoro
- Giudizio di idoneità e accomodamento ragionevole

solo per citare i documenti principali.

[Sul sito](#) si trovano tutte le pubblicazioni, scaricabili gratuitamente:

Introduzione

Rocco Vitale e Susanna Cantoni***

**Coordinatore del Gruppo di Lavoro*

*** Vicepresidente CIIP*

All'interno della CIIP, con il coinvolgimento attivo di esperti, docenti, studiosi ed operatori, si è sviluppato un approfondito confronto e dibattito sull'importanza e l'impatto dell'Intelligenza Artificiale nel mondo della salute e sicurezza sul lavoro.

E' stato creato un apposito Gruppo di Lavoro che ha impostato il lavoro in tre fasi. La prima fase è consistita nella raccolta del materiale e nella ricerca delle fonti istituzionali che a livello europeo (soprattutto) ed italiano avevano elaborato e (o approvato) norme o documenti. Tutta questa documentazione, utile ed importante ai fini di un approccio nel contesto sociale in cui operiamo, è stata pubblicata sul sito della CIIP, alla voce gruppo di lavoro IA, e costituisce un'utile ed importante raccolta bibliografica di riferimento che sta alla base di questo e-book.

Successivamente è iniziata una fase di discussione all'interno del gruppo con riunioni calendarizzate che hanno permesso di individuare i temi su cui concentrare l'attenzione e soprattutto l'importanza di approfondire gli aspetti legati alla sicurezza delle persone che vengono modificati con l'introduzione dell'intelligenza artificiale. Si è tentato di fare un passo in avanti passando dalle previsioni dell'intelligenza artificiale sul lavoro, condizione determinante, all'impatto sui lavoratori ed alla loro salute e sicurezza

L'Intelligenza artificiale (IA) rappresenta una trasformazione profonda nel mondo del lavoro, con impatti significativi sulla salute, sicurezza e benessere dei lavoratori. Questo documento esplora in modo articolato come l'IA influenzi vari aspetti della sicurezza sul lavoro, dalla valutazione dei rischi alla formazione, fino agli aspetti giuridici ed etici.

Un dibattito ed un confronto, in alcuni momenti anche difficile e complesso, interessante ed impegnativo che ha condotto alla scelta di specifici ambiti di intervento.

Evoluzione del lavoro nell'era dell'intelligenza artificiale

Viene presentata una sintesi dell'evoluzione tecnologica dall'intelligenza meccanica a quella artificiale, evidenziando la rivoluzione che l'IA comporta nel contesto lavorativo. Si analizza l'interazione tra uomo e IA, con particolare attenzione all'uso dell'IA in diversi settori e ai nuovi modelli di lavoro digitali, come quello dei riders, che pongono sfide specifiche per la sicurezza e la salute dei lavoratori.

Un progetto innovativo, RECKON, promosso da Inail, è descritto come esempio di tecnologie abilitanti per il monitoraggio degli elementi di contesto (operatore, macchina, ambiente) per prevenire incidenti sul lavoro, sottolineando l'impatto positivo dell'IA sulla sicurezza, ma anche le difficoltà incontrate.

In uno specifico articolo viene presentata un'ampia carrellata sull'utilizzo di nuove tecnologie che impiegano l'IA per eliminare o ridurre alcuni rischi lavorativi presenti in diverse attività/operazioni.

Valutazione dei rischi e responsabilità

Il documento approfondisce come l'impiego dell'IA debba modificare la valutazione dei rischi, integrando il fattore umano e le nuove frontiere tecnologiche. Vengono analizzati i rischi derivanti dalle interferenze tra macchina, uomo e ambiente, e le relative responsabilità. Si sottolinea

l'importanza di comprendere la logica progettuale delle tecnologie per individuarne i rischi connessi e gestire la manutenzione, con l'obiettivo di eliminare o ridurre gli specifici rischi lavorativi.

Partecipazione dei lavoratori

Un focus particolare è riservato al ruolo dei lavoratori nella gestione dell'IA, evidenziando la necessità della loro partecipazione nella progettazione, valutazione e gestione dei rischi. Sono discussi sia i documenti dell'EU OSHA sia le criticità e opportunità legate alla partecipazione degli attori aziendali della prevenzione, inclusi i rappresentanti dei lavoratori.

Formazione e gestione del cambiamento

L'IA è vista come strumento al servizio della formazione per la sicurezza sul lavoro. Vengono presentati approcci efficaci per l'addestramento, come l'uso dell'intelligenza artificiale nella guida di carrelli elevatori, e lo studio delle ricadute formative derivanti dall'uso di sistemi IA, sottolineando l'importanza di gestire il cambiamento attraverso una formazione mirata. Particolare attenzione è dedicata alle innovative opportunità offerte dalla IA per la valutazione nel tempo dell'efficacia della formazione.

Benessere psico-fisico e ruolo del medico competente

Il documento esamina i fattori di rischio per il benessere psico-fisico dei lavoratori legati all'uso dell'IA, le possibili conseguenze e le misure di prevenzione da adottare. Viene inoltre analizzato il ruolo fondamentale del medico competente nel contesto lavorativo con IA, per garantire la tutela della salute. Una recente indagine (in appendice), condotta mediante questionari somministrati ai lavoratori e pubblicata da Eurostat, quantifica alcuni effetti della digitalizzazione sui lavoratori (ritmi di lavoro, lavoro in solitario, sorveglianza sul lavoro, carico di lavoro, riduzione dell'autonomia).

Aspetti giuridici, etici e sostenibilità

Si affrontano gli aspetti giuridici e normativi relativi all'uso dell'IA nel lavoro, con particolare attenzione alla tutela della salute e sicurezza. Vengono discussi anche gli aspetti etici dell'IA, proponendo una visione di un ecosistema digitale basato sull'uomo, con prospettive future orientate alla sostenibilità nel lavoro con l'intelligenza artificiale.

Appendici e linee guida

Il documento si conclude con riferimenti al futuro del lavoro, all'agenda digitale italiana e alle linee guida sull'IA nel mondo del lavoro, fornendo un quadro completo e aggiornato per la gestione dell'intelligenza artificiale in ambito lavorativo.

In sintesi, questo e-book fornisce un'analisi multidimensionale dell'impatto dell'intelligenza artificiale sulla sicurezza e salute sul lavoro, integrando aspetti tecnologici, umani, formativi, giuridici ed etici, con l'obiettivo di promuovere un uso responsabile e sostenibile dell'IA nei contesti lavorativi.

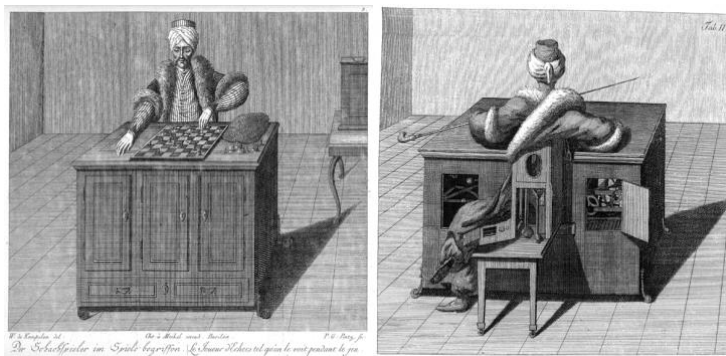
Ci siamo proposti di uscire dal dibattito tra "apocalittici e integrati", come già scriveva Umberto Eco negli anni '60, considerando l'IA una rivoluzione inarrestabile, che offre opportunità ma anche criticità sia per la sicurezza che per il benessere psicofisico dei lavoratori, tema sul quale abbiamo orientato questo lavoro.

Occorre prima di tutto comprendere i cambiamenti in atto e il loro impatto sulla organizzazione del lavoro, per poterli governare a vantaggio sia della qualità della produzione di beni e servizi che del benessere psico fisico dei lavoratori.

Molti articoli insistono, per ragioni diverse, sulla necessità di accompagnare l'introduzione delle nuove tecnologie con il coinvolgimento di tutte le figure aziendali utilizzatrici.

Tutti gli autori concordano che per non rischiare di essere travolti dalle innovazioni, che non sono solo di natura tecnologica, il loro governo dovrebbe essere un processo “democratico”, che deve vedere coinvolte tutte le figure aziendali (sia la *line* aziendale che i “consulenti” e i lavoratori); molteplici sono, infatti le conseguenze sotto i profili della sicurezza, del rispetto delle persone, della loro privacy, della configurazione degli obblighi e delle responsabilità anche giuridici. Alcune preannunciate scelte italiane, all’insegna della semplificazione, sembrano purtroppo negare alcuni di questi principi e virare verso una gestione decisamente verticistica sopprimendo addirittura alcuni diritti consolidati.

Da ultimo, il monito a non dimenticare che dietro e davanti alle nuove tecnologie, nella progettazione e nell’impiego, c’è sempre l’uomo la cui intelligenza critica deve far sì che le nuove tecnologie siano strumenti per migliorare la qualità e la sicurezza del lavoro. Alcuni articoli presentati in questo E-Book dimostrano che non sempre questo avviene e che in diversi casi le nuove tecnologie nascono da condizioni di lavoro molto arretrate (si veda l’articolo di Théophile Simon sui lavoratori filippini) o governano organizzazioni di lavoro altrettanto arretrate quale ad esempio quelle dei riders.



“Il Turco, creato nel 1769 dall’inventore Wolfgang von Kempelen (*ndr per Maria Tessa d’Austria*), veniva presentato come automa in grado di giocare a scacchi. In realtà all’interno della macchina si nascondeva uno scacchista in carne ed ossa. L’idea che oggi l’intelligenza artificiale sia del tutto autonoma è un’illusione simile a quella del turco. Dimentichiamo che dietro i processi apparentemente automatici dell’IA c’è il lavoro di umani chiamati ad ovviare ai limiti della tecnologia”. *Graham, docente di geografia dell’Internet all’Università di Oxford*

Ci scusiamo se alcuni temi sono trattati, sia pur con stile e taglio diverso, in diversi articoli; ciò è dovuto al fatto che gli articoli sono stati scritti senza un ordine temporale preciso in rapporto all’indice, che tra l’altro è andato modificandosi nel tempo proprio grazie ai primi articoli e al confronto all’interno del gruppo, che non sempre siamo riusciti a trasferire per tempo agli autori.

In questa prima edizione dell’E-Book non abbiamo trattato il tema dei costi ambientali, corollario dello sviluppo della IA, argomento di grande attualità ma anche complesso per le numerose implicazioni ambientali: aumento considerevole dei consumi energetici (è stato calcolato che il solo uso di ChatGPT consuma 3 volte l’energia che Google impiega per dare la stessa risposta), dei consumi di acqua per il raffreddamento delle apparecchiature, emissioni di gas serra, aumento dei rifiuti informatici con dispersione di materiali preziosi e sostanze tossiche. Su questi temi si comincia a fare i conti attraverso diversi studi. Una buona notizia, quantomeno per la questione dei rifiuti, è data dai progetti di alcune grandi imprese sull’utilizzo della IA nell’economia circolare, ad esempio con l’utilizzo di robot capaci di smontare diversi rifiuti elettronici e recuperare componenti, materie prime metalli preziosi (vedansi gli articoli pubblicati recentemente da Futura Network, Economist, ...).

Sono argomenti che speriamo di poter trattare in una seconda puntata.

Hanno collaborato alla realizzazione di questo e-book:

Susanna Cantoni: vicepresidente CIIP; **Rocco Vitale:** coordinatore Gruppo di lavoro sulla IA; **Enrico Cigada:** webmaster, curatore EBook e siti CIIP;

ed in ordine alfabetico: Antonio Baldassarre, Alberto Baldasseroni, Alice Caporale, Terenzio Cassina, Andrea Cirincione, Francesco Costantino, Matteo Cozzani, Alessio De Luca, Sonia Fagotti, Andrea Filippini, Barbara Gattoni, Mauro Iori, Cinzia Maiolini, Cristina Mora, Martina Padovan, Alessandro Palla, Paolo Pascucci, Wolfango Pirelli, Sergio Sangiorgi, Giovanni Scudier, Francesca Seghezzi, Rita Somma, Santi Spartà, Simon Théophile, Carlo Zamponi.

Un grande grazie ad Enrico Cigada che, con il suo impegno e professionalità, ha reso possibile questa pubblicazione. Grazie anche a Laura Bodini per i suoi suggerimenti bibliografici, redazionali e di divulgazione.

Un ringraziamento particolare alla Fondazione Aifos che ha promosso la realizzazione dei manifesti in occasione della campagna europea e agli studenti dell'Accademia Santa Giulia di Brescia che li hanno creati. Gli autori delle immagini da noi utilizzate sono indicati nella tabella che segue.

Tutti i manifesti realizzati sono visibili nel "[Museo virtuale per la sicurezza](#)" promosso dalla Fondazione Aifos, Accademia e CIIP.

Il Gruppo di Lavoro di CIIP è composto da: Rocco Vitale, Susanna Cantoni, Cassina Terenzio, Fagotti Sonia, Gattoni Barbara, Francesco Draicchio, Massimo Maldera, Graziano Maranelli, Iori Mauro, Sergio Sangiorgi, Santi Spartà, Giovanni Scudier, Wolfango Pirelli, Giulia Radici (segreteria organizzativa CIIP).

Le immagini concesse dal [Museo virtuale per la sicurezza](#) della Fondazione Aifos sono:

Copertina Anna Percaccini : *Il cervello crea...*

1.1 Cristina Biloni e Nicole Maria Madonia: *Migliora le tue skills...*

1.2 Elisabetta Armani: *L'innovazione...*

1.7 Gaia Bertoli: *Mattoni o pixel*

4.1 Giulia Cavion, Federica Gava: *Sicurezza...*

4.3 Elisabetta Armani: *L'AI non è magia...*

4.3 Giulia Albertelli, Giorgia Di Fonzo: *Affronta il labirinto*

5.1 Vittoria Zambaiti: *Credi ai tuoi occhi*

5.1 Valeria Fogazzi: *Non lasciarti annullare dalla tecnologia*

6.1 Federico Rossi: *Anche il mondo digitale...*

7.3 Cristina Biloni, Nicole Maria Madonia: *Cavalca l'onda dell'IA*

7.5 Cristina Biloni, Nicole Maria Madonia: *Orientati nel*

SOMMARIO

PRESENTAZIONE	2
<i>Gilberto Boschioli</i>	
INTRODUZIONE	4
<i>Rocco Vitale e Susanna Cantoni</i>	
1 IL LAVORO NELL'EPOCA DELL'INTELLIGENZA ARTIFICIALE	10
1.1 Dall'intelligenza meccanica all'intelligenza artificiale: sintesi dell'evoluzione e rivoluzione tecnologica	10
<i>Antonio Baldassarre e Alberto Baldasseroni</i>	
1.2 L'impatto dell'Intelligenza Artificiale sulla salute e la sicurezza al lavoro: principali indicazioni dell'Agenzia Europea EU-OSHA	20
1.3 Intelligenza artificiale e l'uso nel contesto della salute e sicurezza del lavoro: l'uomo di fronte alla A.I.	23
<i>Andrea Cirincione</i>	
1.4 L'utilizzo di nuove tecnologie per eliminare o ridurre rischi lavorativi: nuove tecnologie, DPC, DPI	32
<i>Cristina Mora e Alice Caporale</i>	
1.5 L'utilizzo di piattaforme digitali e la salute e sicurezza dei lavoratori: l'esempio dei riders	46
<i>Francesca Seghezzi</i>	
1.6 Presentazione progetto REKON per la prevenzione di incidenti sul lavoro da interferenze macchina/lavoratore	48
<i>Wolfango Pirelli</i>	
1.7 Integrazione dell'intelligenza artificiale per la sicurezza nei contesti industriali	49
<i>Andrea Filippini</i>	
2 INTELLIGENZA ARTIFICIALE E VALUTAZIONE DEI RISCHI	52
2.1 Valutazione dei rischi, il fattore umano e le nuove frontiere dell'intelligenza artificiale	52
<i>Rita Somma</i>	
2.2 La valutazione del rischio e responsabilità: rischi connessi alle interferenze macchina-uomo-ambiente e relative responsabilità	60
<i>Francesco Costantino</i>	
2.3 La necessità di conoscere la logica che sottende la progettazione al funzionamento delle tecnologie applicate, funzionale alla individuazione dei rischi nonché agli aspetti manutentivi	66
<i>Alessandro Palla e Antonio Baldassarre</i>	
3 INTELLIGENZA ARTIFICIALE E PARTECIPAZIONE DEI LAVORATORI	75
3.1 The Filipino workers at the sharp end of AI	75
<i>Théophile Simon</i>	
3.2 Documenti EU OSHA: la partecipazione dei lavoratori	76
<i>Rocco Vitale</i>	
3.3 La partecipazione degli attori aziendali della prevenzione nella progettazione, valutazione e gestione dei rischi: criticità, opportunità, ruolo della <i>line</i> aziendale	79
<i>Sonia Fagotti</i>	
3.4 La partecipazione degli attori aziendali della prevenzione nella progettazione, valutazione e gestione dei rischi. Criticità, opportunità, ruolo dei lavoratori e dei loro rappresentanti	89
<i>Cinzia Maiolini e Alessio De luca</i>	
4 LA FORMAZIONE PER LA SICUREZZA CON L'INTELLIGENZA ARTIFICIALE PER GESTIRE IL CAMBIAMENTO	94
4.1 Intelligenza Artificiale al servizio della Formazione: quale approccio efficace per la Sicurezza sul Lavoro alla luce degli scenari attesi.	94
<i>Matteo Cozzani</i>	
4.2 Le ricadute formative previste dall'accordo Stato-Regioni con l'utilizzo dell'intelligenza artificiale	99
<i>Carlo Zamponi e Rocco Vitale</i>	
4.3 Costruzione di parametri di benchmark per la valutazione obiettiva dell'efficacia e dell'efficienza nella comunicazione del rischio in ambiente di lavoro	104
<i>Santi Sparta</i>	

4.4	L'Accordo Stato Regioni e l'intelligenza artificiale <i>Rocco Vitale</i>	119
5	INTELLIGENZA ARTIFICIALE E BENESSERE PSICOFISICO DEI LAVORATORI	124
5.1	IA e benessere psico fisico dei lavoratori: fattori di rischio, possibili conseguenze e misure di prevenzione <i>Barbara Gattoni e Sergio Sangiorgi</i>	124
6	IL RUOLO DEL MEDICO COMPETENTE NEL LAVORO CON IA	135
6.1	Il ruolo del Medico Competente nel lavoro con AI <i>Terenzio Cassina</i>	135
7	ASPETTI GIURIDICI ED ETICI	145
7.1	Sistemi di intelligenza artificiale e tutela della salute e della sicurezza sul lavoro <i>Paolo Pascucci</i>	145
7.2	Intelligenza Artificiale, AI Act e sicurezza del lavoro <i>Giovanni Scudier</i>	149
7.3	Aspetti normativi dell'intelligenza artificiale in campo lavorativo <i>Mauro Iori</i>	163
7.4	Linee Guida IA del MLPS	169
7.5	Considerazioni etiche sulla Intelligenza Artificiale in Medicina del Lavoro <i>Antonio Baldassarre e Martina Padovan</i>	170
8	APPENDICE – DOCUMENTI DA SCARICARE	176
8.1	Regolamento EU AI 13 giugno 2024	176
8.2	Il futuro del lavoro, Davos, 2025	176
8.3	Agenda digitale italiana	176
8.4	Disposizioni e deleghe al Governo in materia di intelligenza artificiale	176
8.5	Presentazione volume INAPP	176

1 Il lavoro nell'epoca dell'intelligenza artificiale

1.1 Dall'intelligenza meccanica all'intelligenza artificiale: sintesi dell'evoluzione e rivoluzione tecnologica

Antonio Baldassarre*, Alberto Baldasseroni **

*Prof. Medicina del Lavoro- Università degli studi Firenze

**Medico del lavoro, già Responsabile del CeRIMP-Toscana

Infine, i reggitori della cosa pubblica dovranno capire che la medicina preventiva, per la sua natura e i suoi compiti, per la sua "quantità" e la sua "qualità", non può più fare a meno dei moderni mezzi di calcolo e di elaborazione, ma quando li avrà avuti non sarà più assolutamente la stessa.

Sarà una nuova medicina per una nuova società.

G.A. Maccacaro

Lo sviluppo delle macchine e la capacità di elaborare informazioni hanno apportato contributi immensi alla storia umana, trasformando il nostro stile di vita, le nostre abitudini lavorative e l'interazione con il mondo. Dai dispositivi meccanici per svolgere compiti ripetitivi e pre-programmati, abbiamo percorso una lunga strada verso sistemi altamente sviluppati in grado di simulare i processi di pensiero umano, aprendo così nuove prospettive nell'ambito dell'Intelligenza Artificiale (IA). Questo capitolo si propone di seguire questa linea di sviluppo, esaminando i punti critici che hanno trasformato l'intelligenza meccanica in IA, con particolare attenzione a come questa rivoluzione tecnologica abbia plasmato lo sviluppo del lavoro e delle macchine.

Buoni maestri

Nel corso della storia che, passo dopo passo, sta portando all'avvento dell'IA in medicina, un posto d'onore spetta senza dubbio a Giulio Maccacaro. È il "primo" M., quello che negli anni Sessanta fonda e dirige la rivista A.b.d.c.e. dedicata alle applicazioni biomediche del calcolo elettronico, il M. artefice e direttore dal 1966 dell'Istituto di Biometria di Milano, colui che introduce nel nostro paese un campo nuovo di studi, la statistica applicata alla medicina sperimentale e infine l'epidemiologia¹. L'interesse di Maccacaro per l'informatica come scienza dell'informazione in medicina è quindi precoce e approfondito.

"...l'enorme spiegamento strumentale del rilievo semeiotico, la concentrazione delle indagini diagnostiche, il libero accesso all'assistenza sanitaria, l'evoluzione della medicina da curativa a preventiva, l'espansione dell'epidemiologia alle malattie non infettive, la necessità di una vigilanza farmaco-tossicologica di largo raggio, la redistribuzione di esperienze cliniche, la ristrutturazione dell'organizzazione sanitaria centrale e periferica. Da tutte è posta concordemente l'esigenza, mai prima avvertita in altrettale misura, di coordinare, trasformare e conservare ingenti e crescenti quantità di informazione"².

L'entusiasmo per queste novità trovava nel seguente passaggio espressione ancor più completa:

¹ Saracci R. Informazione per la salute e deformazioni della salute: uno sguardo critico sull'epidemiologia postmoderna. *Epid.Prev.* Anno 31 (5) settembre-ottobre 2007, p.239-246.

² G.A. Maccacaro, A. Colombi Applicazione dell'elaborazione Elettronica alla Medicina "A.b.d.c.e.", anno II, 4, 1967, pp. 175-208, ora in: Giulio A. Maccacaro PER UNA MEDICINA DA RINNOVARE Scritti 1966-1976. Feltrinelli, Milano, 1979, pag.17

“... l'incontro tra medicina ed elaborazione automatica dell'informazione non è il risultato della contingenza ma della necessità. Infatti, è come se il medico avesse moltiplicato, nell' arco di poche generazioni, da un lato le sue afferenze sensoriali e dall'altro le sue efferenze motorie: la storia dell'evoluzione naturale dimostra che a ciò corrisponde sempre un aumento di capacità e di complessità del sistema nervoso centrale. Per questo non è forse eccessivo dire che se la medicina contemporanea non avesse già incontrato i calcolatori andrebbe cercandoli e prevedere che negli anni a venire le forme e i contenuti della sua domanda non saranno senza traccia sullo sviluppo e sulla differenziazione degli elaboratori”³.

In questo scritto, M. si riferiva al ruolo del “Calcolatore” nei confronti della medicina nei suoi aspetti preventivi, curativi e riparativi, ma il cuore del suo ragionamento trattava dell'informazione disponibile già allora e in futuro prevedibilmente molto più ampia. Riferendosi alla funzione “preventiva” della medicina del futuro M. così si esprimeva:

“Ciò equivale, chiaramente, non solo a raccogliere grandi quantità di informazione medica su larghe popolazioni, ma a preordinare un accumulo della stessa in forme idonee ad operazioni continue o periodiche di coordinamento, confronto, recupero. Poiché tali informazioni hanno rilevanza a ciascuno dei livelli fondamentali della biologia umana: individuo, famiglia e comunità e poiché ad ognuno di questi livelli esse nascono in sedi e tempi diversi, si rende evidente l'esigenza di un sistema dinamico di *data linkage* del quale la necessità è da più parti avvertita, la portata è difficilmente sopravvalutabile e la complessità organizzativa supera le possibilità dei sistemi tradizionali”⁴.

L'autore si mostrava consapevole dell'ampiezza del fenomeno segnalato che andava ben al di là delle applicazioni in campo medico:

“È, anzi, indicativo come ... le dimensioni del problema siano divenute ormai tali da renderne comuni le soluzioni possibili o, più realisticamente, le dubbie possibilità di una soluzione: infatti la realizzazione di un archivio medico automatico - inteso come sistema compatto per la raccolta, il trattamento, la conservazione ed il recupero dell' informazione che si crea, con un flusso continuo e crescente, nelle corsie e nei laboratori - non è che un aspetto settoriale del ben più vasto problema della analisi di informazioni narrative e della classificazione dei loro significati”⁵.

A quest'ultimo proposito la bibliografia citata dallo scienziato lombardo segnalava un nome noto anche per le sue posizioni in campo politico e sociale, Noam Chomsky, aprendo in questo modo una finestra sul mondo della linguistica moderna, vera *nursery* dell'IA come la viviamo oggi.

Ma congediamoci dal pensiero di M. con un'ultima citazione che è difficile non definire “preveggente”:

“Se si prescinde dall' aspetto sensoriale del problema - per il quale sono disponibili diverse soluzioni - e si porta l' attenzione su quello logico, si constata l'esigenza di due approcci fondamentali (Rosen, 1967): l'uno mira alla costruzione di macchine costituite da reti modulabili che modificano automaticamente e progressivamente la loro struttura interna come risultato di *apprendimento* ottenuto per esposizioni successive di forme correttamente classificate. L'altro approccio, ovviamente più modesto ma oggi più praticabile, stabilisce in via statistica l'importanza relativa dei caratteri formali valutando la probabilità di ciascuno o di combinazioni degli stessi di presentarsi nelle forme categorizzate. Una macchina adeguatamente programmata può utilizzare tali statistiche così da minimizzare errori di classificazione. E questo secondo approccio, comprensibilmente, quello

³ Ibidem.

⁴ Ivi, pag.23

⁵ Ivi, pag.25

adottato da chi sta attualmente esplorando le possibilità di usare l'elaborazione automatica per problemi di *diagnosi per riconoscimento*"⁶.

Se al tempo in cui scriveva l'approccio di *machine learning* era ancora prematuro nei nostri anni ciò non è più vero.

Non arruoleremo certo M. tra gli entusiasti profeti dell'IA, perché al contrario la sua lucida coscienza critica rilevava già allora i rischi insiti nel modo in cui la manipolazione dell'informazione andava profilandosi. Tuttavia, questa parte dell'opera di M. ci spinge ad approfondire alcuni aspetti del retroterra dal quale origina l'IA di cui oggi tanto si discute.

Linguistic Turn e IA

"Qual è l'utilità della linguistica? [...] è evidente che le questioni linguistiche interessano tutti quelli che, siano storici o filologi, ecc., devono maneggiare testi"⁷.

Il secolo che sta alle nostre spalle è stato caratterizzato dall'irrompere sulla scena della "Linguistica" ossia degli studi sempre più approfonditi sul ruolo e le caratteristiche del linguaggio umano nella comunicazione in qualunque forma essa si realizzi. Semiotica come studio dei segni e delle modalità di trasmissione e semantica, come contenuto del linguaggio hanno permeato di sé molta della Scienza/Filosofia del XX secolo. Anche il campo biologico è stato investito direttamente da questa temperie quando Watson e Crick hanno descritto il "linguaggio della vita" contenuto nel DNA. Le successive tappe nel riconoscimento dei componenti di questo linguaggio e della sua sintassi sono sfociate nel Progetto Genoma con cui alcuni anni fa Craig Venter giunse a decrittare l'intera sequenza del DNA umano. Non può sfuggire l'analogia con la scoperta della stele di Rosetta per il linguaggio dei geroglifici o delle Tavole Eugubine per quello del popolo degli Umbri.

Quindi decifrare il linguaggio e trarne delle regole di sintassi è un passo obbligato per la costruzione dell'IA, passo che fu compiuto progressivamente, nel corso dei decenni, attraverso varie tappe, conosciute con sigle un po' criptiche (*Content analysis*, NLP - *Natural Language Processing*, ML - *Machine learning*, LLMs - *Large Language Models*, LIMs - *Large Image models*, ecc.) rese possibili dalla disponibilità sempre crescente di risorse di calcolo nei moderni processori elettronici, ma al contempo da una massa di informazioni veicolate nella rete delle reti, Internet, la cui entità è del tutto incommensurabile con quanto in precedenza disponibile.

In definitiva, il *Linguistic Turn* ha avuto un impatto importante su come pensiamo l'intelligenza, la conoscenza e la rappresentazione – tutti elementi fondamentali per l'IA. Anche se non c'è una linea diretta e univoca, c'è un dialogo concettuale profondo tra filosofia del linguaggio e sviluppo dell'IA, sia nelle sue basi teoriche sia nelle sue trasformazioni più recenti.

Corollario di questi sviluppi è la definitiva caduta degli steccati disciplinari fra cosiddette Scienze della Natura e Scienze Umane, per definire, tra gli altri, nuovi campi di conoscenza come nel caso delle Digital Humanities e della "Culturomics" sorta di lessicologia computazionale sviluppata a partire dal progetto di Google Books e di N-Gram viewer.

Un secondo punto di repere in questo percorso verso l'IA ci viene dal pensiero e dagli scritti di un altro "buon Maestro" degli anni '70, Marcello Cini, di laurea ingegnere, di vocazione fisico, insegnante all'Università La Sapienza di Roma nella facoltà di Fisica, nel decennio precedente animatore del dibattito interno al PCI sul ruolo della scienza in relazione con la società civile. Più che

⁶ Ivi, pag.40 Il corsivo nell'originale.

⁷ Capitolo II Materia e compiti della linguistica suoi rapporti con le scienze connesse, pag.16 Da: Saussure, F. de. "Corso di linguistica generale, introduzione, traduzione e commento di Tullio De Mauro." *Roma-Bari: Laterza* (2005 19° Ed.).

al famoso libro collettaneo “L’Ape e l’Architetto” che tante polemiche provocò alla sua prima uscita nel 1976, ci riferiamo alle riflessioni di Marcello Cini contenute nel suo contributo critico alla riedizione di quel testo avvenuta nel 2011, trentacinque anni dopo la sua prima pubblicazione⁸. In questo testo Cini riflette sui grandi cambiamenti intercorsi nel frattempo e sul significato della produzione capitalista di beni materiali e immateriali. La profonda differenza fra questi ultimi rispetto ai primi è alla base del passaggio dalla fase “meccanica” della produzione capitalista, soggetta alle cicliche crisi di sovrapproduzione e di distruzione della base produttiva, alla fase “informatica”, che ha come oggetto l’informazione e la sua trasformazione in merce, sia pure immateriale, ma al tempo stesso non soggetta a deterioramento o a “sovrapproduzione” bensì ad accrescimento cumulativo, senza limiti.

“La definizione di merce immateriale è dunque autocontraddittoria. È l’unica “merce” che, all’atto del suo consumo, non solo non viene a “deperire”, a finire e produrre scarti, ma produce altra *materia prima*, nuova e in relazione con la precedente, che moltiplica la materia prima a disposizione dell’industria di produzione di senso e della produzione della sfera cognitiva generale dell’umanità.”

“La dimensione della rete planetaria produce un fattore di moltiplicazione impensabile fino a pochi anni or sono, una moltiplicazione che allude ad una capacità nuova che sembra emergere come un fattore adattativo di nuova specie. La sedimentazione culturale (tutte le conoscenze accumulate dall’umanità nel corso della storia e disponibili al genere umano) e i processi di comprensione e socializzazione delle stesse idee, che le persone si fanno di queste nozioni accumulate, rappresentano un *background* gigantesco che viene messo in produzione attraverso i nuovi modelli di economia basati sull’informazione”.

Sono questi i concetti che stanno alla base dell’IA, qualsiasi sia l’applicazione che di essa si intenda fare.

Tornando all’oggi

Se definiamo “Intelligenza Meccanica” (IM) la fase iniziale dell’interazione uomo-macchina, definita dalla capacità delle macchine di svolgere compiti fissi e ripetitivi con precisione ed efficienza, si capisce come questa “intelligenza” non è legata alla comprensione o all’indipendenza, ma si fonda esclusivamente sulla rigorosa osservanza delle istruzioni impartite. Storicamente, l’IM ha raggiunto il suo apice nel campo dell’automazione industriale, dove paradigmi produttivi come il fordismo e il taylorismo hanno ridefinito la produzione in termini di scomposizione dei compiti e standardizzazione dei processi. Qui, le macchine si sono evolute come strumenti integrativi del lavoro umano per massimizzare l’efficienza e la produttività attraverso la replicazione meccanica dei compiti.

Uno dei concetti centrali che emergono a questo punto è il computazionalismo, che considera la mente come una macchina per l’elaborazione delle informazioni, simile a un computer. Nel suo articolo “Computing Machinery and Mentality”⁹, Barry McMullin riprende questo concetto, esaminando in che misura la capacità della macchina di elaborare simboli la renda concepibile come una rappresentazione della mente. Tuttavia, McMullin presenta anche i limiti di tale prospettiva, in particolare con la presentazione dell’argomento della “stanza cinese” di John Searle¹⁰.

⁸ Marcello Cini, L’Ape e l’Architetto: trentacinque anni dopo. In: Giovanni Ciccotti, Marcello Cini, Michelangelo de Maria, Giovanni Jona-Lasinio L’Ape e l’Architetto-Paradigmi scientifici e materialismo storico. FrancoAngeli, Milano, 2011.

⁹ McMullin B. Computing machinery and mentality. *Brain Cogn.* 1997 Jun;34(1):28-47. doi: 10.1006/brcg.1997.0905

¹⁰ Searle, John (1980). Minds, brains, and programs. *Behavioral and Brain Sciences* 3 (3):417-57

Per Searle, sebbene la manipolazione simbolica possa generare risposte apparentemente intelligenti, questo non equivale a una vera comprensione o conoscenza.

Ad esempio, una macchina per la traduzione di parole non ha idea del significato delle parole; applica semplicemente regole sintattiche e semantiche determinate in precedenza. Questa situazione solleva anche questioni fondamentali sulla natura dell'intelligenza e sulla differenza tra essere in grado di fare qualcosa ed essere in grado di comprenderla effettivamente. I limiti dell'IA sono chiari: non è creativa, non può rispondere in modo appropriato a circostanze imprevedute e non può comprendere il contesto. Questi dispositivi hanno una rigidità e una specializzazione che impediscono loro di apprendere dall'esperienza o di funzionare al di fuori dei parametri specifici per cui sono stati programmati. L'IA, nonostante tutti questi limiti, serve da modello di base per il futuro e dimostra che le macchine possono essere utilizzate per svolgere operazioni in modo autonomo, liberando così gli esseri umani da lavori ripetitivi e noiosi.

L'IA rappresenta un enorme passo avanti rispetto all'automazione, grazie alla replicazione di capacità intellettuali umane di alto livello come l'apprendimento, il ragionamento, la comprensione del linguaggio. Sviluppata formalmente a metà del XX secolo, la disciplina ha registrato una crescita senza precedenti a un ritmo accelerato, partendo da sistemi basati su regole e progredendo verso modelli in grado di apprendere automaticamente dai dati.

Un principio fondamentale dell'IA è il test di Turing, concettualizzato da Alan Turing, il pioniere della computazione, nel 1950. Questa misura valuta se una macchina può emulare il comportamento cognitivo in modo tale da produrre risposte indistinguibili da quelle di un essere umano. In altri termini, se un valutatore umano non è in grado di discernere una differenza tra le risposte di una macchina e quelle di un essere umano durante un'interazione di domande e risposte, si può concludere che la macchina possiede capacità umane.

Come test di intelligenza, il Test di Turing, come lo descrive McMullin, non affronta a sufficienza la questione della reale comprensione o coscienza di una macchina, replicando così le problematiche dell'argomento della "Stanza Cinese" di Searle, volta a dimostrare in modo conclusivo che è impossibile che una macchina digitale possa comprendere il linguaggio o pensare.

L'argomento si concentra in particolare sulla capacità di una macchina di superare il Test di Turing senza possedere un'effettiva "comprensione" di ciò che sta eseguendo, ma semplicemente eseguendo la manipolazione di simboli entro regole specifiche.

McMullin parla di alcune ipotesi di IA, che concordano con la varietà di soluzioni ai problemi posti da questa disciplina:

- H_P (fisicalismo): Sostiene che qualsiasi evento o stato mentale può, in linea di principio, essere completamente riducibile a eventi e stati fisici, senza alcuna eccezione; i processi cognitivi sono intesi come un epifenomeno dell'encefalo.
- H_C (computazionalismo): tutti gli stati e gli eventi mentali possono essere ridotti, in linea di principio, completamente e senza residui, a stati ed eventi di una macchina di calcolo universale; l'attività neurale è di natura computazionale ed i calcoli neurali, sulla base di un insieme di regole di calcolo (algoritmo), sono alla base della cognizione.
- H_T (Computational Turing Test): il test di Turing viene superato da alcuni sistemi con presunti eventi e stati mentali e da un computer di uso generale.

Questi presupposti contribuiscono efficacemente alla ricchezza del dibattito sull'IA, che si estende oltre la capacità computazionale in sé per affrontare questioni più basilari riguardanti la mente e la sua coscienza. Le argomentazioni di Searle, e le critiche meno specifiche al computazionalismo,

hanno spinto la ricerca verso aree che mirano ad andare oltre l'elaborazione simbolica, esplorando invece meccanismi di apprendimento e flessibilità.

L'evoluzione dei metodi di IA ha visto una crescente tendenza ad abbandonare i sistemi indipendenti dai dati e basati su regole (tipici dell'IM e dei primi sistemi esperti) per passare a sistemi basati sull'apprendimento.

Negli anni '60 Giulio Maccacaro, pioniere dell'informatica medica e cibernetica, come visto, intuendo questa direzione, concettualizzava due approcci generali alla progettazione di macchine intelligenti:

- Reti modulari: reti che modificano autonomamente e gradualmente la propria struttura interna in seguito all'apprendimento ricevuto tramite l'esposizione a forme successive correttamente classificate. È una previsione del moderno apprendimento automatico e delle reti neurali, in cui la macchina impara a identificare schemi e prendere decisioni sulla base di una grande quantità di dati, ma senza essere programmata specificamente per ogni singolo caso.
- Reti statistiche: un piano meno ambizioso, ma più praticabile, che calcolava statisticamente l'importanza relativa delle caratteristiche formali, stimando la probabilità che ciascuna di esse o gruppi di esse comparissero nelle forme classificate. Questo approccio, pur non essendo avanzato quanto le reti modulari, rappresenta un'evoluzione significativa nella diagnosi e nella classificazione automatica, poiché riduce gli errori mediante l'analisi probabilistica dei dati.

Maccacaro predisse l'importanza dell'apprendimento automatico in un'epoca in cui la potenza di calcolo era limitata e i dati scarsi e disaggregati, così contribuendo a gettare le basi per lo sviluppo di sistemi intelligenti alla base del "data science".

Il passaggio da una forma meccanica di intelligenza, in cui predominano istruzioni predeterminate, a un'IA capace di crescita e apprendimento ha aperto opportunità prima inimmaginabili, trasformando non solo i contesti tecnologici, ma anche le interazioni con essi. L'IA è diventata più di un semplice strumento, evolvendosi in qualcosa in grado di apprendere e interagire con l'ambiente in modo più complesso e autodeterminato.

L'impatto dell'IA sul lavoro

Frutto dell'evoluzione dell'automazione di attività manuali e ripetitive, l'IA sfrutta la capacità computazionale emulando quelle cognitive, portando a una trasformazione senza precedenti del mercato del lavoro, ridefinendo ruoli, competenze e la natura stessa delle attività produttive.

Un aspetto cruciale di questa metamorfosi riguarda il passaggio da un'economia radicata nella produzione di beni materiali a un'economia caratterizzata dal "capitalismo immateriale", in cui conoscenza, informazione e servizi sono centrali. Cini richiama l'attenzione sul fatto che il lavoro, precedentemente frammentato e divisibile quantitativamente secondo i principi fordisti e tayloristi, viene riorganizzato in formazioni in cui l'elemento individuale qualitativamente indispensabile non può essere quantificato. In questo nuovo paradigma, la produzione di "beni immateriali" e, di conseguenza, il primato della conoscenza come "bene comune" assume una posizione centrale. La conoscenza, a differenza dei beni materiali, non diminuisce con l'uso, ma viene aumentata e trasmessa, innescando così un "ciclo cognitivo" che alimenta l'industria fondata sulla creazione di significato.

Questa trasformazione richiede un cambiamento radicale nel set di competenze necessarie. I compiti ripetitivi e prevedibili, sia mentali che fisici, stanno diventando sempre più soggetti all'automazione. Il mercato del lavoro richiede quindi più professionisti dotati di capacità di *problem solving*, pensiero critico, creatività, intelligenza emotiva e competenze sociali.

Invece di sostituire completamente i lavoratori umani, l'IA dovrà coadiuvarli nello svolgimento dei compiti più banali, liberando così gli esseri umani affinché possano dedicarsi a qualcosa che aggiunga più valore, qualcosa che richieda intuizione e giudizio.

L'evoluzione degli approcci all'IA ha visto un progressivo spostamento dai sistemi basati su regole



esplicitate a modelli che apprendono dai dati, come appare altamente rappresentativo nel settore medico e come concettualizzato da Maccacaro con la necessità di introdurre "metodi moderni di calcolo ed elaborazione" nella pratica della medicina preventiva. Il volume di dati medici da elaborare, convertire e archiviare ha reso inevitabile l'introduzione di sistemi computerizzati. L'IA aiuterà sempre di più i medici a diagnosticare malattie, interpretare immagini diagnostiche, accelerare la scoperta di farmaci e personalizzare il piano di trattamento per casi specifici, migliorando così l'efficienza e l'accuratezza dell'assistenza ai pazienti. Ma il ruolo del medico non può essere sostituito dall'IA nell'empatia, nel processo decisionale clinico articolato e nell'instaurare relazioni significative con i pazienti.

Il futuro del lavoro nell'era dell'IA è complesso e impegnativo. Sebbene l'automazione eliminerà posti di lavoro in alcuni settori, ne creerà anche altri e darà vita a nuove professioni.

L'aggiornamento e la riqualificazione professionale diventano sempre più necessari per i lavoratori. Queste sfide devono essere affrontate attraverso politiche pubbliche e strategie aziendali, stimolando l'istruzione e la formazione per preparare la forza lavoro al cambiamento in atto.

L'obiettivo non è semplicemente quello di adattarsi all'IA, ma di sfruttarne il potenziale per creare un futuro del lavoro più produttivo, equo e migliore.

Gli sviluppi tecnici che hanno portato alle attuali forme di IA

La linguistica delle macchine o, meglio, l'elaborazione del linguaggio naturale (Natural Language Processing, NLP), è una delle colonne portanti dell'IA, poiché consente alle macchine di comunicare in termini più complessi, utilizzando il linguaggio umano.

Il XX secolo ha visto una grande "svolta linguistica", un paradigma che ha enfatizzato il linguaggio in vari campi, dalla filosofia alla scienza. Questa transizione ha visto il linguaggio non più come un semplice canale di comunicazione, ma come una forma fondamentale per la nostra comprensione del mondo e la nostra capacità di elaborare le informazioni. Cini scrive che la conoscenza del linguaggio e delle sue strutture sintattiche è stata essenziale per lo sviluppo dell'IA. Il paragone con la scoperta del linguaggio del DNA, che ha reso possibile il Progetto Genoma, supporta l'idea che la capacità di interpretare e scomporre strutture complesse sia al centro dello sviluppo dell'IA.

Nel corso degli anni, la programmazione neuro linguistica (PNL) ha attraversato diverse fasi, partendo da approcci iniziali come la Content Analysis, focalizzati sul recupero di informazioni dai testi, fino ai più recenti e potenti Large Language Models (LLM)¹¹.

Gli LLM, come la traduzione automatica e la tecnologia degli assistenti virtuali, sono in grado di creare testi coerenti e contestualmente appropriati, rispondere a domande, riassumere report e persino creare testi originali.

I loro successi si basano sulla capacità di riconoscere deboli schemi e correlazioni statistiche in enormi volumi di dati testuali. Questa capacità è stata possibile grazie alle crescenti capacità di calcolo dei moderni processori elettronici e, soprattutto, all'immenso database di informazioni diffuso via Internet, una risorsa inestimabile rispetto a quelle precedenti.

La linguistica automatica, tuttavia, non si limita all'elaborazione del testo, ma comprende anche la comprensione del significato, la risoluzione del contesto e la formulazione di risposte contestualmente pertinenti. Si tratta di un'interazione uomo-macchina più simile a quella umana rispetto alla semplice immissione di comandi. L'IA, dotata di capacità di elaborazione del linguaggio naturale, viene progressivamente riconosciuta come un assistente di conversazione, un estrattore di informazioni e un generatore di contenuti. La "culturomica", ad esempio, è un approccio di lessicografia computazionale che trae spunto dall'iniziativa Google Libri e dal visualizzatore N-Gram, illustrando come l'elaborazione computazionale di enormi quantità di testi possa essere utilizzata per stabilire tendenze culturali e linguistiche, dimostrando così la confluenza tra scienze umane e scienze naturali. La rilevanza della linguistica automatica continuerà a crescere ulteriormente nei prossimi anni con la continua espansione dell'IA.

La capacità delle macchine di comprendere e generare un linguaggio naturale è fondamentale per lo sviluppo di interfacce sempre più utilizzabili, per l'automazione di processi come la scansione di enormi quantità di testo (ad esempio nella revisione legale o nell'analisi di resoconti finanziari) e per lo sviluppo di sistemi intelligenti che interagiscono con il mondo in modi più simili a quelli umani.

Le sfide future includono l'evitare sottigliezze linguistiche, ironia, sarcasmo ed espressioni idiomatiche, che richiedono una conoscenza approfondita dell'ambiente sociale e culturale.

Conclusioni

“se ogni strumento riuscisse a compiere le sue funzioni o dietro un comando o prevedendolo in anticipo [...] così anche le spole tessessero da sè e i plettri toccassero la cetra, i capi artigiani non avrebbero davvero bisogno di subordinati, nè i padri di schiavi”
(Aristotele, Politica, Libro I)

Aristotele, nel IV secolo a.C. fu tra i primi a tentare di formalizzare il pensiero umano attraverso la logica deduttiva ovvero che il ragionamento può essere espresso come un sistema di regole formali. Le sue opere rappresentano il primo tentativo sistematico di definire regole del pensiero corretto, un'idea fondamentale che avrebbe ispirato nei secoli lo sviluppo delle macchine intelligenti.

Dopo i secoli bui, nel corso del Rinascimento e dell'Illuminismo, l'interesse per le macchine capaci di simulare il comportamento umano crebbe enormemente. Scienziati e filosofi, come Pascal prima¹²

¹¹ Nel campo del riconoscimento delle immagini, oggetto di attenzione da parte di Maccacaro nel periodo descritto sopra, si parla di LIM-Large Images Models che stanno trovando importanti applicazioni attraverso l'uso dei droni per esplorare il terreno e le costruzioni, ma anche, purtroppo, negli scenari di guerra attuali.

¹² Pascal, B. (1645). Lettre dédicatoire à Monseigneur le Chancelier.

e Leibniz poi¹³, svilupparono calcolatori meccanici, quest'ultimo definendo la sua *Machina Arithmetica* come "*Supra Hominem*" ovvero superiore all'uomo, suggerendo come grazie all'utilizzo di una macchina, anche una mente non particolarmente dotata potrebbe ottenere i risultati corretti; altri, come Descartes¹⁴, speculavano sul fatto che anche il pensiero umano potesse essere ridotto a procedimenti meccanici, pur definendo l'essere umano come una macchina divina. Il vero punto di svolta avviene nel XX secolo, quando la logica formale incontra la computazione, anche grazie a menti quali Alan Turing che, introducendo il suo gioco dell'imitazione (meglio noto come "macchina di Turing"), modello teorico di un calcolatore universale, pose le basi per pensare al cervello come un sistema computazionale. Claude Shannon, qualche anno dopo, sviluppò la teoria dell'informazione, dimostrando come la logica proposizionale o booleana possa essere realizzata con circuiti elettrici, possibile grazie a Norbert Wiener, padre della cibernetica, ovvero dello studio dei sistemi autoregolanti, fondamentali per il controllo e l'adattamento nelle macchine.

Nel 1956, durante la conferenza di Dartmouth, nasce ufficialmente il campo dell'intelligenza artificiale. I pionieri (McCarthy, Minsky, Simon, Newell, Shannon) erano ottimisti: credevano che in pochi anni avrebbero risolto il problema dell'intelligenza artificiale generale. Al primo impulso, anche per limiti della tecnologia dell'epoca, è seguito il c.d. primo inverno della IA negli anni '70-'80. Gli anni successivi, inoltre, sono stati caratterizzati da periodi di entusiasmo e delusioni circa lo sviluppo della IA.

L'evoluzione non è stata lineare, ma piuttosto segnata da innovazioni, dibattiti filosofici e progressi tecnici che hanno trasformato il modo in cui interagiamo con la tecnologia e la nostra percezione di noi stessi. L'IM, che enfatizzava l'automazione e la riproducibilità, svolse un ruolo fondamentale negli sviluppi del lavoro all'inizio del secolo XX, specie in campo industriale, liberando gli individui da compiti banali e migliorando la produttività in modo straordinario. Tuttavia, i suoi limiti intrinseci, basati sull'incapacità di comprendere e apprendere, hanno stimolato la ricerca di nuove frontiere. L'avvento dell'IA ha innescato una rivoluzione straordinaria, rendendo possibile apprendere dall'esperienza, ragionare e comunicare in modo progressivamente naturale.

La controversia sul computazionalismo, insieme a critiche come l'obiezione della "stanza cinese" di Searle, ha evidenziato la difficoltà di misurare e definire l'intelligenza nei sistemi artificiali. Ciò ha incoraggiato gli sforzi verso lo sviluppo di approcci più avanzati, tra cui l'apprendimento automatico.

Le implicazioni per il mondo del lavoro sono state profonde. Questo passaggio dal capitalismo materiale a quello immateriale, in cui conoscenza e informazione sono le nuove valute, sta ridefinendo le competenze del lavoro e le funzioni lavorative.

L'automazione tramite IA sta liberando gli esseri umani da compiti ripetitivi, ma richiede un continuo aggiornamento e sviluppo di competenze individuali come la creatività, il pensiero analitico e l'intelligenza emotiva. La medicina, come abbiamo visto, è un ottimo esempio di come l'IA possa assistere e potenziare la pratica umana, senza mai sostituirla completamente. Infine, la linguistica delle macchine con l'elaborazione del linguaggio naturale (NLP) e i Large Language Models (LLM) è diventata un elemento determinante nel dialogo uomo-macchina. La capacità delle macchine di interpretare e riprodurre il linguaggio naturale ha aperto nuove possibilità per la comunicazione, il recupero delle informazioni e la creazione di contenuti. La "svolta linguistica" del XX secolo ha effettivamente reso possibile questo progresso, dimostrando che l'interpretazione del linguaggio ha l'importanza di sviluppare sistemi di IA più sofisticati e unificati nelle nostre vite.

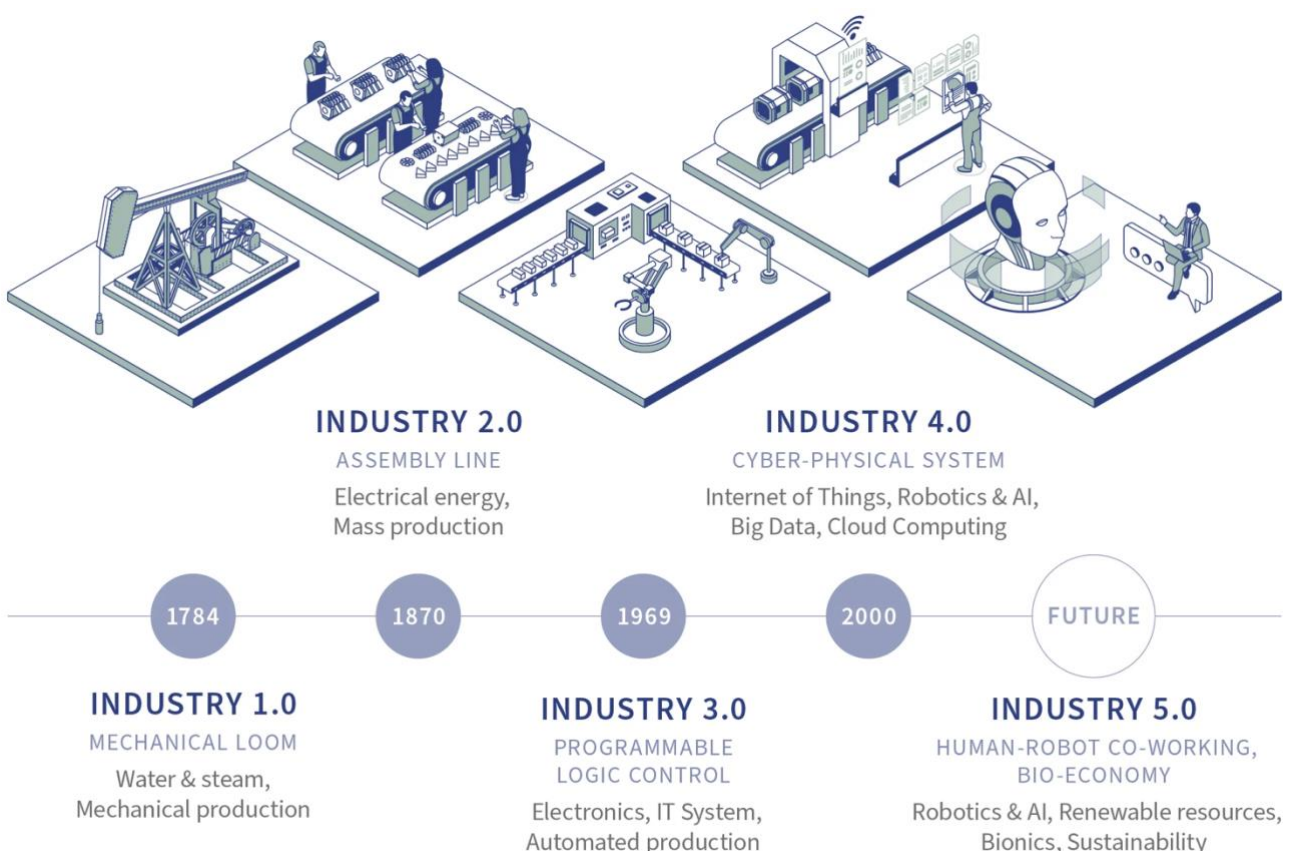
¹³ Morar F-S. Reinventing machines: the transmission history of the Leibniz calculator. *The British Journal for the History of Science*. 2015;48(1):123-146. doi:10.1017/S0007087414000429

¹⁴ Descartes, R. (1664, postumo). *L'homme*.

Infine, ma non meno importante, il salto definitivo dall'IM all'IA è ancora lontano. Siamo solo all'inizio di un'era in cui le macchine diventeranno più intelligenti, autonome e capaci di percepire il mondo in modo complesso. Le sfide future non riguardano solo il progresso tecnologico, ma anche il controllo etico e sociale di queste tecnologie emergenti. La governance è necessaria per garantire che l'IA funzioni come uno strumento a beneficio degli esseri umani, contribuendo a migliorare la qualità della vita e a risolvere alcuni dei maggiori problemi globali.

Con l'avvento di modelli sempre più potenti (reti neurali profonde, transformer), l'IA ha compiuto progressi straordinari, superando gli umani in vari compiti specifici (visione artificiale, linguaggio, giochi strategici), sebbene l'efficienza non equivalga alla comprensione dei valori umani. Le IA moderne ottimizzano funzioni di obiettivo senza una vera comprensione del contesto o delle conseguenze etiche delle loro azioni, richiamando l'importanza di una progettazione attenta a tali aspetti

“se per raggiungere i nostri scopi usiamo un ente meccanico senza poter interferire efficacemente con il suo funzionamento [...] sarebbe meglio essere assolutamente certi che lo scopo immesso nella macchina sia lo scopo che desideriamo davvero”¹⁵



¹⁵ Wiener N. Some Moral and Technical Consequences of Automation. Science. 1960 May 6;131(3410):1355-8. doi: 10.1126/science.131.3410.1355

1.2 L'impatto dell'Intelligenza Artificiale sulla salute e la sicurezza al lavoro: principali indicazioni dell'Agenzia Europea EU-OSHA

Agenzia Europea per la Salute e la Sicurezza sul Lavoro (EU-OSHA). Documento di sintesi "Impact of artificial intelligence on occupational safety and health until the year 2025"

1.2.1 Applicazioni dell'intelligenza artificiale negli ambienti di lavoro

L'intelligenza artificiale (IA) ha il potenziale di permettere sviluppi innovativi ed estremamente interessanti negli ambienti di lavoro, attraverso l'aumento della disponibilità dei dati e dei big data e la capacità di elaborarli per mezzo di algoritmi, determinando cambiamenti profondi e su vasta scala nelle modalità lavorative. L'IA viene impiegata in un'ampia gamma di applicazioni e strumenti per il lavoro assistito e l'analisi dei dati, consentendo l'automazione di compiti sempre più complessi nonché la gestione e il processo decisionale automatizzati o semi-automatizzati sul luogo di lavoro. Le applicazioni dell'IA nei processi di lavoro sono svariate: cobot¹⁶, tecnologie indossabili e tablet di assistenza lungo la catena di montaggio della produzione, chatbot nelle fabbriche, nei magazzini e nei call center, dispositivi di protezione individuale intelligenti, processi algoritmici nelle applicazioni per risorse umane come la «people analytics»¹⁷ e la «gamificazione»¹⁸. L'IA potrebbe creare delle opportunità ma anche sollevare nuove problematiche per la salute e la sicurezza sul lavoro (SSL), la sua gestione e la sua regolamentazione. Il dibattito sull'IA verte per la maggior parte sul numero dei posti di lavoro, ma dovrebbe anche riguardare la qualità degli stessi. In tal senso, la SSL è un aspetto fondamentale.

1.2.2 L'IA nell'automazione dei compiti e nella SSL

I robot che integrano l'IA stanno diventando mobili, intelligenti e collaborativi. Il loro utilizzo evita ai lavoratori di trovarsi in situazioni pericolose e migliora la qualità del lavoro affidando compiti ripetitivi a macchine veloci, accurate e instancabili. I cobot possono inoltre agevolare l'inserimento in un posto di lavoro a molte persone (lavoratori anziani o con disabilità) e collaborano con i colleghi umani in un'area di lavoro condivisa.

Tuttavia, l'aumento della mobilità dei cobot e della loro autonomia decisionale, basata su algoritmi di autoapprendimento, potrebbero renderne meno prevedibili le operazioni per chi collabora con tali macchine; ciò potrebbe comportare un maggior rischio di incidenti provocati da collisioni o dai dispositivi utilizzati dagli stessi cobot. L'eccessivo affidamento alla tecnologia potrebbe altresì causare una dequalificazione e rischi per la sicurezza; il fatto che i cobot siano collegati all'Internet delle cose può essere causa di problemi di sicurezza informatica e di rischi associati alla sicurezza funzionale. I dipendenti che devono adeguarsi al ritmo e al livello di lavoro di un cobot potrebbero essere messi sotto pressione per raggiungere lo stesso grado di produttività. L'aumento del lavoro con i robot potrebbe inoltre ridurre sensibilmente il contatto con i colleghi umani e il sostegno derivante dai contatti sociali, con possibili effetti negativi per la sicurezza e la salute dei lavoratori, in particolare quella mentale.

Oggi, con la crescente diffusione dell'IA, i sistemi automatizzati sono in grado di svolgere non solo compiti fisici, ma anche una serie di compiti cognitivi, quali la guida autonoma o l'assistenza, per

¹⁶ Un cobot o co-robot (robot collaborativo) è un robot concepito per interagire fisicamente (e socialmente) con le persone in un ambiente di lavoro condiviso. Cfr. Jansen, A. et al., 2018, *Emergent risks to workplace safety; working in the same space as a cobot*, TNO Report R10742.

¹⁷ L'uso di big data e strumenti digitali per «misurare, registrare e comprendere le prestazioni dei dipendenti, gli aspetti inerenti alla pianificazione della forza lavoro, la gestione dei talenti e la gestione operativa». Cfr. Collins, L. et al., 2017, *People analytics: recalculating the route*, Deloitte Insights.

¹⁸ L'uso delle meccaniche di gioco e del «game thinking» per coinvolgere i lavoratori.

esempio, in campo legale o nelle diagnosi mediche. L'utilizzo di sistemi basati sull'IA è dunque previsto in molti ambienti e settori diversi, da quello manifatturiero e agricolo a quello assistenziale e alberghiero, nei trasporti e nei servizi, ivi compresi i lavori a contatto con la clientela. Poiché il contenuto di questi lavori e dei compiti da svolgere è destinato a cambiare nel tempo, potrebbero sorgere nuovi problemi nell'ambito della SSL.

Per esempio, l'automazione dei compiti può essere associata a un lavoro maggiormente sedentario e a una minore varietà delle mansioni, lasciando ai dipendenti i lavori ripetitivi. Tale automazione rischia di generare noia e un carico insufficiente di lavoro cognitivo, pressione psicologica relativamente al proprio rendimento e intensificazione dei ritmi di lavoro, oltre a determinati fattori di rischio, quali l'isolamento e una scarsa interazione con i colleghi; inoltre, può incidere negativamente sul lavoro di squadra – tutti rischi psicosociali noti.

1.2.3 Il ricorso all'IA a fini di gestione e di monitoraggio dei lavoratori

L'IA ha anche favorito l'emergere di nuove forme di monitoraggio e di gestione dei lavoratori: le tecnologie digitali che ne fanno uso permettono infatti di attuare modalità di controllo e gestione dei dipendenti nuove, diffuse, costanti e a basso costo, in virtù dell'acquisizione in tempo reale di grandi quantità di dati sui lavoratori. Questi dati possono essere raccolti durante e al di fuori dell'orario lavorativo e in diversi ambienti di lavoro, nonché al di fuori di essi e, talvolta, al di là dello stretto necessario o di ciò che è legalmente consentito.

Si possono acquisire dati sui lavoratori attraverso dispositivi mobili o dispositivi di monitoraggio indossabili o integrati (negli abiti, nei dispositivi di protezione individuale o persino a contatto col corpo). Tali dati includono i clic della tastiera, il contenuto delle e-mail, i siti web visitati, il numero e il contenuto delle telefonate, le informazioni acquisite dai social media, i luoghi individuati tramite il rilevamento GPS, i movimenti corporei, i segni vitali, gli indicatori di stress e affaticamento, le espressioni microfacciali, il tono di voce e la «sentiment analysis».

I dati raccolti vengono utilizzati per informare la dirigenza e prendere decisioni automatizzate e semi-automatizzate basate su algoritmi o su forme più avanzate di IA, in modo da consentire ai datori di lavoro di esercitare un maggiore controllo sui dipendenti e sul luogo di lavoro, integrare sistemi di classificazione o altri parametri nella valutazione delle prestazioni, migliorare queste ultime e la produttività dei dipendenti, razionalizzare l'organizzazione del lavoro e la produzione, ridurre i costi di monitoraggio e di sorveglianza, tracciare il profilo dei lavoratori, influenzarne e regolamentarne il comportamento o migliorare la gestione delle risorse umane. In tale contesto emergono nuovi campi come la «people analytics» e la gamificazione.

Queste nuove forme di monitoraggio e gestione dei lavoratori possono dare adito a problemi giuridici, normativi ed etici, nonché a preoccupazioni per quanto riguarda la SSL e, in particolare, la salute mentale dei lavoratori. Possono infatti causare la perdita di controllo dei dipendenti sul loro lavoro e fare aumentare la microgestione, la pressione psicologica relativamente al proprio rendimento, la competitività, l'individualizzazione e l'isolamento sociale. I lavoratori potrebbero avere l'impressione che la loro privacy venga violata, cosa che rappresenta anche una fonte di ansia e stress, oltre a non avere la possibilità di fare una pausa quando ne hanno bisogno, con il rischio di incidenti e problemi di salute come disturbi muscoloscheletrici e malattie cardiovascolari.

Orari di lavoro instabili, come quelli a breve termine definiti automaticamente da algoritmi, hanno svariati impatti negativi sui dipendenti, tra cui l'intensificarsi del conflitto tra lavoro e vita familiare, lo stress sul lavoro e l'incertezza del reddito. L'uso dei dati dei lavoratori per premiarli o penalizzarli potrebbe provocare stress e precarietà occupazionale e, poiché le componenti operative principali delle forme di gestione dei dipendenti basate sull'IA comprendono spesso una «scatola nera», è possibile che i lavoratori e i loro rappresentanti non abbiano informazioni né potere sulle strategie e sulle decisioni adottate.

1.2.4 Un'opportunità per migliorare la sicurezza e la salute dei lavoratori

Nuove forme di monitoraggio dei dipendenti basate sull'IA potrebbero offrire l'opportunità di migliorare la sorveglianza della SSL, ridurre l'esposizione a vari fattori di rischio, tra cui molestie e violenze, e fornire segnalazioni tempestive di stress, problemi di salute e affaticamento. Consulenze personalizzate in tempo reale possono incidere sul comportamento dei lavoratori e migliorare sicurezza e salute. Il monitoraggio basato sull'IA potrebbe promuovere la prevenzione fondata su dati concreti, una valutazione avanzata dei rischi negli ambienti di lavoro e ispezioni in materia di SSL mirate, più efficienti e basate sui rischi. Le organizzazioni potrebbero utilizzare le informazioni per individuare eventuali problemi a livello di SSL, rischi psicosociali inclusi, e la necessità di interventi in tale ambito a livello organizzativo.

Tuttavia, sono necessarie decisioni etiche nonché strategie e sistemi efficaci per gestire la grande quantità di dati personali sensibili che è possibile generare. Disposizioni giuridiche adeguate che conferiscano agli organi di vigilanza l'accesso a dati anonimizzati potrebbero consentire di elaborare misure di prevenzione e politiche basate su dati concreti. L'esigenza di acquisire dati sui lavoratori dovrebbe essere controbilanciata dal loro diritto alla privacy, alla salute e alla sicurezza. È importante garantire la trasparenza nella raccolta e nell'utilizzo di tali dati e si dovrebbero mettere i dipendenti e i loro rappresentanti nella condizione di avere lo stesso accesso alle informazioni.



Riferimenti

- (cfr. <https://osha.europa.eu/en/emerging-risks/developments-ict-and-digitalisation-work>)
- in particolare: EU-OSHA, 2018, *Prospettive in merito ai rischi nuovi ed emergenti in materia di salute e sicurezza sul lavoro correlati alla digitalizzazione nel periodo fino al 2025*
- (<https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated/view>);
- EU-OSHA, 2019, *L'SSL e il futuro del lavoro: vantaggi e rischi degli strumenti di intelligenza artificiale negli ambienti di lavoro*
- (<https://osha.europa.eu/en/publications/osh-and-future-work-benefits-and-risks-artificial-intelligence-tools-workplaces/view>);
- EU-OSHA, 2019, *Il futuro ruolo dei big data e dell'apprendimento automatico nell'efficienza delle ispezioni nel settore della salute e della sicurezza*
- <https://osha.europa.eu/en/publications/future-role-big-data-and-machine-learning-health-and-safety-inspection-efficiency/view>);
- EU-OSHA, 2020, *Dispositivi di protezione individuale intelligenti: pensare la tutela del futuro* (<https://osha.europa.eu/en/publications/smart-personal-protective-equipment-intelligent-protection-future/view>).

1.3 Intelligenza artificiale e l'uso nel contesto della salute e sicurezza del lavoro: l'uomo di fronte alla A.I.

Andrea Cirincione

Psicologo del Lavoro, formatore e consulente aziendale; Consigliere nazionale Aifos

Abstract (italiano)

Il saggio esplora in modo ampio e interdisciplinare l'impatto dell'intelligenza artificiale sul mondo del lavoro, con particolare attenzione al tema della sicurezza. A partire da una ricognizione storica sul rapporto tra uomo e tecnologia, si indagano le sfide emergenti poste dall'adozione dell'IA in ambiti produttivi, organizzativi e cognitivi: dalla coabitazione con macchine autonome alla trasformazione delle competenze, dalla sorveglianza digitale ai nuovi rischi psicosociali. Il testo integra riflessioni filosofiche, normative (AI Act, GDPR, diritto del lavoro), culturali e organizzative, evidenziando sia i pericoli legati all'opacità decisionale e alla disumanizzazione, sia le opportunità per migliorare benessere, equità e prevenzione. Con uno sguardo comparativo internazionale, vengono presentati modelli alternativi di governance tecnologica e scenari di coevoluzione responsabile. Il lavoro emerge così come crocevia tra etica, intelligenza collettiva e progettazione partecipata, in una visione che non contrappone umano e artificiale, ma li armonizza in una nuova alleanza fondata su responsabilità condivisa, consapevolezza critica e desiderio di futuro.

1.3.1 Introduzione storica e scenario attuale

La paura che le macchine possano “rubare il lavoro” non nasce con l'intelligenza artificiale. Già all'inizio del XIX secolo, in Inghilterra, nacque il movimento dei luddisti, operai e artigiani tessili che distruggevano i telai meccanici introdotti nelle fabbriche, ritenendoli responsabili della perdita del lavoro e del crollo dei salari. Il nome deriva da *Ned Ludd*, una figura leggendaria che si dice avesse distrutto un telaio per protesta: la sua storia divenne simbolo e bandiera di una ribellione diffusa.

La protesta contro un uso della tecnologia che accentua le disuguaglianze e ignora i diritti dei lavoratori è una dinamica ricorrente: ogni rivoluzione industriale ha portato con sé lo spettro della disoccupazione tecnologica, ma anche l'opportunità – se ben governata – di ridefinire competenze, tutele e giustizia sociale. L'intelligenza artificiale si inserisce in questa traiettoria con una peculiarità: non tocca solo il “fare”, ma anche il “decidere”. Non solo per svolgere compiti fisici o meccanici, ma come partner cognitivo. E qui la posta si alza.

La riflessione sulla sicurezza e sul lavoro nell'epoca dell'IA ci interroga non solo su “cosa fa la macchina”, ma su “cosa fa fare all'uomo”. E, soprattutto, su chi decide le regole di questa interazione. Perché ogni tecnologia, come scriveva il sociologo Langdon Winner, è sempre anche una forma di ordine politico. Secondo l'OCSE (2023), il 27% dei lavori in paesi avanzati è ad alto rischio di automazione entro il 2030, ma l'IA creerà 97 milioni di nuovi ruoli (*World Economic Forum, 2023*). Bisogna governare una transizione che ridefinisce potere, dignità e identità.

Se la macchina a vapore ha potenziato il muscolo umano, l'IA insidia direttamente le funzioni mentali. Non solo esegue, ma decide, predice, talvolta “consiglia” soluzioni. A prima vista, sembra una liberazione. Ma a un'analisi più attenta, emerge il bisogno di ridefinire le responsabilità, i confini, i linguaggi. Il rischio è una “opacità algoritmica” e una conseguente responsabilità evanescente.

Esemplare il caso di SyRI (System Risk Indication), un sistema algoritmico progettato per individuare potenziali frodi nei sussidi sociali. Criticato per la sua discriminazione nei confronti di gruppi vulnerabili. Nel 2020, un tribunale olandese ha stabilito che SyRI violava i diritti umani, portando alla sua abolizione. Questo caso ha sollevato importanti questioni etiche sull'uso degli algoritmi nei

servizi pubblici. Chi risponde? Ci prepariamo a nuove *checklist* aziendali, per mappare le fonti dati e verificare i bias, designare un “Responsabile Etico dell’IA” interno, fare audit semestrali con partecipazione sindacale.

Il filosofo Hans Jonas ci metteva in guardia sul fatto che ogni potere tecnico implica una nuova etica della responsabilità. Pensiamo a un sistema di IA che, basandosi su un’enorme mole di dati storici, decide di reindirizzare le turnazioni in una fabbrica per “massimizzare l’efficienza”. Se la variabile efficienza è calcolata solo sulla base della produttività e non considera la salute psicofisica dei lavoratori, potremmo trovarci davanti a un sistema tanto intelligente quanto pericolosamente miope.

In questo scenario, la relazione uomo-macchina non è più lineare. Non è un semplice utilizzo di strumenti, ma un’interazione reciproca e complessa, un “intreccio” cognitivo profondo dove l’umano si affida alla macchina per alcune scelte e la macchina, a sua volta, si addestra sul comportamento umano. Una spirale che richiede regole nuove, sguardi critici e molta vigilanza.

Sintesi- L’IA non è una rivoluzione inedita, ma l’ennesima curva di una lunga danza tra speranza e timore, dove il lavoro diventa campo di battaglia tra dignità e disuguaglianza. L’interazione con l’IA svela ambiguità irrisolte: decisioni opache, responsabilità diffuse, algoritmi che apprendono i nostri errori e li restituiscono in forma automatizzata

1.3.2 Privacy e sorveglianza algoritmica

Nel 2025 si stima che il 40% delle ore lavorative sarà toccato in qualche modo da forme di automazione intelligente. Questo dato, tratto da un rapporto del *World Economic Forum*, mostra come l’IA non sia più confinata ai romanzi di fantascienza. In fabbrica, l’adozione di cobot (robot collaborativi) riduce drasticamente gli incidenti legati a compiti ripetitivi o ad alta usura. Questi dispositivi sono capaci di percepire la presenza del lavoratore umano e adattarsi dinamicamente alla sua azione. Eppure, anche in questi ambienti apparentemente sicuri, emergono nuove sfide: come reagisce il sistema in caso di errore sensoriale? Quali sono i protocolli quando la comunicazione tra umano e robot si interrompe?

Il problema si acuisce negli ambienti d’ufficio. Qui, i software di IA si occupano di valutazioni delle performance, di suggerire promozioni, di filtrare CV. Con quali parametri avvengono queste valutazioni? Gli algoritmi replicano (senza saperlo) i bias dei dati su cui sono stati addestrati? Un celebre caso è quello di Amazon, che nel 2017 fu costretta a ritirare un sistema di IA per il recruiting: il software penalizzava i CV femminili perché il training set era stato costruito su anni di assunzioni prevalentemente maschili. La macchina aveva semplicemente “imparato” la cultura esistente.

Ecco perché, nella nuova alleanza tra umano e macchina, non è sufficiente “insegnare bene” all’IA: serve anche una cultura organizzativa che sappia supervisionare, interrogare e – se necessario – disobbedire alla macchina. Ogni tecnologia può facilmente trasformarsi in strumento di controllo e normalizzazione. Lo intuì già alla fine del Settecento Jeremy Bentham, quando concepì il Panopticon, un modello di prigione dove i detenuti, pur non potendo vedere il sorvegliante, si comportavano come se fossero costantemente osservati.

Uno studio britannico (Moore&Piwek, 2019) ha analizzato l’impatto del monitoraggio digitale (es. software di tracciamento dell’attività, analisi delle emoticon nelle e-mail) su lavoratori in contesti ibridi o remoti. Il 62% dei lavoratori intervistati (campione di 400 persone nel Regno Unito) ha riferito ansia legata alla “visibilità costante” delle proprie attività digitali, percepita come una forma di controllo asimmetrico.

Meccanismi identificati: paura di penalizzazioni per "inattività" (es. pause non registrate); stress da ottimizzazione forzata delle metriche di produttività; alienazione dovuta alla riduzione dell'autonomia.

Pertanto, il "Panopticon digitale" non è solo controllo, ma normalizzazione: l'algoritmo definisce cosa è "efficiente", influenzando la percezione del sé. Persino i nostri dispositivi ci notificano suggerimenti per dormire di più, camminare di più, lavorare meglio. Il confine tra aiuto e intrusione è sottile. Anche nei luoghi di lavoro l'IA può trasformarsi da assistente a sorvegliante invisibile.

Questo confine è ogni giorno più fragile. I sistemi di IA possono analizzare l'uso del computer, la velocità di digitazione, il tono delle e-mail. Possono stabilire se un dipendente è stanco, stressato o poco produttivo. Possono anche, potenzialmente, inviare segnalazioni automatiche ai superiori. Che fine faranno libertà, dignità e fiducia? Il lavoratore è interpretato ma non si sa con quale neutralità.

Fortunatamente, alcune aziende stanno scegliendo strade più etiche e trasparenti: garantiscono l'anonimato dei dati raccolti e chiedono il consenso esplicito dei lavoratori ("opt-in"). Altre sembrano concentrate sull'estrazione del massimo rendimento di ogni comportamento. Il risultato? Un ambiente lavorativo dominato dal sospetto, dall'ansia e da un progressivo distacco psicologico tra persone e organizzazione. Serve allora un equilibrio dinamico tra protezione e rispetto. E serve formazione: perché troppo spesso, la sorveglianza viene introdotta "per il bene di tutti", senza discuterne davvero con chi ne è oggetto.

Sintesi- Dalla linea di montaggio al recruiting digitale, l'IA cambia ambienti e processi, ma porta con sé nuovi rischi: bias, sorveglianza e personalizzazione delle relazioni lavorative. L'IA trasforma la prevenzione in controllo: il Panopticon non ha più torri, ma righe di codice. Il rischio non è solo essere osservato, ma interpretato senza appello.

1.3.3 Formazione continua e nuove competenze

Una delle implicazioni più critiche dell'introduzione massiva dell'IA nei luoghi di lavoro è il rischio di obsolescenza delle competenze. Serve una ridefinizione delle capacità richieste ai lavoratori. Non è più sufficiente conoscere una procedura, bisogna comprendere anche la logica di un algoritmo. E domani? Potrebbe servire la capacità di adattarsi a interfacce cognitive dinamiche, con sistemi sempre meno prevedibili.

Il paradosso è che più un sistema diventa "intelligente", più diventa grigio per chi non ha una formazione adeguata. Ecco perché la formazione deve diventare parte dell'identità professionale di ciascuno. Prendiamo l'ambito sanitario: i software di IA vengono sempre più usati per l'analisi di immagini diagnostiche, per suggerire terapie, per gestire flussi di pazienti. Il rischio per un medico è diventare un mero esecutore, oppure, peggio, prendere decisioni errate basate su fiducia cieca nella tecnologia.

È qui che si parla di "competenza aumentata": la tecnologia va saputa integrare criticamente nella propria pratica. E bisogna saper dire "no", quando un suggerimento algoritmico contrasta con il buon senso clinico. Senza formazione l'IA non valorizza le persone, ma genera alienazione e disagio organizzativo, con maggior esposizione a stress, demotivazione e burnout.

Come ha osservato Albert Bandura, psicologo canadese esperto di apprendimento, "le persone devono percepirsi come efficaci per mantenere motivazione e benessere". Senza una solida auto-efficacia percepita, l'individuo perde il controllo sul proprio ruolo e sull'ambiente, con effetti negativi

anche sulla sicurezza. E senza sicurezza psicologica, non c'è possibilità di sicurezza tecnica o procedurale.

Quando si parla di IA e lavoro ci si lancia nelle competenze tecniche (*hard skills*): programmazione, scienza dei dati, sicurezza informatica (*cybersecurity*). Ma saranno cruciali le competenze trasversali, quelle “umane” che -al momento- caratterizzano l'essere umano. Tra queste, alcune stanno acquisendo particolare rilievo:

- **Pensiero critico:** parlare al sistema, riconoscerne i pregiudizi (*bias*), di essere passivi.
- **Alfabetizzazione digitale:** saper leggere una *dashboard*, capire un *report* di *AI performance*.
- **Empatia e comunicazione:** farsi capire da colleghi, clienti, altri interessati, con l'automazione.
- **Capacità di apprendimento continuo:** rapida trasformazione, aggiornarsi sempre.

La nuova competenza non è “saper usare uno strumento (*tool*)”, ma “saper interagire in modo responsabile con esso”. E la vera differenza la farà chi saprà essere più umano, non meno. Se parliamo di produttività l'IA può aumentare l'efficienza, ma il vero valore sta in qualità del lavoro, creatività, inclusione. Ecco perché è urgente reimmaginare le metriche. Cosa significa “lavorare bene” in un ambiente intelligente? È davvero solo questione di risultato? O possiamo cominciare a valutare anche la soddisfazione, il benessere, l'equità?

In questo senso, l'IA può essere strumento di emancipazione, se orientata a ridurre compiti ripetitivi e alienanti, adattare i ruoli alle capacità individuali (inclusione di persone con disabilità), offrire percorsi di crescita personalizzati, favorire il bilanciamento tra vita lavorativa e personale. Un'IA progettata per valorizzare la persona – e non solo l'impresa – è perfettamente possibile. Ma richiede una progettazione etica, multidisciplinare e lungimirante. Serve un'alleanza tra tecnologi, giuristi, psicologi, ergonomi, filosofi. Serve, in fondo, riscoprire il lavoro non solo come mezzo, ma come spazio di senso.

Sintesi- L'alfabetizzazione algoritmica diventa una nuova forma di cittadinanza professionale: chi non sa dialogare con la macchina rischia di diventare invisibile o marginalizzato. Nel mondo dell'IA, a fare la differenza sarà chi sa restare umano: pensiero critico, empatia, adattabilità diventano le competenze strategiche del lavoro aumentato. L'efficienza non basta: la tecnologia può essere leva di inclusione, benessere e crescita personale, se orientata verso metriche che valorizzino la qualità del vivere.

1.3.4 Etica, diritto e responsabilità diffuse

Già adesso la distribuzione della responsabilità è un esercizio delicato, e quando entra in gioco l'IA, il tema si complica. Chi è responsabile di un errore compiuto da un algoritmo? L'azienda che lo utilizza? Il gruppo di sviluppatori? Il fornitore della piattaforma? Il sistema stesso? Nel diritto attuale, le macchine non hanno personalità giuridica. Tuttavia, le loro decisioni producono effetti concreti, spesso irreversibili.

È il caso, ad esempio, dei sistemi di riconoscimento facciale impiegati in contesti di sicurezza aziendale, che possono “bloccare” un dipendente a causa di un falso positivo. Chi risponde? E come si risarcisce un danno immateriale come la perdita di fiducia o la stigmatizzazione? Il regolamento europeo sull'intelligenza artificiale – l'AI Act – è un primo tentativo di dare una risposta. Classifica i sistemi in base al rischio che comportano e prevede obblighi di trasparenza, supervisione umana e valutazione d'impatto per quelli più critici. Ma il lavoro è solo all'inizio.

Il tema non è che la responsabilità venga “scaricata” sulla macchina, ma condivisa tra tutti gli attori coinvolti: progettisti, datori di lavoro, lavoratori stessi. Questo significa, tra le altre cose, che chi lavora deve avere voce in capitolo sulle tecnologie che lo riguardano. Che i sindacati devono acquisire nuove competenze per negoziare anche sulle piattaforme digitali. Che le organizzazioni devono dotarsi di comitati etici interni in grado di valutare l’impatto delle innovazioni non solo in termini di produttività, ma di equità, dignità e benessere.

La prevenzione oggi si confronta con minacce invisibili: violazioni di dati, manipolazioni informatiche, decisioni automatizzate errate. La sicurezza del lavoro, nell’era dell’IA, è anche sicurezza informatica, psicologica, organizzativa. Si impone un passaggio culturale: dai Dispositivi di Protezione Individuale (DPI) al Data Protection Impact Assessment (DPIA). Quest’ultimo non è un oggetto da indossare, ma un processo da attuare. È una valutazione obbligatoria secondo il GDPR per tutti i trattamenti di dati personali che possono comportare un rischio elevato per i diritti e le libertà delle persone. E nel mondo del lavoro, i dati personali abbondano. Pensiamo a un’azienda che utilizza una piattaforma di IA per tracciare i movimenti dei dipendenti, monitorarne le performance e suggerire bonus o sanzioni. Senza una DPIA, un simile sistema può facilmente sfuggire di mano, generando un ambiente lavorativo distopico, disumanizzato. Con una DPIA fatta bene, invece, si possono identificare i rischi, mitigarli, e magari scoprire che alcune funzioni sono eccessive o inutili.

La prevenzione 4.0 implica anche gli asset digitali, i modelli algoritmici, l’adozione di standard aperti e auditabili. L’innovazione deve procedere in un perimetro di fiducia. Come ha ricordato il filosofo Luciano Floridi, “*non dobbiamo solo chiederci cosa possiamo fare con l’IA, ma anche cosa dovremmo fare*”. Il diritto del lavoro nasce come risposta a un’asimmetria di potere tra datore di lavoro e lavoratore, e con l’IA questa asimmetria si complica. I tradizionali strumenti giuridici (contratti, orari, tutele contro il licenziamento) fanno fatica a intercettare i rischi emergenti.

Il Regolamento Europeo sull’Intelligenza Artificiale (AI Act) tenta di colmare questa lacuna introducendo categorie di rischio e obblighi specifici. Ma resta una normativa ancora distante dalle specificità del lavoro quotidiano. È urgente un aggiornamento del diritto del lavoro che preveda, ad esempio:

- Il diritto alla spiegazione delle decisioni algoritmiche che incidono su carriera, retribuzione o condizioni contrattuali; il diritto a non essere soggetti a processi decisionali completamente automatizzati; la possibilità per i rappresentanti dei lavoratori di partecipare alla valutazione d’impatto delle tecnologie IA; l’obbligo per le aziende di fornire formazione e aggiornamento continuo anche su competenze digitali e algoritmiche.

Sintesi- In un ecosistema decisionale diffuso, la responsabilità rischia di dissolversi: serve una nuova architettura etica e giuridica per evitare che l’errore diventi sistemico. La sicurezza evolve dai caschi alle valutazioni di impatto algoritmico: la protezione del lavoratore passa anche per i suoi dati, il suo volto, le sue decisioni automatizzate. Il diritto è in ritardo sull’algoritmo: serve riconoscere il diritto alla spiegazione, alla revisione umana, alla partecipazione sindacale nei sistemi di decisione automatica.

1.3.5 Predittività e cognizione

“Prevenzione” non è più solo evitare che un rischio noto si concretizzi, ma prevedere l’insorgere di eventi non ancora accaduti. Qui va la sicurezza predittiva alimentata dall’intelligenza artificiale. Immaginiamo una grande impresa manifatturiera dove decine di sensori distribuiti su macchinari, strumenti e ambienti generano ogni secondo una mole di dati; su questi interviene l’IA, che attraverso algoritmi di *machine learning* è in grado di riconoscere schemi ricorrenti e anticipare guasti, anomalie

o comportamenti rischiosi. Un compressore che inizia a vibrare in modo anomalo, un sistema idraulico che accumula pressione oltre soglia: l'IA può segnalarli prima che si trasformino in pericoli concreti. Secondo alcuni dati (fonte Rapporto INAIL 2023) questo ridurrebbe gli incidenti di un 40%.

Si aumentano la sicurezza e l'efficienza economica, si riducono i tempi di inattività, si ottimizzano gli interventi di manutenzione, si allunga la vita delle attrezzature. Il flusso dati in un sistema di manutenzione predittiva (sensori → cloud → dashboard operatori) è già implementato in settori come l'energia, la logistica e l'aerospaziale. Tuttavia, anche le tecnologie predittive non sono infallibili. Gli algoritmi possono basarsi su dati incompleti o di scarsa qualità, oppure sbagliare nel valutare il contesto.

Il rischio latente è che la fiducia cieca nel sistema porti a un indebolimento dell'attenzione umana, la riduzione della vigilanza. Ecco perché la sicurezza predittiva non deve sostituire il giudizio umano, ma affiancarlo, supportarlo, stimolarlo. Come in un'orchestra, in cui la macchina è un ottimo strumento, ma la partitura e il ritmo devono ancora essere diretti da una coscienza umana.

Nel passaggio all'economia digitale, il corpo lascia spazio alla mente. Non che il rischio fisico sparisca, tutt'altro: basta visitare un cantiere o un impianto chimico per rendersene conto. Ma la quota di lavoro che oggi si svolge davanti a uno schermo, in ambienti "sicuri", è cresciuta esponenzialmente. E con essa, sono cresciuti i rischi invisibili: affaticamento mentale, stress cronico, solitudine organizzativa.

L'interazione con sistemi intelligenti può aggravare le fragilità psicologiche già presenti nel contesto lavorativo. Si può perdere il senso di controllo sul proprio lavoro, sentendosi progressivamente escluso o marginalizzato. A tutto ciò si aggiungono fenomeni nuovi, ancora poco studiati ma molto reali: il senso di disorientamento davanti a cambiamenti troppo rapidi, la dipendenza da feedback digitali, l'ansia da aggiornamento costante delle proprie competenze.

È il rischio cognitivo, il nuovo fronte della sicurezza del lavoro. Per affrontarlo servono politiche mirate: valutazioni del rischio psicosociale e interventi di supporto psicologico. Ma serve anche una rivoluzione culturale: il lavoratore è un soggetto pensante, senziente, in relazione con un ecosistema complesso. L'IA può essere alleata. Alcune aziende stanno già sperimentando sistemi digitali per analizzare il benessere dei lavoratori ("*wellbeing analytics*"), che valutano l'uso delle e-mail, la frequenza delle riunioni o il tono delle comunicazioni per suggerire pause, ferie o una diversa organizzazione del lavoro. Ma anche qui vale la regola aurea: non è lo strumento che conta, ma l'intenzione con cui viene usato.

Sintesi- Prevedere è meglio che prevenire, ma delegare alla macchina la sorveglianza dei segnali deboli può generare nuove cecità. La vigilanza è un affare umano. L'interazione prolungata con sistemi intelligenti sposta il rischio sul piano mentale: ansia, isolamento e disorientamento sono le nuove emergenze della sicurezza.

1.3.6 Prospettive: coevolvere con intelligenza e restare umani

Non tutte le transizioni sono uguali, questa dell'IA è pervasiva, trasversale, asimmetrica. Riguarda l'industria e la cultura, la giustizia e la pubblicità, la medicina e l'arte. Ma soprattutto, ridefinisce la relazione tra intelligenza umana e sistemi artificiali. In ambito lavorativo, questo significa immaginare una nuova forma di coevoluzione: non più la macchina che sostituisce l'uomo, ma l'uomo che ripensa sé stesso alla luce della macchina. Questo richiede coraggio, visione, ma anche una gestione lungimirante e condivisa.

L'Italia ha inserito nel suo Piano Nazionale di Ripresa e Resilienza (PNRR) numerosi interventi dedicati alla digitalizzazione, alla formazione e alla ricerca. Tuttavia, c'è ancora una lacuna: la visione del lavoro come campo di sperimentazione dell'IA viene spesso affrontata in chiave economica o tecnologica, raramente come questione sociale e culturale. Quale etica del lavoro saprà integrare il dato con il senso, l'efficienza con la giustizia, l'innovazione con la memoria. Perché il lavoro non è solo ciò che facciamo, ma anche ciò che siamo. E se cambia il modo di lavorare, cambia anche la nostra identità.

Un esempio emblematico è quello delle cooperative di moderatori di contenuti digitali, che collaborano con grandi piattaforme online. Questi lavoratori sono assistiti da IA che pre-selezionano i contenuti da valutare, ma restano esposti a immagini violente, stress e ambiguità normative. Il loro lavoro è essenziale per la sicurezza di tutti, ma spesso invisibile, sottopagato, poco riconosciuto. Non basta parlare di “transizione digitale”: bisogna parlare di “giustizia digitale”.

Nel mondo dell'IA, tutto cambia velocemente. Ma alcune domande restano immobili. Chi siamo? Dove stiamo andando? E soprattutto: chi vogliamo diventare? L'IA come ogni strumento, può essere usato per costruire o per distruggere, per includere o per escludere, per emancipare o per controllare. Sul lavoro la sfida radicale: quella di restare umani in un mondo automatizzato. Potremmo dedicarci a: creatività, empatia, senso del limite, cooperare, correggere, prendersi cura. In questo senso, la sicurezza sul lavoro diventa il banco di prova di una civiltà che vuole essere non solo tecnologicamente avanzata, ma anche giusta, inclusiva, sostenibile. Un luogo in cui la vita umana – con la sua fragilità e la sua forza – sia rispettata, protetta, valorizzata.

Come ha scritto Italo Calvino nelle sue “Lezioni americane”, il futuro appartiene a chi saprà coniugare leggerezza e precisione, velocità e profondità. Una strada può essere quella di riscoprire la forza dell'intelligenza collettiva. L'innovazione come frutto di confronto, ascolto, negoziazione. È qui che entra in gioco la progettazione partecipata. La sicurezza, infatti, non si impone: si co-costruisce. Questo approccio riduce i conflitti, aumenta la comprensione dei sistemi e soprattutto favorisce un senso di controllo diffuso.

Alcuni modelli di democrazia partecipativa nei luoghi di lavoro, come le esperienze di co-design digitale sviluppate nei paesi nordici (Finlandia, Svezia, Danimarca), offrono spunti concreti. I lavoratori vengono coinvolti fin dalla fase di analisi dei fabbisogni, e i sistemi vengono calibrati in base a valori esplicitamente discussi. Questo approccio è noto come “*Digital Participatory Design*”: i sistemi vengono modellati in base a criteri co-definiti, favorendo trasparenza, accettabilità e sostenibilità sociale della tecnologia.

In una società dove la tecnologia evolve più velocemente della regolamentazione, la partecipazione diretta degli utenti può diventare uno strumento potente di prevenzione e giustizia. Per questo parlare di intelligenza artificiale e lavoro significa, in ultima analisi, parlare dell'umano. Il lessico umano prevede di lavorare con passione, con dignità, con solidarietà.

Ecco perché serve, oggi più che mai, una nuova narrazione. Non l'IA come salvezza, né come minaccia, ma come occasione per rivedere il nostro patto sociale e culturale. In questo senso, l'arte, la letteratura e la filosofia hanno un ruolo cruciale. Possono aiutarci a dare un volto, una voce e persino un'anima al lavoro che cambia. Perché, come ci ricorda Primo Levi, “*amare il proprio lavoro è la miglior approssimazione concreta alla felicità sulla terra*”. Ma anche la psicologia lo conferma: secondo Abraham Maslow, “*l'uomo si realizza pienamente solo quando lavora a ciò che ama, in un contesto che gli permette di crescere*”. Il lavoro, dunque, non è solo un mezzo di sostentamento, ma una dimensione fondamentale dell'autorealizzazione umana.

Se l'intelligenza artificiale può aiutarci ad avvicinarci a questa felicità – non sostituendoci, ma liberandoci – allora avremo davvero costruito un futuro intelligente: più efficiente, certo, ma soprattutto più umano.

Sintesi- Non siamo più davanti alla macchina, ma dentro un ecosistema cognitivo: l'unica strada percorribile è la co-evoluzione, purché guidata da scelte condivise e visione etica. L'intelligenza artificiale è solo uno strumento: la vera sfida è restare umani, scegliendo di usarla per espandere creatività, cura e giustizia, non per delegare coscienza e responsabilità. L'innovazione non può essere un'imposizione tecnocratica: solo una progettazione condivisa con i lavoratori può garantire giustizia, efficacia e sostenibilità. Lavorare è dare senso, non solo produrre. Se l'IA ci aiuterà a liberare tempo e mente per esprimerci meglio, allora avremo davvero scelto l'intelligenza giusta.

1.3.7 Sguardi globali: il governo del possibile

Affrontare il tema “IA e lavoro” significa anche considerare le traiettorie che diverse culture e sistemi giuridici stanno seguendo. Non esiste, infatti, un'unica visione globale sull'intelligenza artificiale applicata ai luoghi di lavoro.

In Europa, l'approccio all'intelligenza artificiale è cauto e pone al centro la tutela dei diritti delle persone. L'Unione Europea sostiene uno sviluppo dell'IA a misura d'uomo, come indicato sia nell'AI Act, che stabilisce regole vincolanti, sia nel più recente AI Pact, un accordo volontario tra aziende e Stati membri per anticipare l'applicazione di tali regole. I valori fondamentali promossi includono trasparenza dei sistemi, correttezza nei risultati, sicurezza tecnica e presenza costante di una supervisione umana.

Negli Stati Uniti, il modello dominante è quello dell'assenza di regole vincolanti (“*deregulation*”). L'innovazione è incentivata dal mercato e le aziende tecnologiche mantengono ampi margini di autonomia. I rischi vengono spesso gestiti a valle, attraverso azioni collettive (“*class action*”) o scandali mediatici. Il tema della sorveglianza sul lavoro, ad esempio, è trattato in modo molto più permissivo.

In Asia, troviamo invece una forte centralità dello Stato. In Cina, l'IA è una tecnologia chiave del piano “Made in China 2025”, ma il suo utilizzo nei contesti lavorativi solleva questioni legate al controllo sociale. In Giappone e Corea del Sud, l'automazione è invece vista come una risposta alla crisi demografica, e la cooperazione uomo-macchina è promossa come modello culturale.

Confrontare questi approcci significa capire che anche la competizione tra modelli di governance dell'IA è parte del paesaggio del lavoro futuro. Quale modello vogliamo seguire? E, più importante, quale modello vogliamo contribuire a costruire? Siamo ancora padroni degli strumenti che creiamo? O ne siamo diventati estensioni inconsapevoli? L'intelligenza artificiale – così potente, così invisibile – ci costringe a guardare in faccia questa domanda. E a rispondere non solo con leggi e codici, ma con cultura, con visione, con coraggio.

Il futuro non ci è dato: va progettato. E nel progetto, la sicurezza non è solo uno standard da raggiungere, ma un diritto da difendere, un bene comune da coltivare. Il lavoro del futuro – aumentato, ibrido, assistito – potrà essere davvero uno spazio di emancipazione, se sapremo dotarci di nuove lenti per osservarlo e nuove mani per modellarlo. C'è un'immagine metaforica che ben sintetizza questa sfida: l'uomo che danza con la macchina. Non un duello, ma una coreografia di un futuro condiviso. Dove la tecnica segue il passo della dignità. Dove l'algoritmo si piega all'etica.



Per trasmettere questa idea con la sensibilità di un'artista ho scelto un'opera di Benedetta Cappa (1897–1977), che è stata una delle protagoniste dimenticate del Futurismo italiano, nonché moglie di Filippo Tommaso Marinetti. Artista, scrittrice e teorica, fu tra le prime a esplorare la fusione tra sensibilità umana e tecnologia in chiave non solo celebrativa, ma poetica. La sua opera “Sintesi delle comunicazioni aeree” (tempera ed encausto su tela, 1933) è un dipinto astratto in cui onde, traiettorie, segnali e vibrazioni si intrecciano in uno spazio dinamico e ritmico. Non ritrae macchine o umani, ma il loro dialogo: linee dinamiche dove tecnologia e sensibilità si fondono. Così, il lavoro del futuro chiede armonia al posto del conflitto. Non vi è figura umana riconoscibile, ma l'intero quadro è attraversato da un'intelligenza mobile, quasi danzante, che richiama la percezione aumentata di un soggetto che si fonde con le tecnologie dell'aria e della trasmissione.

È adatta perché non oppone l'umano alla macchina, ma li immagina come compagni di volo, co-coreografi di un mondo in movimento. Anticipa visivamente l'idea che “l'intelligenza si fa anche saggezza” quando tecnica e dignità si intrecciano in una forma nuova di bellezza. La chiamata ad agire può prevedere:

1. Creare “Laboratori di co-design” in ogni distretto industriale, dove lavoratori e ingegneri progettino insieme strumenti IA.
2. Introdurre un “Indice di Umanità” per valutare l'impatto sociale delle tecnologie sul lavoro.

Perché, citando ancora Primo Levi, «*la macchina perfeziona l'uomo solo se l'uomo non si fa macchina*».

Sintesi Finale- L'intelligenza artificiale ci obbliga a rinegoziare il senso stesso del lavoro, tra automazione e umanità, sorveglianza e fiducia, efficienza e giustizia. In questo crocevia epocale, la sicurezza non è solo prevenzione tecnica, ma garanzia culturale di un lavoro che resti spazio di dignità, relazione e futuro. Non ci serve una macchina perfetta: ci serve un'umanità all'altezza delle macchine che crea. E se il lavoro sarà davvero “intelligente”, lo sarà solo nella misura in cui saprà restare umano.

1.4 L'utilizzo di nuove tecnologie per eliminare o ridurre rischi lavorativi: nuove tecnologie, DPC, DPI

Cristina Mora, Alice Caporale

Dipartimento di Ingegneria Industriale – Università di Bologna

L'innovazione tecnologica ha sempre rappresentato un fattore chiave nello sviluppo industriale, contribuendo a migliorare sia l'efficienza produttiva che la sicurezza sul lavoro. Con l'avvento dell'Industria 5.0, definita dalla Commissione Europea come "un'evoluzione dell'Industria 4.0 che enfatizza la sostenibilità, la resilienza e la centralità dell'uomo nel processo produttivo", si compie un ulteriore passo avanti. L'integrazione tra automazione avanzata, intelligenza artificiale (AI) e attenzione al benessere del lavoratore permette di coniugare l'aumento dell'efficienza operativa con la riduzione dei rischi, grazie all'introduzione di soluzioni tecnologiche sempre più personalizzate e mirate. In questo contesto l'organizzazione e la gestione del lavoro sono sempre più influenzati dalla digitalizzazione: i sistemi digitali, e in particolare quelli basati su algoritmi e AI, stanno infatti diventando parte integrante dei luoghi di lavoro, trasformando i modi in cui vengono svolti e coordinati i compiti lavorativi e supervisionati i lavoratori, in ambito manifatturiero e non solo.

L'Intelligenza artificiale fa riferimento alla simulazione dell'intelligenza umana in macchine programmate per pensare e imparare come gli umani. Essa prevede lo sviluppo di algoritmi e modelli computazionali che permettono di riprodurre azioni che richiedono l'uso dell'intelligenza umana. L'AI si divide in due categorie: Internet of Things (IoT) e AI generativa e comprende diversi campi, quali la robotica, il computer vision, il machine learning e sistemi esperti e l'uso di algoritmi che permettono ai computer di imparare dall'esperienza (El-Helaly, 2024).

L'AI gioca oggi un ruolo cruciale in vari aspetti dei processi lavorativi, rivoluzionando la modalità in cui le attività sono svolte e gestite. Le tecnologie appartenenti all'AI trovano applicazione in diverse aree, quali la gestione di macchine e di processi produttivi, la movimentazione e lo stoccaggio dei materiali, la gestione e formazione dei lavoratori e la loro sicurezza. In un contesto in cui l'errore umano rimane una causa importante di incidenti sul lavoro, l'AI può giocare un ruolo importante per la sua capacità di processare e analizzare i dati in tempi rapidi e di identificare potenziali rischi e pericoli che possono non essere notati dall'uomo (Shah and Mishra, 2024).

L'adozione di tecnologie basate sull'AI, pertanto, sta trasformando il modo in cui le aziende affrontano la prevenzione degli infortuni, offrendo strumenti più precisi ed efficienti per proteggere i lavoratori.

È importante, però, richiamare l'attenzione anche all'uso responsabile dell'AI, come ci ricorda il regolamento europeo sull'intelligenza artificiale entrato in vigore il 1° agosto 2024, che mira a promuovere lo sviluppo e la diffusione responsabili dell'intelligenza artificiale nell'UE, fornendo requisiti e obblighi chiari a sviluppatori e operatori per quanto riguarda gli usi specifici dell'AI. Così come è importante tenere in considerazione anche i potenziali impatti negativi dell'uso dell'AI negli ambienti di lavoro, come problemi etici e di privacy nei confronti dei lavoratori.

1.4.1 Gli strumenti alla base dell'Intelligenza Artificiale

Entriamo ora nel merito degli strumenti e delle tecnologie su cui si fonda l'uso dell'AI. I sistemi digitali in grado di migliorare la salute e sicurezza dei lavoratori si basano, infatti, su diversi **tipi di tecnologie**, quali: *sistemi di raccolta dati* (quali sensori, videocamere, sistemi ottici, microfoni), *sistemi di trasmissione dei dati* (quali bluetooth, radiofrequenza, Internet of Things) e *sistemi di processamento dei dati* e trasferimento delle informazioni utili ai lavoratori (quali gli algoritmi di Intelligenza Artificiale), che interagiscono tra loro come raffigurato in figura 1. Nello specifico con

Internet of Things si intende comunemente una rete di “oggetti” (devices) interconnessi, “attrezzati” con tecnologie di riconoscimento capaci di “interagire” tra loro e/o verso i punti nodali di un sistema informatico dedicato che li governa. Con Intelligenza Artificiale si fa riferimento ad una tecnologia legata alla progettazione e allo sviluppo di sistemi dotati di capacità di apprendimento automatico e di adattamento, ispirate ai modelli di apprendimento umani. L’AI, infatti, utilizza *algoritmi avanzati di machine learning, reti neurali e altri strumenti* per analizzare numerosi dati complessi in tempo reale e prendere quindi decisioni più mirate. Nell’ambito della sicurezza sul lavoro questo apre la strada ad una grande potenzialità: quella di fornire previsioni e raccomandazioni per prevenire incidenti.

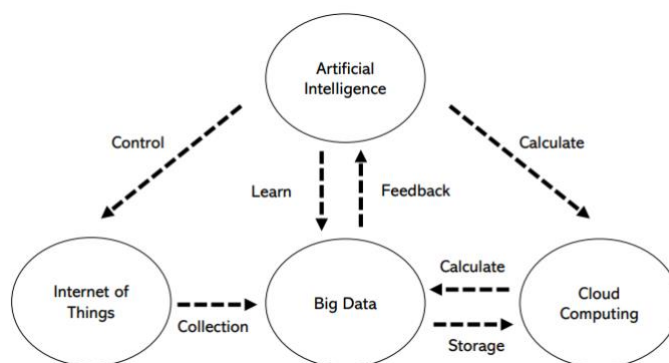


Fig. 1 Sistema di raccolta e analisi dei dati (fonte Berastegui, 2024)

Possibili **strumenti e soluzioni per la sicurezza** basati sull’intelligenza artificiale sono i Dispositivi di Protezione Individuali intelligenti (smart DPI), i sistemi basati sulla Realtà Virtuale e sulla Computer Vision, i droni e i veicoli aerei senza pilota e alcune tipologie di esoscheletro che utilizzano le reti neurali.

Esempi di smart DPI sono gli stivali intelligenti e i caschi intelligenti. I primi monitorano continuamente l'ambiente circostante l’operatore e rilevano condizioni non sicure, determinando segnalazioni in tempo reale o interventi che prevengono il rischio; i secondi sono dotati di una serie di sensori, tra cui GPS, RFID, UWB, AVM che sono in grado di monitorare la locazione dei lavoratori, la loro attività, l’ambiente circostante e la loro salute personale, oltre che la qualità dell’aria. L’efficacia dei DPI, quindi, può essere potenzialmente migliorata dall’abbinamento di sensori e videocamere potenziate dall’AI per segnalare tempestivamente eventuali pericoli. Grazie a particolari sensori incorporati, sarà infatti possibile inviare dati in tempo reale a un sistema centralizzato capace di analizzare se i DPI sono utilizzati in modo corretto e in quali circostanze (se ne riporta un esempio in figura 2).



Fig.2 Esempio di sistema basato su smart DPI (<https://safetyforge.it/>)

Un esempio di utilizzo della Computer Vision è il monitoraggio dei lavoratori attraverso camere termiche e l'identificazione di potenziali rischi, quali lo stress microclimatico.

I droni sono utili per fare ispezioni e interventi di manutenzione diretta, riducendo il rischio di effetti negativi dovuti allo sforzo fisico o all'esposizione a condizioni climatiche e ambientali avverse;

I robot collaborativi (cobot) ed esoscheletri sono capaci di fornire un supporto fisico avanzato, prevenendo infortuni e mitigando lo stress causato dal sollevamento ripetuto di carichi pesanti.

1.4.2 Aree di applicazione dell'Intelligenza Artificiale

Le principali aree di applicazione dell'AI in relazione al positivo impatto sulla sicurezza sul lavoro sono:

- **Monitoraggio in Tempo Reale**
- **Previsione degli Infortuni**
- **Formazione Personalizzata**
- **Manutenzione Predittiva**
- **Comunicazione e Risposta alle Emergenze**

Per quanto riguarda il **monitoraggio in tempo reale** delle condizioni di lavoro, si citano *sensori avanzati e sistemi di visione artificiale* che possono rilevare situazioni potenzialmente pericolose prima che si verifichino incidenti. Ad esempio, i sistemi di monitoraggio che utilizzano l'AI possono analizzare il comportamento dei conducenti dei macchinari pesanti, rilevando segni di stanchezza o distrazione e inviando avvisi per prevenire incidenti. Altro esempio è quello di telecamere dotate di AI per identificare automaticamente se i lavoratori indossano l'equipaggiamento di protezione individuale corretto in aree ad alto rischio.

In ambito di **previsione degli Infortuni**, l'AI può analizzare enormi quantità di dati per identificare pattern che precedono gli infortuni. Attraverso l'apprendimento automatico (machine learning), i sistemi possono prevedere incidenti analizzando fattori come il tempo, le condizioni ambientali, i comportamenti passati dei lavoratori e le attività in corso. A titolo di esempio si cita la piattaforma di AI che raccoglie dati dai sensori indossabili dei lavoratori per prevedere infortuni legati a movimenti ripetitivi e posture scorrette, o il sistema di analisi predittiva che valuta i dati storici degli incidenti e identifica i potenziali pericoli, permettendo alle aziende di adottare misure preventive mirate.

Le tecnologie basate sull'AI stanno rivoluzionando anche la **formazione dei lavoratori**. Simulazioni di realtà virtuale (VR) potenziate dall'AI offrono esperienze di formazione immersiva, permettendo ai lavoratori di affrontare situazioni pericolose in un ambiente controllato.

Anche l'AI applicata alla **manutenzione predittiva** delle attrezzature consente di prevedere i guasti e i malfunzionamenti prima che si verifichino, attraverso l'analisi dei dati ricavati dai sensori integrati nei macchinari, ed elaborati poi dagli algoritmi di AI riducendo così il rischio di incidenti legati a attrezzature difettose.

Infine, in **caso di emergenza**, la velocità e l'accuratezza della comunicazione sono fondamentali per evitare incidenti mortali. In tal senso i sistemi di IA possono coordinare le risposte alle emergenze, fornendo istruzioni chiare e in tempo reale ai lavoratori e ai soccorritori.

Da queste aree di applicazione emerge l'elevato potenziale che l'AI può offrire nel processo di Valutazione dei Rischi e nelle Misure di Prevenzione e Protezione nei luoghi di lavoro.

1.4.3 La gestione del personale basata su AI e algoritmi

Con riferimento alla gerarchia dei controlli del rischio (NIOSH), riportata in figura 3, un ruolo importante nella riduzione dei rischi rivestono anche le procedure amministrative e l'organizzazione del lavoro (Administrative Controls).

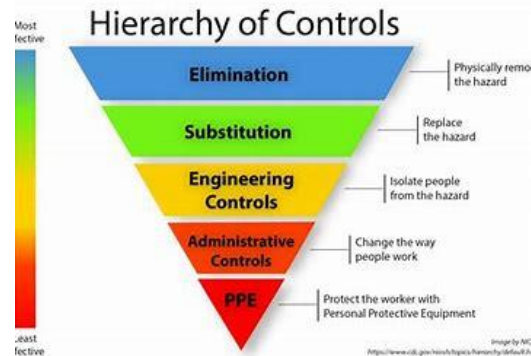


Fig. 3 Schema della gerarchia di controllo del rischio (fonte NIOSH)

In questo ambito si collocano pertanto tutte le forme di gestione del personale che possono portare benefici in termini di sicurezza sul lavoro. Anche in questo campo può giocare un ruolo importante l'introduzione di sistemi digitali che acquisiscono dati in tempo reale dall'ambiente di lavoro, dai lavoratori e dalle attività svolte e inserendoli poi in sistemi basati su AI e algoritmi in grado di adottare decisioni automatizzate o semi-automatizzate o di fornire informazioni utili ai datori di lavoro o ai lavoratori stessi. Tali informazioni possono poi essere utilizzate per assegnare compiti, pianificare turni di lavoro, monitorare e valutare il comportamento e le prestazioni dei lavoratori (EU-OSHA, 2025).

Gli effetti reali dell'applicazione di sistemi di gestione del personale basati su AI e algoritmi sono il miglioramento della previsione della domanda, della programmazione dei turni, dell'assegnazione dei compiti ai lavoratori sulla base delle loro capacità e delle loro caratteristiche antropometriche e culturali, incrementando in questo modo la loro sicurezza e il benessere sul lavoro.

1.4.4 Ambiti di applicazione di tecnologie di Intelligenza Artificiale per la sicurezza

a) Logistica - Tecnologia AI per la sicurezza nella logistica

Uno degli ambiti più importanti di applicazione dell'Intelligenza Artificiale riguarda la logistica e la gestione della supply chain, portando alla nascita della logistica 4.0, definita come una nuova era che vede le aziende utilizzare tecnologie avanzate come l'Internet of Things, l'intelligenza artificiale, la blockchain e la robotica per ottimizzare la gestione della supply chain e la movimentazione delle merci, come schematizzato in figura 4.

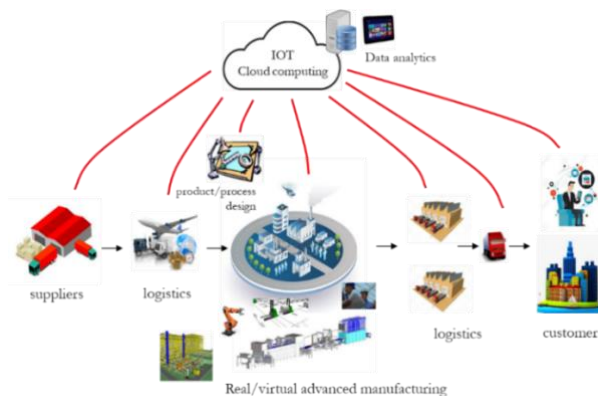


Fig. 4 Manufacturing 4.0: SMART SUPPLY CHAIN

L'efficacia dell'AI nella Logistica 4.0 si manifesta anche in ambito di sicurezza sul lavoro, andando ad agire su quei fattori di rischio che determinano infortuni e incidenti mortali sia nella movimentazione delle merci che nelle attività di stoccaggio e magazzino. La gestione della sicurezza nei magazzini presenta, infatti, sfide significative: incidenti durante la movimentazione dei carichi, sovraffollamento e il rischio di errori dovuti a scarsa visibilità o mancanza di tracciabilità adeguata. Da analisi statistiche INAIL emerge inoltre che l'uso dei carrelli industriali rappresenta la maggiore causa di infortunio, come si evince dai dati di figura 5.

DENUNCE DI INFORTUNIO E CASI MORTALI PER IL SETTORE DEI TRASPORTI E MAGAZZINAGGIO PER DIVISIONE ATECO E ANNO EVENTO					
Infortunati in complesso					
Divisione Ateco 2007	2016	2017	2018	2019	2020
trasporto terrestre e trasporto mediante condotte	17.846	18.153	17.195	16.367	12.384
trasporti marittimi e per vie d'acqua	189	149	167	188	99
trasporto aereo	435	484	428	412	137
magazzinaggio e attività di supporto ai trasporti	15.884	15.633	14.777	14.152	9.107
servizi postali e attività di corriere	8.707	8.583	8.645	8.332	7.527
trasporti e magazzinaggio	43.061	43.002	41.212	39.451	29.254
Casi mortali					
Divisione Ateco 2007	2016	2017	2018	2019	2020
trasporto terrestre e trasporto mediante condotte	96	104	117	88	120
trasporti marittimi e per vie d'acqua	-	-	-	-	1
trasporto aereo	-	-	1	-	-
magazzinaggio e attività di supporto ai trasporti	33	22	32	23	19
servizi postali e attività di corriere	5	10	9	6	25
trasporti e magazzinaggio	134	136	159	117	165

Fonte: Banca Dati Statistica, dati aggiornati al 30.04.2021

Incidenti, fattori di rischio e attività lavorative che hanno determinato incidenti durante le attività di stoccaggio		
	Trasporto e stoccaggio (90 casi)	Commercio e vendita (21 casi)
Incidenti		
contatto con oggetti in movimento o veicoli	23%	24%
variazione della velocità o ribaltamento del veicolo	23%	10%
caduta di oggetti dall'alto	21%	14%
caduta di lavoratori dall'alto	14%	38%
Fattori di rischio		
carrelli industriali	80%	71%
lavori in altezza	4%	10%
Attività lavorativa		
Movimentazione materiali	70%	43%
Movimentazione manuale materiali	11%	24%
Trasporto	11%	24%

Fig. 5 Statistiche infortuni e casi mortali per trasporto e magazzinaggio (fonte INAIL e Botti et al., 2022)

Da database InforMO di Inail (INAIL, 2019) emerge che le cause più comuni incidenti gravi derivanti dalle attività di magazzinaggio sono il contatto con un oggetto o un veicolo in movimento, la variazione di velocità o il ribaltamento del veicolo, la caduta di oggetti dall'alto e la caduta del lavoratore infortunato dall'alto. I carrelli elevatori sono i fattori di rischio più comuni per gli incidenti gravi che si verificano durante le attività di magazzinaggio.

In questo ambito l'uso dell'intelligenza artificiale può essere utile per ridurre gli infortuni attraverso l'impiego di tecnologie collegate all'AI, quali la **videosorveglianza intelligente**, **i sensori di prossimità e sistemi di anticollisione**. La videosorveglianza intelligente si basa sull'impiego di telecamere dotate di intelligenza artificiale che monitorano costantemente le attività e rilevano comportamenti anomali o situazioni di pericolo, come movimenti non autorizzati o condizioni che potrebbero portare a incidenti, attivando un allarme in tempo reale e consentendo un intervento tempestivo del personale di sicurezza.

I sensori di prossimità, installati sui mezzi di movimentazione (ad esempio carrelli elevatori), rilevano la presenza di persone o ostacoli nelle vicinanze e i sistemi di anticollisione attivano freni automatici e allarmi acustici e visivi, riducendo il rischio di collisioni.

Se prima i sistemi di anticollisione erano basati sull'impiego di tecnologia radar, tag indossabili dalle persone e connessione, oggi si apre una nuova frontiera basata sull'AI e sull'impiego di una rete neurale addestrata per il riconoscimento delle persone e dei mezzi solo attraverso l'impiego di video e immagini. È sufficiente quindi installare sul veicolo un sistema di rilevamento selettivo basato sull'impiego di video e immagini per permettere di riconoscere parti del corpo umano e la relativa distanza senza tag e radar.

Solo a titolo di esempio si cita il sistema di rilevamento selettivo KiwiEye (<https://kiwitron.com/it/>) un sistema anticollisione basato su **intelligenza artificiale** in grado di rilevare oggetti, segnaletica e persone anche senza DPI. KiwiEye monitora costantemente i potenziali pericoli e rallenta automaticamente il mezzo in caso di situazioni critiche. Ideale per magazzini e cantieri, migliora i **tempi di reazione degli operatori** e riduce le distrazioni, contribuendo a raggiungere l'obiettivo "zero infortuni". Il sistema si basa su una rete neurale addestrata per riconoscere persone e mezzi senza l'impiego di radar e di tag e consente in automatico il rallentamento del veicolo solo quando necessario. Il sistema consente, inoltre, di rilevare automaticamente tramite QRCode apposto all'ingresso di un reparto o di una area di lavoro le caratteristiche di movimentazione richieste (come, ad esempio, la velocità e l'altezza massima delle forche per l'ingresso) e di adeguare le caratteristiche di movimentazione di conseguenza.

In figura 6 si riportano alcune immagini esemplificative del sistema e relativi accessori: il *tablet touch screen* che permette di visualizzare in real time lo streaming di KiwiEye, il *Datalogger con display touch* che consente di visualizzare sul display la presenza di eventuali ostacoli nell'area circostante, di localizzare i mezzi e gestirne gli accessi, il *dispositivo con interfaccia a LED* che attiva il rallentamento del mezzo, in cui il colore e la direzione delle luci indicano la distanza e la posizione dell'ostacolo rilevato da KiwiEye.



Fig. 6 Sistema di rilevamento KiwiEye e accessori (<https://kiwitron.com/it/>)

b) Assistenza Domiciliare - Tecnologia AI per la sicurezza nella assistenza domiciliare

Un ambito innovativo di applicazione dell'intelligenza artificiale è l'Assistenza Domiciliare. L'AI sta infatti trasformando anche questo settore, offrendo strumenti innovativi che supportano sia i pazienti che gli infermieri di famiglia. Alcune applicazioni chiave sono: il monitoraggio remoto dei pazienti, la previsione di complicazioni, il supporto alla gestione delle terapie, l'assistenza virtuale e l'analisi dei dati per una migliore pianificazione.

In particolare, tra gli strumenti per il monitoraggio remoto dei pazienti si possono citare i Dispositivi indossabili (es. smartwatch, braccialetti) e sensori domestici, che possono raccogliere dati in tempo reale su parametri vitali come pressione sanguigna, frequenza cardiaca, glicemia e saturazione di ossigeno, collegati all'AI che analizza questi dati per identificare anomalie e inviare alert agli

infermieri o ai medici, permettendo interventi tempestivi. Uno schema rappresentativo del sistema di monitoraggio basato su AI è riportato in figura 7. Gli algoritmi di AI, basandosi su dati storici e trend attuali, possono prevedere il rischio di problemi in pazienti con malattie croniche per poter agire in modo preventivo. Possono inoltre aiutare a personalizzare i piani terapeutici mentre app e dispositivi con AI possono ricordare ai pazienti di assumere i farmaci, migliorando l'aderenza terapeutica. Infine, l'AI può analizzare grandi volumi di dati sanitari per identificare trend e bisogni specifici della popolazione e individuare di conseguenza dei piani mirati.



Figura 7: rappresentazione schematica per il monitoraggio remoto della salute umana

L'introduzione dell'AI nell'ambito dell'assistenza domiciliare può portare quindi ad un miglioramento della qualità dell'Assistenza, attraverso l'impiego di strumenti precisi e tempestivi e permette una migliore prevenzione, riducendo i ricoveri e consentendo una maggiore personalizzazione delle cure, in funzione delle esigenze specifiche di ogni paziente. In tale contesto però è necessario affrontare anche le sfide etiche e tecniche che l'AI presenta, per garantire che la tecnologia sia utilizzata in modo responsabile e umano. Alcune preoccupazioni sollevate in merito all'integrazione tra AI e assistenza domiciliare riguardano infatti la privacy e sicurezza dei dati sanitari per la loro sensibilità.

Un esempio di successo dell'applicazione di AI nell'assistenza domiciliare è rappresentato dalla **teleriabilitazione**, che è diventata una risorsa essenziale, non solo per i pazienti con patologie neurologiche e croniche, ma anche per trattare problematiche muscoloscheletriche. Il sistema di teleriabilitazione comprende un kit per il paziente, un tablet ad uso del professionista e una Web console per la gestione amministrativa. La ARC Unit, destinata al paziente, è il cuore del sistema ed è costituita da 5 sensori inerziali indossabili, una base di ricarica e un tablet con un'applicazione dedicata. Questi sensori vengono posizionati sui principali segmenti corporei del paziente (caviglie, polsi e tronco) e monitorano i movimenti durante gli esercizi, fornendo dati precisi che vengono analizzati in tempo reale. Alla base del sistema c'è un algoritmo di Intelligenza Artificiale che ha il compito di analizzare i movimenti del paziente in tempo reale.

L'algoritmo è in grado di segmentare i movimenti in ripetizioni corrette e di identificare eventuali errori, fornendo un feedback immediato. Questo approccio permette di calcolare in modo automatico e preciso l'aderenza al programma riabilitativo individuale e di adattare la terapia alle necessità specifiche di ogni paziente.

c) Ambienti di lavoro ad alto rischio: Tecnologie AI per la sostituzione dell'intervento diretto dell'operatore

In diversi ambiti e settori, inoltre, è possibile individuare ambienti di lavoro che possiamo definire "ad alto rischio" e in cui lo svolgimento di attività da parte dell'operatore umano comporta un elevato rischio di infortunio anche mortale.

Un esempio di queste attività è quello di lavori in un ambiente confinato e/o sospetto di inquinamento, che secondo la recente norma UNI 11958:2024, si definisce come "Spazio circoscritto

non progettato e costruito per la presenza continuativa di un lavoratore, ma di dimensioni tali da consentirne l'ingresso e lo svolgimento del lavoro assegnato, caratterizzato da vie di ingresso o uscita limitate e/o difficoltose, con possibile ventilazione sfavorevole, all'interno del quale non è possibile escludere la presenza o lo sviluppo di condizioni pericolose per la salute e la sicurezza dei lavoratori". A questi si aggiungono anche gli ambienti cosiddetti "assimilabili" che la stessa norma indica come ambienti che "presentano caratteristiche strutturali e rischi analoghi agli ambienti confinati e/o sospetti di inquinamento". In figura 8 si riportano due immagini esemplificative di ambienti confinati e/o sospetti di inquinamento.



Figura 8: esempi di Ambienti Confinati

Vista la molteplicità di infortuni spesso mortali che accadono ogni anno in tali luoghi, si considera prioritario lavorare sulla riduzione del rischio e meglio ancora sulla sua eliminazione ed oggi ciò è reso possibile anche attraverso l'impiego di tecnologie "no man entry" che consentono di svolgere l'attività richiesta (i.e. manutenzione, pulizia, controllo, ...) senza prevedere l'ingresso dell'operatore.

Anche in questo caso può risultare estremamente utile l'impiego dell'AI per il monitoraggio e il controllo della strumentazione a distanza e per la raccolta e successiva rielaborazione di dati utili per svolgere analisi e per istruire al meglio le attrezzature allo svolgimento dei compiti mediante algoritmi di machine learning.

1.4.5 La Banca delle Soluzioni: un contenitore di soluzioni

Nel contesto di una crescente attenzione alla tecnologia come supporto alla sicurezza, al benessere dei lavoratori e alla prevenzione dei rischi, il progetto "Banca delle Soluzioni" emerge come un'iniziativa di particolare rilievo. Nato nel 2014 grazie alla collaborazione tra il Dipartimento di Ingegneria Industriale dell'Università di Bologna e l'AUSL di Bologna, con il coinvolgimento di diversi enti territoriali preposti alla sicurezza sul lavoro, quali il Servizio di Prevenzione e Sicurezza negli Ambienti di Lavoro (SPSAL) delle Aziende Unità Sanitarie Locali della Regione Emilia-Romagna, l'Ispettorato del Lavoro di Bologna, i Vigili del Fuoco dell'Emilia-Romagna, l'Ordine degli Ingegneri della Provincia di Bologna, la Direzione regionale di INAIL.

Il progetto Banca delle Soluzioni si propone di individuare lo stato dell'arte in termini di soluzioni tecnologiche, sia automatiche che manuali, presenti sul mercato o in via di prototipazione e successiva commercializzazione, il cui impiego è in grado di sostituire o affiancare l'operatore nelle attività rischiose, migliorando così le condizioni di lavoro e riducendo o eliminandone il rischio. Se inizialmente l'attenzione era rivolta alle soluzioni tecnologiche per ridurre i rischi in ambienti confinati e i rischi da sovraccarico biomeccanico, nel 2021 il progetto si è ampliato per includere il rischio microclima, offrendo strumenti per misurare e ottimizzare le condizioni ambientali nei luoghi di lavoro e ad oggi è in corso l'ampliamento al settore Logistica. Abbracciando la logica della gerarchia dei controlli anche la Banca delle Soluzioni, a fianco alle soluzioni ingegneristiche e tecniche, affianca

l'introduzione di procedure per agevolare la riduzione dei rischi e della "Banca dei Casi", per indicare l'applicabilità delle soluzioni presenti nella Banca delle Soluzioni.

L'adozione di tecnologie innovative nei vari settori industriali

L'integrazione di tecnologie avanzate nella gestione della sicurezza sul lavoro consente di sviluppare soluzioni sempre più efficaci per ridurre o eliminare i rischi, adattandosi alle specifiche esigenze di ogni settore industriale. L'intelligenza artificiale (AI) e l'Internet of Things (IoT), insieme a sensori biometrici e dispositivi indossabili, permettono di raccogliere e analizzare dati in tempo reale, monitorando costantemente le condizioni ambientali e fisiche dei lavoratori e le eventuali interferenze tra operatori e attrezzature (macchine e veicoli). Queste informazioni vengono utilizzate per migliorare l'ergonomia delle postazioni di lavoro, il microclima e le condizioni logistiche e attivare autonomamente meccanismi di protezione, incrementando sicurezza e benessere. In questo ambito si annoverano alcune tecnologie "no-man entry" per le attività in ambienti confinati, alcune soluzioni di progettazione di postazioni di lavoro intelligenti, alcuni Dispositivi di Protezione Collettiva (DPC) e DPI.

Tecnologie "no-man entry" per le attività in ambienti confinati

Di seguito sono riportate alcuni esempi di tecnologie, inserite nella Banca delle Soluzioni e relative a diversi settori lavorativi, che permettono l'esecuzione di lavori in ambienti confinati mantenendo l'operatore al di fuori dell'ambiente stesso. Si considerano attività di ispezioni in condotte o reti fognarie eseguite con dispositivi muniti di telecamere e sensori in grado di catturare immagini ed eseguire la profilazione della condotta, creando banche dati per la gestione futura degli interventi (figure 9 e 10).

No man entry | Condotte, reti fognarie, cunicoli tecnologici

Dispositivo per le video ispezioni subacquee in condotte e reti fognarie



Utilizzo
Ispezione subacquea delle condizioni interne delle condotte e delle reti fognarie.

Posizione dell'operatore
Esterno.

Dimensione del serbatoio/condotto/cunicolo
Condizioni di operatività di un dispositivo generico:
Diametri condotte: da 450 fino a 2200 mm.
Punto di accesso: diametro minimo 450 mm.
Livello acqua: da 1/3 a pieno.
Lunghezza video ispezione: fino a 1500m.



Metodo
Il sistema riesce a realizzare un'ispezione di tipo multi-sensor, navigando all'interno della condotta. Il dispositivo è dotato di sensore sonar, inoltre è in grado di catturare immagini video e realizzare una profilazione scanner della condotta piena.

Caratteristiche di mobilità
Sistema mobile, non-climbing.

Caratteristiche di esplosività
Non disponibile.

[bancadellesoluzioni] Per avere informazioni su come trovare questa soluzione, visita il sito www.bancadellesoluzioni.org
CONCORDO O PRODUCO ALTRE SOLUZIONI COME QUESTA? SCRIVI A info@bancadellesoluzioni.org
Scadenza offerta 31/10/2025 e aggiornamento 31/10/2025

Fig. 9 Dispositivo per video ispezioni subacquee

No man entry | Condotte, reti fognarie, cunicoli tecnologici

Sistemi periscopici per ispezioni visive computerizzate



Utilizzo
Ispezioni di condotte per verificare lo stato delle tubazioni danneggiate e individuare condizioni generali, punti danneggiati, natura del danno e altre informazioni utili alla programmazione di un successivo intervento di manutenzione.

Posizione dell'operatore
Esterno.

Dimensione del serbatoio/condotto/cunicolo
Qualsiasi diametro minimo che consenta l'ingresso del dispositivo.
Autonomia di lavoro: 3 ore continue.



Metodo
Questi sistemi si prestano all'ispezione di pozzi, vasche e serbatoi, consentendo il controllo di cavità non altrimenti accessibili. La video ispezione è controllata in remoto e può avvenire mediante telecamera rotante filoguidata, la quale cattura le immagini ad alta definizione direttamente all'interno della condotta. L'impiego di sonde, generatori e rilevatori di campi elettromagnetici consente un servizio di rilevamento di tubazioni metalliche e non. I dati rilevati possono essere raccolti e visualizzati su documenti audiovisivi e cartografici, permettendo così di creare banche dati per la gestione degli interventi. Lo spostamento della navicella nelle tubazioni avviene con sistema di avanzamento a spinta o motorizzato.

Caratteristiche di mobilità
Sistema mobile, non-climbing.

Caratteristiche di esplosività
Alcuni dispositivi sono certificati Explosion Proof, abilitati a lavorare in ambienti saturi di vapori infiammabili ed esplosivi.

[bancadellesoluzioni] Per avere informazioni su come trovare questa soluzione, visita il sito www.bancadellesoluzioni.org
CONCORDO O PRODUCO ALTRE SOLUZIONI COME QUESTA? SCRIVI A info@bancadellesoluzioni.org
Scadenza offerta 31/10/2025 e aggiornamento 31/10/2025

Fig. 10 Videocamera per ispezioni in condotte

No man entry | Attività di scavo

Microtunneling teleguidato con talpa

Utilizzo
Realizzazione di canalizzazioni sotterranee e posa di reti fognarie.

Posizione dell'operatore
Esterno.

Dimensione del serbatoio/condotta/cunicolo
Adatto per la realizzazione di condotte per la rete fognaria.



Metodo
Tecnologia no dig. Testa perforante e asse muovono entrambi in modo rotatorio. La posa delle condotte avviene attraverso un unico pozzo di spinta. La traiettoria è controllata elettronicamente.

Caratteristiche di mobilità
Sistema fisso, non-climbing.

Caratteristiche di esplosività
Non disponibile.

[bancadelle soluzioni]

Per avere informazioni su come trovare questa soluzione, visita il sito www.bancadelle soluzioni.org
 CONSIGLIO O PRODUCO AL TRE SOLUZIONI COME QUESTA? SCRIVA A info@bancadelle soluzioni.org
 Scheda rivista il 15/10/2024 e aggiornata il 01/09/2022

Fig. 11 Microtunneling teleguidato con talpa

No man entry | Cisterne e serbatoi

Drone per l'ispezione di ambienti confinati

Utilizzo
Ispezione delle condizioni interne delle condotte e delle reti fognarie.

Posizione dell'operatore
Esterno.

Dimensione del serbatoio/cisterna
Variabili in funzione del dispositivo utilizzato.



Metodo
Il dispositivo è costituito da un veicolo radiocomandato derivato dall'ambito militare e utilizzato per diverse applicazioni in campo civile e industriale. Il drone è in grado di raggiungere posizioni di osservazione privilegiate o difficilmente raggiungibili, consentendo all'operatore di svolgere le ispezioni a distanza e senza compromettere la propria sicurezza. Grazie al drone è possibile compiere ispezioni visive di condotte o altri ambienti di difficile accesso. La gabbia consente di urtare pareti senza il rischio di rompersi e senza modificare la traiettoria del drone, specialmente in ambienti bui. Il dispositivo è in grado simultaneamente di registrare e trasmettere a terra immagini in HD ed IR. Le luci LED consentono di operare in ambienti totalmente privi di illuminazione. La gabbia della macchina in figura ha un diametro di 42cm che consente l'ingresso nei più comuni passi d'uomo. Gli ambienti in cui questo strumento viene principalmente utilizzato sono le cisterne ed i serbatoi industriali, può essere utilizzato anche per ambienti confinati all'interno di navi, silos, condotte, reti fognarie e tubazioni in genere.

Caratteristiche di mobilità
Sistema mobile, non-climbing.

Stato della cisterna
Out-of-service.

Caratteristiche di esplosività
Non ATEX.

[bancadelle soluzioni]

Per avere informazioni su come trovare questa soluzione, visita il sito www.bancadelle soluzioni.org
 CONSIGLIO O PRODUCO AL TRE SOLUZIONI COME QUESTA? SCRIVA A info@bancadelle soluzioni.org
 Scheda rivista il 15/10/2024 e aggiornata il 21/02/2022

Fig. 12 Drone per l'ispezione di ambienti confinati

Per le attività di scavo si considera l'esempio del microtunneling teleguidato con talpa (figura 11) in cui il microtunneller è guidato dall'esterno mediante una consolle di comandi, ubicata in un container, che consente di impostare e controllare i parametri di avanzamento in funzione del terreno attraversato. Infine, si riporta la scheda del drone per ispezione di ambienti confinati (figura 12), principalmente utilizzato in cisterne e serbatoi, in grado di registrare e trasmettere a terra immagini del luogo da ispezionare, evitando l'ingresso dell'operatore in un luogo impervio e buio.

Postazioni di lavoro intelligenti

Le postazioni di lavoro intelligenti rappresentano una delle soluzioni più innovative per ottimizzare l'ergonomia e la sicurezza nelle linee di assemblaggio, come si evince dalla scheda tecnica corrispondente riportata in Figura 13. Queste postazioni sono progettate per adattarsi automaticamente alle caratteristiche fisiche dell'operatore, regolando in tempo reale elementi come l'altezza, la profondità e la disposizione degli strumenti, in conformità con le linee guida dell'antropometria. Questo adattamento avviene grazie all'uso di sistemi di telecamere che rilevano i dati biometrici dell'operatore, consentendo una personalizzazione immediata della postazione. La tecnologia alla base di queste postazioni intelligenti integra l'Intelligenza Artificiale (AI) e l'Internet delle Cose (IoT) per monitorare e analizzare costantemente le condizioni di lavoro. I sensori biometrici e i dispositivi indossabili raccolgono dati in tempo reale, permettendo di monitorare le condizioni ambientali e fisiche, ottimizzare l'ergonomia e attivare autonomamente meccanismi di protezione. Queste soluzioni avanzate rispondono alle esigenze di un ambiente di lavoro dinamico, garantendo produttività e benessere. Esse permettono infatti di ottimizzare il flusso di lavoro, consentono di monitorare in tempo reale i progressi e di migliorare la gestione della produzione. Inoltre, l'integrazione di sensori biometrici e algoritmi avanzati consente alle postazioni di lavoro intelligenti di adattarsi automaticamente alle caratteristiche fisiche dell'operatore, ottimizzandone l'ergonomia. Questi sistemi regolano l'altezza del piano di lavoro, l'inclinazione degli schermi e la disposizione degli strumenti, riducendo il rischio di infortuni muscoloscheletrici e aumentando il

comfort dell'operatore, specialmente in ambienti di lavoro ad alta intensità. In sintesi, le postazioni di lavoro intelligenti rappresentano una convergenza tra tecnologia avanzata e ergonomia, offrendo soluzioni personalizzate che migliorano la sicurezza, l'efficienza e il benessere degli operatori nelle linee di assemblaggio.

Metalmecanica | Progettazione delle aree di lavoro

Stazioni di assemblaggio assistite

Descrizione
Assemblaggio di componenti.

Modalità d'uso
La postazione di lavoro intelligente integra diverse funzionalità progettate per ottimizzare l'efficienza operativa e facilitare l'interazione tra operatore e macchina. Utilizzando la tecnologia RFID, esse identificano automaticamente i pezzi in arrivo e controllano i dati necessari per la produzione, fornendo assistenza operativa durante il montaggio tramite proiezione visiva e istruzioni lineari. I sistemi joko-yoko generano un unico corretto degli strumenti e bloccati in caso di errori, monitorando anche i parametri di qualità in tempo reale per una risposta immediata a deviazioni. Queste postazioni si riconfigurano in base all'efficienza e alle esigenze fisiche degli operatori, migliorando comfort e sicurezza, mentre la flessibilità degli strumenti hardware integrabili e la collaborazione con robot consentono un adattamento continuo alle necessità produttive.

Caratteristiche tecniche
Sistemi progettati in base alle esigenze di produzione. Equipaggiati con videocamere 2D per la lettura dei movimenti delle mani dell'operatore e sistemi RFID per identificare i componenti da assemblare. La postazione è progettata per lavorare in sinergia con robot collaborativi, migliorando l'efficienza e la produttività nel processo di assemblaggio. La soluzione è scalabile, permettendo l'aggiunta di moduli o funzionalità in base all'evoluzione delle necessità operative.

Costo
Non disponibile.



[bancadelle soluzioni]

Per altre informazioni o per richiedere un preventivo, visitate il sito www.bancadelle soluzioni.it
CONSIGLIO PRODUCT A.I.M.E. SOLUZIONI COME QUESTE AI SOGNI E www.bancadelle soluzioni.it
Stato: creato il 28/09/2023 e aggiornato il 20/10/2024

Fig. 13 Stazione di assemblaggio assistita

Dispositivi di monitoraggio | Monitoraggio e misurazione microclima

Kit IoT

Descrizione
Registrazione e controllo dei parametri ambientali in tempo reale per poterne correggere le eventuali anomalie e migliorare la qualità ambientale in ambienti moderati, limitando le inefficienze energetiche.

Modalità d'uso
Sistemi integrati per la gestione dell'intero filiera dei dati (coltura, hardware e cloud), caratterizzati da versatilità di canali, Sensori Wireless, Gateway, Cloud e Web Dashboard. I dati elaborati vengono restituiti all'utente sotto forma di applicazione con cui l'operatore può modificare i parametri in tempo reale. In base all'applicazione viene selezionato un protocollo di raccolta dati che consente la rilevazione dei dati ottimali.

Vantaggi

- Soluzione scalabile e personalizzabile
- Installazione e manutenzione possono essere effettuate dal cliente (plug and play)
- Absenza di infrastruttura e cablaggio
- Risultati dati in tempo reale

Svantaggi

- Algoritmi per l'elaborazione dei dati vengono sviluppati sulla base del singolo scenario e pertanto sono esclusi dalla fornitura base.

Caratteristiche tecniche
Sensori wireless personalizzati, le caratteristiche tecniche subiscono delle variazioni. Dato dei sensori: 5-10 anni. Qualità di protezione: IP67. Frequenza di raccolta dati: completamente personalizzabile in base al protocollo di raccolta dati. Trasmissione dati: WiFi / 4G. Stoccaggio dei dati: cloud e offline fino a 2gb. Temperatura di esercizio varia in base alle schede nell'intervallo: -20 / +65°C. Range di umidità varia in base alle schede: 0 / 95%.

Manutenzione
Sostituzione delle pile dei sensori.

Conformità alle norme
Gateway certificata CE.

Costo
Acquisto 1.500-2000€ centralina con 10 sensori ambientali/energetici a scelta
cloud 50-60€ al mese
licenziazione 450€ al giorno
Manutenzione straordinaria 450€ al giorno



[bancadelle soluzioni]

Per altre informazioni o per richiedere un preventivo, visitate il sito www.bancadelle soluzioni.it
CONSIGLIO PRODUCT A.I.M.E. SOLUZIONI COME QUESTE AI SOGNI E www.bancadelle soluzioni.it
Stato: creato il 14/04/2023 e aggiornato il 13/09/2024

Fig. 14 Kit IoT per il monitoraggio e la modifica dei parametri ambientali in tempo reale

I sistemi di protezione collettiva (DPC) sono progettati per garantire la sicurezza dei lavoratori attraverso la protezione di aree o processi specifici. Grazie all'impiego di sensori avanzati, AI e IoT, questi sistemi monitorano continuamente le condizioni ambientali e le attività lavorative, rilevando potenziali pericoli come temperature estreme o la presenza di sostanze nocive.

Un esempio di queste soluzioni è rappresentato dai kit IoT per il monitoraggio e la modifica dei parametri ambientali in tempo reale, come illustrato in Figura 14. Questi kit si compongono di una centralina che raccoglie i dati ambientali tramite sensori wireless posizionati strategicamente. I dati vengono inviati a un gateway e poi al cloud, dove vengono elaborati. L'operatore può visualizzarli tramite una web dashboard e, se necessario, modificare i parametri in tempo reale tramite un app. Queste soluzioni variano in base ai sensori utilizzati e ai campi di applicazione. Ad esempio, i sensori di temperatura e umidità sono tra i più utilizzati nella gestione degli edifici, in particolare per regolare il riscaldamento e la climatizzazione (HVAC) in base alle condizioni ambientali e alla presenza di persone, evitando sprechi energetici e prevenendo problemi di umidità e muffa. In sintesi, l'integrazione di tecnologie avanzate nei sistemi di protezione collettiva, come l'uso di sensori intelligenti e soluzioni IoT, rappresenta un passo significativo verso ambienti di lavoro più sicuri ed efficienti, rispondendo alle esigenze di un'industria sempre più attenta al benessere e alla protezione dei suoi lavoratori.

Dispositivi di protezione individuale (DPI) avanzati:

L'innovazione ha portato allo sviluppo di DPI più efficienti e interconnessi. A questo proposito, la Banca delle Soluzioni ha mappato alcuni strumenti di rilevamento gas fissi e portatili per la sicurezza

ed ergonomiche, di sistemi di protezione collettiva e DPI intelligenti. Tuttavia, per garantire un utilizzo responsabile di queste innovazioni, è fondamentale accompagnarle con un adeguato quadro normativo che tuteli i lavoratori. In questo contesto, il progetto "Banca delle Soluzioni" rappresenta un valido supporto per le aziende, promuovendo l'adozione di tecnologie avanzate finalizzate alla protezione della salute e sicurezza dei lavoratori, contribuendo così a creare ambienti di lavoro più sicuri ed efficienti. Investire in soluzioni basate sull'AI non solo protegge i lavoratori, ma migliora anche l'efficienza e la sostenibilità delle attività aziendali. Infine, mentre l'AI offre enormi vantaggi in termini di prevenzione degli infortuni, è importante considerare anche le implicazioni etiche e sociali di queste tecnologie. È essenziale garantire che l'uso dell'AI nella sicurezza sul lavoro rispetti i diritti e la dignità dei lavoratori e che venga impiegato in modo responsabile e trasparente.

Tra i rischi associati all'utilizzo dell'AI si annoverano l'intensificazione del lavoro e la maggiore pressione sulle prestazioni, la limitazione dell'autonomia professionale dei lavoratori e la preoccupazione in materia di privacy.

In conclusione, l'integrazione dell'AI nella sicurezza sul lavoro rappresenta una grande opportunità per migliorare la protezione dei lavoratori e aumentare l'efficienza aziendale e con il giusto approccio e l'impegno per un utilizzo etico e responsabile, l'AI può contribuire in modo significativo a creare ambienti di lavoro più sicuri e salutaris per tutti.

Bibliografia

- Berastegui P. 2024, Artificial intelligence in Industry 4.0, implication for occupational safety and health – Report 2024. European Trade Union Institute.
- Botti L., M., Melloni R., 2022, Accidents at work: an insight into logistics operations, XXVII Summer School "Francesco Turco", Riviera dei Fiori 7-9 Settembre 2022.
- EU-OSHA (Agenzia Europea per la sicurezza e la salute sul lavoro), 2025, "Verso sistemi di gestione del personale basati su intelligenza artificiale e algoritmi per luoghi di lavoro più produttivi, più sicuri e più sani".
- EU-OSHA (Agenzia Europea per la sicurezza e la salute sul lavoro), 2024, "Principles for design and development – smart digital systems for improving workers safety and Health"
- El-Helaly M., 2024, Artificial Intelligence and Occupational Health and Safety, Benefits and Drawbacks, Med Lav 2024, 115 (2).
- NIOSH (National Institute for Occupational Safety and Health), Hierarchy of Controls
- Shah I.A. and Mishra S., 2024, Artificial intelligence in advancing occupational health and safety: an encapsulation of developments, Journal of Occupational Health, 2024, 66 (1).
- UNI 11958:2024 "Ambienti confinati e/o sospetti di inquinamento – Criteri per l'identificazione dei pericoli e la valutazione dei rischi", 14 novembre 2024.

Sitografia

- https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_it
- <https://www.novasafe.it/it/articolo/550/ai-e-sicurezza-sul-lavoro-innovazioni-e-sviluppi-come-lintelligenza-artificiale-trasforma-la-prevenzione-degli-infortuni-nei-luoghi-di-lavoro.html>
- <https://www.assocarenews.it/infermiere-di-famiglia-e-intelligenza-artificiale-qual-futuro-per-lassistenza-ai-pazienti/>
- <https://www.agendadigitale.eu/sanita/riabilitazione-senza-barriere-lia-ridisegna-lassistenza-domiciliare/>

- <https://www.novasafe.it/it/articolo/550/ai-e-sicurezza-sul-lavoro-innovazioni-e-sviluppi-come-lintelligenza-artificiale-trasforma-la-prevenzione-degli-infortuni-nei-luoghi-di-lavoro.html>
- <https://safetyforge.it/smartdpi/>
- <https://kiwitron.com/it/>
- <https://it.emcelettronica.com/limpatto-delle-tecnologie-indossabili-sulla-moderna-assistenza-sanitaria>
- <https://www.bancadellesoluzioni.org/it/>

1.5 L'utilizzo di piattaforme digitali e la salute e sicurezza dei lavoratori: l'esempio dei riders

Francesca Seghezzi

Associazione Ambiente e Lavoro

Negli ultimi anni, il lavoro nel settore del food delivery ha conosciuto una crescita esponenziale, trainata dalla diffusione delle piattaforme digitali e da un modello di consumo sempre più rapido e frammentato. Già nel 2021, oltre 570.000 persone avevano svolto attività lavorative tramite piattaforme digitali in Italia, con circa 160.000 rider attivi nel solo ambito del food delivery. Il profilo prevalente è quello di un giovane uomo, con un'età media di circa 30 anni e una significativa presenza di lavoratori migranti: a Milano, ad esempio, oltre il 60% dei rider è straniero.

Il mercato del food delivery, nel frattempo, ha continuato a espandersi. Nel 2022 ha generato un volume d'affari pari a 1,8 miliardi di euro, circa il 44% del mercato online Food&Grocery italiano. Nel 2024, almeno il 76% della popolazione italiana risulta raggiunta da almeno una piattaforma di food delivery, incluse molte aree urbane medie e piccole. Questa diffusione capillare, unita alla logica delle consegne rapide e continuative, rende centrale il ruolo dei rider e impone una riflessione seria sulle loro condizioni di lavoro, in particolare in tema di salute e sicurezza.

1.5.1 Rischi fisici: tra strada, carichi e inquinamento

I rider operano principalmente su strada, utilizzando biciclette, scooter o monopattini. I rischi di incidenti stradali sono tra i più evidenti, alimentati da ritmi serrati, traffico urbano e tempi di consegna sempre più compressi. A ciò si aggiungono i problemi muscolo-scheletrici, dovuti al trasporto continuativo di carichi pesanti e a posture scorrette protratte nel tempo. Si registrano frequentemente dolori a schiena, collo e arti superiori, oltre a tendiniti e disturbi cronici.

Un ulteriore fattore critico è l'esposizione a condizioni meteorologiche avverse. I rider lavorano in tutte le stagioni, sotto pioggia, neve o caldo estremo, senza che vi siano obblighi effettivi per le piattaforme di fornire dispositivi protettivi adeguati. Inoltre, l'esposizione a inquinamento atmosferico (smog, polveri sottili) aumenta il rischio di patologie respiratorie, malattie cardiovascolari, e disturbi neurologici.

1.5.2 Infortuni e incidenti tra i rider

Il lavoro del rider è caratterizzato da un elevato rischio di infortuni, in particolare incidenti stradali. Con l'obbligo di assicurazione INAIL in vigore dal 2020, oggi disponiamo di dati ufficiali. Nel triennio 2021–2023, l'INAIL ha registrato 1.337 denunce di infortunio da parte di rider, di cui 7 con esito mortale. Il profilo prevalente è quello di un uomo giovane (92% maschi, 60% under 35).

Gli incidenti si concentrano principalmente in quattro regioni: Lazio, Lombardia, Sicilia e Piemonte, che da sole rappresentano il 61% dei casi. Circa il 77% degli infortuni avviene "in occasione di lavoro", ossia durante le consegne, e la quasi totalità dei decessi rientra in questa categoria.

Secondo fonti sindacali e giornalistiche, i numeri reali potrebbero essere significativamente più alti. Si stima infatti che almeno il 60% degli incidenti non venga denunciato. Tra il 2021 e il 2023 sono stati almeno 12 i rider deceduti durante l'attività lavorativa, e altri 7 decessi sono stati registrati nel solo 2024.

Questa sottodenuncia è spesso legata a un inquadramento lavorativo debole, alla scarsa consapevolezza dei propri diritti o al timore di perdere l'accesso alla piattaforma. È evidente che il lavoro dei rider, sebbene centrale per un settore in crescita, resta tra i più pericolosi e meno tutelati.

1.5.3 Rischi psicosociali: pressione algoritmica e isolamento

Accanto ai rischi fisici, il lavoro dei rider comporta numerosi rischi psicosociali. La pressione algoritmica – ovvero il controllo esercitato dalle piattaforme tramite app che monitorano tempi, percorsi e performance – può generare ansia e stress costanti. I rider che non rispettano le tempistiche o rifiutano le consegne rischiano penalizzazioni, fino alla disattivazione.

Il lavoro individuale e frammentato comporta inoltre isolamento sociale. I rider non hanno colleghi, non accedono a spazi comuni e spesso non conoscono i propri referenti. Questo porta a una condizione di invisibilità che rende ancora più difficile organizzarsi o difendersi collettivamente. Alcuni, soprattutto nelle fasce orarie serali, sono anche esposti a rischi di aggressione o furto.

1.5.4 Tutele e prospettive normative

Sul piano normativo, la Legge n.128/2019 ha introdotto alcune tutele minime per i rider, come la copertura INAIL e l'obbligo per le piattaforme di garantire una retribuzione che non sia esclusivamente a cottimo. Tuttavia, molti rider sono ancora formalmente lavoratori autonomi.

La giurisprudenza ha fatto alcuni passi avanti: diverse sentenze (Palermo 2022 e 2023, Torino 2024) hanno riconosciuto la necessità di valutare i rischi legati al calore, di consegnare il DVR ai rider, e di rendere trasparenti gli algoritmi di gestione.

Due importanti pronunce del Tribunale e della Corte d'Appello di Milano hanno rafforzato il riconoscimento delle tutele per i rider.

La sentenza n. 3237/2023 del Tribunale di Milano ha riconosciuto che la prestazione lavorativa dei rider rappresenta una collaborazione etero-organizzata, soggetta alle regole del lavoro subordinato. In particolare, due società di food delivery sono state condannate a versare i contributi alla Gestione lavoratori dipendenti per il periodo in cui i rider hanno effettuato le consegne.

La Corte d'Appello di Milano, con sentenza del 9 febbraio 2023, ha confermato la natura subordinata del rapporto di lavoro di un rider, riconoscendo l'applicazione della disciplina del lavoro subordinato a tempo pieno, con inquadramento nel sesto livello del CCNL Commercio e 14 mensilità. Questa sentenza rappresenta un precedente rilevante nell'affermazione dei diritti dei rider come lavoratori subordinati a tutti gli effetti.

A livello europeo, la nuova Direttiva UE sul lavoro tramite piattaforma (approvata a fine 2023) prevede il principio della presunzione di subordinazione: sarà la piattaforma a dover dimostrare che un rider è davvero autonomo. L'Italia dovrà recepire la direttiva entro il 2026.

1.5.5 Conclusione

I rider sono tra i lavoratori più rappresentativi dell'economia digitale contemporanea: iperconnessi, monitorati, ma spesso invisibili e vulnerabili. La loro sicurezza non può essere lasciata all'arbitrio delle piattaforme o all'adattabilità individuale. Garantire salute e sicurezza per questi lavoratori significa ridefinire il concetto di lavoro dignitoso nell'era degli algoritmi.

1.6 Presentazione progetto REKON per la prevenzione di incidenti sul lavoro da interferenze macchina/lavoratore

Wolfgango Pirelli

Associazione Ambiente e Lavoro

REKON: Progetto Inail per promuovere Tecnologie abilitanti per il monitoraggio degli elementi di contesto (Operatore-Macchina-Ambiente) per la prevenzione di incidenti sul lavoro (in allegato il progetto integrale)

Il progetto Reckon ha l'obiettivo di introdurre una tecnologia bluetooth che permetta di rilevare le zone/situazioni critiche aziendali (interferenza fra macchine e persone) e quindi dare elementi per attuare misure mirate di prevenzione degli incidenti.

La sperimentazione ha coinvolto 3 aziende (2 nella provincia di Lecco, 1 nella provincia di Bergamo). Solo 1 azienda, dopo la sperimentazione ha mantenuto attivo il sistema che ha però evidenziato sia problemi che potenzialità.

Sono stati coinvolti il Politecnico di Lecco, l'associazione industriale Confapi di Lecco ed i risultati sono stati presentati in un convegno a cui ha partecipato anche l'ATS di Lecco. All'interno delle aziende si è cercato il coinvolgimento delle RSU/RLS e delle Organizzazioni sindacali territoriali ma incontrando difficoltà.

La sperimentazione consisteva nel testare questa tecnologia attraverso precise rilevazioni usando diverse modalità. Le rilevazioni non solo avevano una funzione preventiva nel momento stesso in cui si svolgono le attività lavorative, ma i dati raccolti servivano ad una analisi più complessiva circa i rischi presenti in azienda.

Problematiche e potenzialità emerse:

- il mantenimento dei dispositivi è abbastanza impegnativo, ma questo limite potrebbe essere superato passando a tecnologie più efficienti e ad una migliore personalizzazione dei dispositivi stessi;
- la sperimentazione ha incontrato resistenze sindacali, legate all'utilizzo dei dati che emergono nell'uso di questi dispositivi e che rischiano di essere utilizzati quali strumenti di controllo del lavoro. Andrebbero su questo punto approfonditi gli strumenti tecnologici adottati ed il loro sviluppo non invasivo così come andrebbero rafforzate le modalità di relazioni sindacali finalizzate al pieno coinvolgimento consapevole dei lavoratori, come del resto previsto dall'art. 4 dello Statuto dei lavoratori (L. 300/70);
- dove si è sperimentato il progetto, l'azienda è stata costretta a fare i conti con un nuovo sistema di rilevazione dei pericoli che ha permesso di "imparare" un nuovo approccio alla prevenzione tenendo conto di variabili che soltanto l'utilizzo di strumenti tecnologici finalizzati al monitoraggio del contesto consente di rilevare. Ad esempio, se il lavoratore si avvicina troppo ad una macchina o se nell'ambiente in cui lavora sono presenti sostanze inquinanti.

1.7 Integrazione dell'intelligenza artificiale per la sicurezza nei contesti industriali

Andrea Filippini

Co-Founder, President & CEO di Kiwitron S.p.A.

1.7.1 Premessa

L'adozione dell'intelligenza artificiale (AI) in ambito industriale è spesso accolta con diffidenza, percepita come estranea ai metodi consolidati e fonte di incertezze organizzative, soprattutto nel campo della sicurezza. È quindi importante chiarire che queste tecnologie non mirano a sostituire le persone, ma a supportarle nei momenti in cui l'attenzione può calare, migliorando la prevenzione e l'efficienza.

Molte aziende non utilizzano alcun sistema per ridurre i rischi di infortunio e, solo dopo aver scoperto le soluzioni disponibili, si rendono conto delle opportunità mancate. L'AI applicata alla sicurezza industriale non sostituisce il lavoro umano, ma lo affianca. Anche un lieve calo dell'attenzione può compromettere la prontezza dell'operatore di fronte a un rischio, ed è proprio in questi momenti che la tecnologia può intervenire a supporto. È in questi momenti che la tecnologia può fare la differenza. L'attenzione non è costante, e i sistemi intelligenti aiutano a ridurre l'impatto delle fluttuazioni cognitive. Anche chi causa involontariamente un incidente può subire ripercussioni emotive: prevenire significa tutelare tutti.

1.7.2 Analisi del rischio e applicazioni alle macchine mobili

Il caso studio è maturato, in una azienda, a seguito dell'avvio della sostituzione progressiva dei carrelli elevatori frontali con transpallet. Nella situazione lavorativa abituale con l'utilizzo dei carrelli elevatori il pericolo principale era rappresentato dal possibile schiacciamento di una persona mentre il nuovo scenario operativo, con l'uso dei transpallet, ha fatto emergere situazioni differenti, come ad esempio il rischio di fratture alla caviglia. Ai fini di attuare una attività di prevenzione ci si è rivolti ad una azienda ad alta tecnologia¹⁹ per valutare come l'intelligenza artificiale potesse essere utilizzata per evitare l'insorgenza delle nuove tipologie di rischio.

Analizzato il nuovo scenario sono state sviluppate soluzioni specifiche: tale approccio, volto a trasformare ogni criticità in una proposta progettuale, è alla base di una metodologia che, consolidata nel tempo, ha contraddistinto sin dalle prime fasi la storia dell'azienda K.

La prima soluzione sviluppata è il risultato di un lungo e articolato percorso, atto a comprendere come l'AI potesse essere impiegata concretamente nella salvaguardia della vita umana nei contesti industriali. Tradurre questa visione in una tecnologia affidabile ha richiesto investimenti significativi e un costante confronto con i clienti finali, incontrando i quali è emersa con frequenza una tensione ricorrente: se da un lato i responsabili HSE evidenziano la necessità di garantire standard di sicurezza più elevati, dall'altro i responsabili della produzione tendono ad associare le misure di sicurezza ad un inevitabile calo della produttività. Si è scelto di affrontare questo nodo sviluppando soluzioni in grado di coniugare entrambe le esigenze: la riduzione degli incidenti e il mantenimento – o persino il miglioramento – dell'efficienza operativa.

Il principio è semplice ma fondamentale: un operatore che lavora in sicurezza, senza stress, guida con maggiore tranquillità e svolge il proprio lavoro in modo più efficace. La tecnologia sviluppata si

¹⁹ Kiwitron azienda specializzata in sviluppo e produzione di hardware e software per veicoli di lavoro nelle aree industriali.

basa sull'impiego dell'AI per il riconoscimento di persone e ostacoli in movimento. Non vengono utilizzati strumenti convenzionali come TAG o radar, ma algoritmi visivi avanzati, addestrati per identificare la struttura morfologica del corpo umano – testa, tronco, braccia, gambe – e per calcolarne la distanza dal mezzo in movimento. In presenza di una situazione potenzialmente pericolosa, il sistema interviene automaticamente rallentando il veicolo, prevenendo l'impatto.

1.7.3 Gestione dinamica della velocità e produttività

Un altro ambito di applicazione dell'AI riguarda la gestione automatizzata delle velocità operative dei mezzi. In molti impianti produttivi e logistici, i carrelli elevatori sono limitati a una velocità massima di 6 km/h per motivi di sicurezza, nonostante possano viaggiare a 14 km/h. Questo compromesso incide negativamente sulla produttività.



Le tecnologie intelligenti consentono di definire velocità differenziate in funzione dell'ambiente circostante: è possibile autorizzare una velocità di 10 km/h all'esterno degli stabilimenti, riducendola in automatico a 8 km/h negli spazi interni e a 2 km/h in caso di rischio per la presenza di pedoni. Questo modello di gestione dinamica consente di mantenere elevati standard di sicurezza migliorando l'efficienza operativa.

Il sistema, inoltre, è in grado di leggere codici QR o sensori di prossimità disposti nei vari punti dello stabilimento, modificando la velocità del mezzo in base alla zona attraversata. Tale adattamento si traduce in un incremento tangibile della produttività, riducendo i tempi di percorrenza nei tratti sicuri e limitando il rischio nei punti critici.

Questa capacità di adattamento si accompagna a una funzione fondamentale: la raccolta sistematica dei dati. Da ogni interazione tra mezzo e ambiente, infatti, si generano informazioni preziose che alimentano analisi sempre più raffinate del rischio operativo.

1.7.4 Heatmap e analisi dei dati

Ogni situazione in cui un mezzo si avvicina a un ostacolo, a un pedone o a un'area a rischio viene rilevata e geolocalizzata, generando mappe di calore che evidenziano le zone più critiche dello stabilimento. Le aziende possono usare questi dati per rivedere la viabilità interna, introducendo ad esempio sensi unici. Le heatmap sono utili soprattutto nei contesti con turni su più fasce orarie, dove i rischi possono variare tra giorno e notte a causa di percorsi diversi o minore supervisione.

1.7.5 Sistemi digitali e verifica operativa

La prevenzione richiede anche strumenti adeguati per la gestione delle attività quotidiane. Le checklist pre-operative sono spesso cartacee o assenti: digitalizzarle consente un controllo più affidabile e centralizzato, in modo da monitorare costantemente lo stato della flotta, individuare guasti e anomalie prima che possano diventare causa di infortuni.

1.7.6 Co-progettazione e risposta a esigenze specifiche

L'attività di ricerca e sviluppo è stata orientata all'ascolto delle esigenze specifiche del lavoro. Un caso concreto riguarda l'aumento di infortuni legati all'utilizzo dei transpallet con pedana, causati in parte da condotte scorrette degli operatori, come la guida con il piede fuori dal piano di appoggio.

In risposta, è stato sviluppato un sistema con sensori perimetrali capace di rilevare ostacoli lungo il percorso e di distinguere l'utilizzo improprio del mezzo. Questa soluzione agisce in modo proattivo, rallentando la macchina e allertando l'operatore in caso di comportamento non conforme, contribuendo così a ridurre i rischi legati alla distrazione, allo stress ed alle casualità gestionali.

1.7.7 Altri scenari applicativi

L'AI è impiegata anche per evitare collisioni tra mezzi in incroci ciechi, regolando dinamicamente la velocità in base alla direzione di avvicinamento. Altri ambiti includono:

- **Gru a ponte (carriponte):** i sistemi monitorano l'area sottostante, attivando segnali se rilevano persone nelle zone delimitate.
- **Rulli trasportatori:** nei settori del riciclo e smaltimento dei rifiuti, si sono verificati casi in cui operatori hanno perso i sensi e sono stati trascinati fino a tramogge o compattatori. Le soluzioni adottate con l'uso dell'Intelligenza Artificiale rilevano tempestivamente la presenza umana e attivano un allarme, permettendo il blocco del rullo in tempo utile.

1.7.8 Visione strategica e prospettive future

L'adozione dell'AI in ambito industriale rappresenta oggi una delle principali leve per l'evoluzione dei modelli di sicurezza. Le esperienze, in corso di attuazione, dimostrano che è possibile coniugare tutela della salute, prevenzione degli infortuni ed efficienza operativa attraverso soluzioni tecnologiche avanzate, sviluppate in stretta collaborazione con i lavoratori ed i responsabili aziendali.

L'utilizzo dell'intelligenza artificiale non può essere lasciato ad un sistema informatico che ne riduca la sua operatività a semplici algoritmi ma serve una progettazione con un team dalle competenze trasversali che vanno dall'ingegneria informatica all'elettronica e all'intelligenza artificiale, basate sulla ricerca e sull'innovazione, con l'obiettivo di contribuire concretamente alla sicurezza delle persone nei luoghi di lavoro.

2 Intelligenza artificiale e valutazione dei rischi

2.1 Valutazione dei rischi, il fattore umano e le nuove frontiere dell'intelligenza artificiale

Rita Somma

Docente di Medicina del Lavoro - Dipartimento di Neuroscienze Università degli Studi di Padova, Consulente H&S, vicepresidente Aifos.

2.1.1 Premessa

I lavoratori non sempre sono esposti allo stesso livello di rischio per la salute e la sicurezza: alcuni gruppi specifici di lavoratori possono essere esposti a maggiori rischi (o soggetti a particolari esigenze). Una evidenza cristallizzata inequivocabilmente, nero su bianco, sia dalla direttiva quadro dell'UE 89/391/CEE che dal Decreto Legislativo 9 aprile 2008, n. 81, Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro (G.U. n. 101 del 30 aprile 2008 e smi). Entrambe le norme, infatti, dispongono espressamente che, per garantire l'uniformità di tutela prevenzionistica nei luoghi di lavoro, i datori di lavoro debbano considerare, nella valutazione dei rischi e nella definizione delle misure di tutela, la presenza di gruppi di lavoratori esposti a rischi particolari, come quelli connessi alle differenze di genere, all'età, alla provenienza da altri Paesi e quelli correlati alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di Lavoro (art. 1 e 28 del D. Lgs. 81/08).

L'indirizzo del legislatore appare particolarmente chiaro: per raggiungere lo stesso risultato nel livello essenziale di diritto alla tutela della salute e sicurezza sul lavoro, è necessario considerare le diverse condizioni espositive di partenza, guardando non solo a concetti di rischio assoluti ma anche a variabili relative a caratteristiche particolari dei destinatari dell'azione prevenzionistica, la reale popolazione di lavoratori presenti nell'ambito dell'organizzazione, in sinergia tra loro.

Eppure questo resta un aspetto del disposto legislativo che, seppur rilevante concettualmente, non è spesso visualizzato con l'attenzione che merita, appiattito dalla necessità di calcolabilità probabilistica del rischio, che necessità di eliminare l'entropia, indirizzandosi verso una valutazione dei rischi che considerano generalizzanti "Gruppi omogenei di lavoratori", suddivisi per mansioni, attività, rischi espositivi, etc., dimenticando la specificità legata a queste differenze particolari. Il calcolo ragionieristico del rischio, che accomuna la fisica, l'ingegneria e le scienze sociali, proprio perché può essere applicato a fenomeni disparati: dal fumo, all'energia nucleare, agli incidenti della strada, agli investimenti monetari pretende di essere razionale ma non può esserlo, e non può ancora di più esserlo se declinato genericamente²⁰. Questo è un assunto imprescindibile dal quale partire.

E se dobbiamo dirla tutta, alzando coraggiosamente ancora di più l'asticella, il quadro che considera la variabilità umana nella costruzione di un impianto prevenzionistico diventa ancora più complesso

²⁰ Beck (1989) definisce i calcoli probabilistici come un tipo di etica senza moralità, una moralizzazione tecnologica che pretende di essere razionale ma non può esserlo ("La pretesa della razionalità scientifica di rilevare obiettivamente la pericolosità del rischio si smentisce sempre da sé: da una parte si regge su un castello di carte di assunti speculativi, e si muove esclusivamente nel quadro di enunciati di tipo probabilistico, le cui prognosi in fatto di sicurezza a rigore non potrebbero essere confutate nemmeno dal reale verificarsi degli incidenti. Dall'altra, per poter parlare sensatamente di rischi occorre aver prima assunto una prospettiva orientata sui valori. L'accertamento dei rischi si basa su possibilità matematiche e su interessi sociali, anche e soprattutto quando viene presentato con certezza scientifica").

se scavalchiamo la cornice, allargando gli orizzonti, per guardare alla singola persona (il lavoratore), oltre la targhettizzazione nelle categorie definite per giungere a toccare le capacità e limitazioni caratterizzanti di ogni individuo. Ed oltre ci sono, è quasi pleonastico dirlo, altre differenze che possono impattare sulle condizioni iniziali e, dunque, sull'esposizione al rischio: differenze culturali, di lingua, sociali, cognitive, antropometriche, biomeccaniche, di istruzione, di potere, generazionali, economiche, di stile di vita, etc., da considerarsi anche in prospettiva evolutiva nel tempo²¹.

Ma questa variabilità umana, con la propria specificità eterogenea, sembra, troppo spesso, totalmente assente ingiustificata dalla costruzione delle pratiche prevenzionistiche. Nella realtà, infatti, il modellamento privilegiato è basato sull'immagine stereotipata di un "lavoratore standard", rappresentato generalmente da un maschio di mezza età, di corporatura media, psico-fisicamente normodotato, madrelingua, che riproduce però solo un piccolissimo percentile della varietà della popolazione lavorativa. Le persone reali presentano, infatti, una estrema variabilità psico-fisica, sociale e comportamentale, anche intraindividuale in relazione a processi di invecchiamento, che non può non essere considerata.

Con queste premesse diventa chiaro che l'approccio prevenzionistico non può essere neutrale, ma deve essere attento alla soggettività, in un atteggiamento mentale inclusivo (ndr. della persona), che richiede di conservare la consapevolezza che l'astrazione impersonale della valutazione dei rischi è un'operazione strumentale e, pertanto, nella fase applicativa, è essenziale introdurre nel sistema le variabili che erano state date per costanti, costringendo a ragionare sulla tutela della persona reale, con tutte le sue sfaccettature. Se questo non avviene, il risultato non risolve il problema, oppure il problema non era quello che era stato inizialmente affrontato, con la variabilità umana che tenderà, quasi inevitabilmente, a trasformarsi in diseguaglianze, ossia in vantaggi e svantaggi per le persone e i gruppi che di tali differenze sono portatori.

Con queste premesse, diventa chiaro che i dati che emergono dalla valutazione dei rischi sono importanti ma devono intendersi come punto di partenza e non di arrivo: l'azione prevenzionistica, per essere sostanziale, deve essere "sartorialmente" cucita addosso al destinatario dell'azione di tutela. Eppure, nella realtà, l'approccio della standardizzazione omogeneizzante nella gestione del rischio appare culturalmente difficile da superare. Non aiuta al cambiamento la difficoltà attuativa dovuta alla carenza di strumenti e di metodologie condivise che possano facilitare l'inversione del paradigma in tale direzione.

Da queste considerazioni parto per la mia proposta di analisi, cercando di sollecitare qualche riflessione ma anche una proposta operativa che possa avvalersi di nuove frontiere sfruttando le potenzialità dell'Intelligenza Artificiale, per superare i processi di appiattimento prodotti dall'attuale sistema di gestione della sicurezza.

2.1.2 Valutazione dei rischi e IA

L'IA è già stata sdoganata da tempo per supportare la tutela della salute e della sicurezza sul lavoro: monitoraggio in tempo reale attraverso sensori e videocamere (analisi delle immagini e dei dati provenienti da sensori per individuare comportamenti a rischio, condizioni ambientali pericolose, prevenire collisioni, ad esempio), dispositivi indossabili (Smartwatch e braccialetti intelligenti per monitorare i parametri vitali dei lavoratori, identificare condizioni di sovraccarico fisico, monitorare lo stato di stanchezza dei conducenti, segnalare eventuali anomalie), manutenzione predittiva, formazione, assistenza ai lavoratori (Chatbot e assistenti virtuali), monitoraggio intelligente degli

²¹ R. SOMMA P. FAVARANO, AIFOS https://aifos.org/home/news/int/nostre_attivita/diversity-e-valutazione-dei-rischi

accessi nei cantieri, etc. Molto ancora c'è senz'altro da fare, ma diverse sono le attività di ricerca già avviate ed in corso.

Meno percorsa è stata invece la strada dell'utilizzo dell'AI per contribuire all'Analisi dei rischi ed io vorrei partire proprio da qui, sostenendo la necessità di un approccio epistemologico strumentale della I.A. alla gestione dei rischi in relazione ad uno dei tasselli fondamentale dell'impianto prevenzionistico meno standardizzabile: il fattore umano, oltretutto quello al quale oggi vengono imputati la maggioranza degli infortuni. L'uso dell'IA potrebbe supportare nella valutazione dei rischi e nella definizione delle misure di prevenzione e protezione per considerare anche le caratteristiche di variabilità della reale popolazione di lavoratori.

L'idea potrebbe essere quella di un sistema basato sull'I.A. che consenta di *matchare* il livello di rischio assoluto valutato del documento di valutazione dei rischi con le caratteristiche, capacità e limitazioni eterogenee della popolazione di lavoratori di riferimento per valutare eventuali discrasie espositive, anche con l'obiettivo di adattare le misure di prevenzione alle peculiarità del singolo lavoratore, migliorare l'ambiente di lavoro e le modalità di lavoro per renderlo compatibile ad esigenze di sicurezza e di salute.

Sostanzialmente l'idea è di agire in prevenzione, con il supporto dell'I.A., che diventa così un ulteriore strumento che può essere messo in campo e che, consentendo di analizzare grandi quantità di dati, può quindi supportare nella complessa questione della gestione del rischio in relazione al fattore umano, con la molteplicità degli aspetti che coinvolge, anche in relazione ai risultati degli studi aperti dalle ricerche nel campo delle neuroscienze.

2.1.3 L'intelligenza artificiale, valutazione e gestione dei rischi

L'I.A. potrebbe, pertanto, essere utilizzata per intrecciare i dati della valutazione dei rischi in termini "assoluti" con le variabili complesse "relative" in relazione a caratteristiche particolari della reale popolazione di lavoratori, supportando nell'organizzazione del lavoro e nell'individuazione di misure di prevenzione e protezione "personalizzate", cucite sartorialmente addosso al lavoratore.

Un sistema che utilizza l'I.A. potrebbe, pertanto, inserire nella gestione del rischio le variabilità ergonomiche (fisiche, cognitive, organizzative)²² della popolazione di lavoratori per fornire:

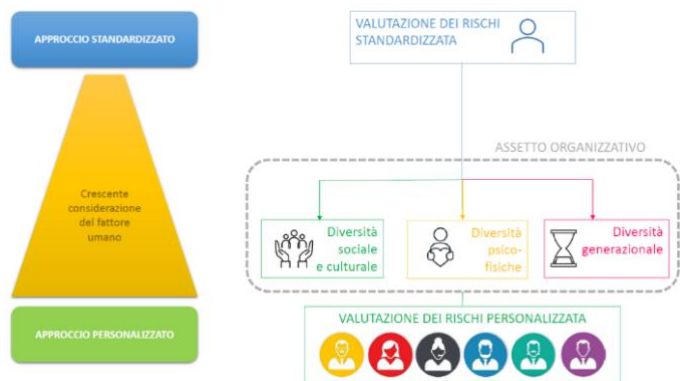
- Valutazione del rischio adattata "soggettivamente" (vedasi prossimo capitolo)
- Dati sull'adeguatezza della risorsa rispetto all'organizzazione del lavoro (natura del compito, preparazione delle attività, carico di lavoro, procedure, strumenti e metodi, ambiente, etc.). (N.B. Ad esempio, potrebbe fornire, anche sulla scorta dei risultati della sorveglianza sanitaria e di altre variabili definite, quali movimenti ergonomici possono essere compiuti o meno da quel lavoratore).
- Indicazioni per eventuali variabili del protocollo sanitario definito dal Medico Competente rispetto al fattore umano.
- Indicazioni per eventuali caratteristiche peculiari di DPI (in base a caratteristiche antropometriche, di sesso, di età, ad esempio, etc.).
- Il fabbisogno specifico di formazione aggiuntivo soggettivo (in base a capacità di apprendimento, lingua, istruzione, abilità, esperienza, etc.). Questo è un punto fondamentale di supporto per l'I.A. (rilevazione del fabbisogno formativo del singolo, inclusiva della persona), che andrebbe percorso. Ne parlo qui: <https://www.puntosicuro.it/informazione-formazione-addestramento-C-56/formazione-per-la-sicurezza-un-abito-prevenzionistico-su-misura-AR-22007/>

- Ed individuare ogni ulteriore azione correttiva necessaria per la gestione soggettiva del rischio.

L'obiettivo primario del progetto ipotizzato è il miglioramento del livello di affidabilità dell'operatore e più in generale del sistema all'interno del quale il singolo lavoratore opera, tenendo conto della complessità di tutti gli elementi con i quali egli si deve interfacciare, che richiede il superamento degli standard, indirizzando verso una valutazione dei rischi (sempre più) "sartoriale" ma anche progettazione, formazione, politiche o procedure a supporto dei lavoratori.

Il sistema con l'utilizzo di I.A. dovrebbe pertanto riuscire a:

- analizzare l'organizzazione del lavoro, il compito e le sue caratteristiche (sostenibilità psico-fisica);
- analizzare l'individuo che deve svolgerlo (competenza e caratteristiche personali);
- individuare eventuali criticità e correttivi (es. fornitura di attrezzature più "ergonomiche", formazione mirata, introduzione di controlli sanitari specifici, etc.).



2.1.4 Una proposta metodologica per la valutazione dei rischi soggettiva

L'I.A. potrebbe dunque essere utilizzata per una Valutazione dei Rischi "adattata alla variabilità umana". Partendo dai risultati della Valutazione dei Rischi realizzata con la classica matrice $R=P \times D$, con la quale il rischio è definito con la semplice correlazione tra la probabilità di accadimento dell'evento negativo e la gravità delle lesioni da esso causate, l'idea è quella di aggiungere un aggravante di rischio dato dalla diversità data (di genere, età, antropometrica, etc.), rappresentata, ad esempio, da un fattore K.

$$R' = P \times D \times K$$

dove:

R' = Rischio dato dalla presenza di gruppi di lavoratori "particolari"

$P \times D$ = probabilità x Danno

K = aggravante di rischio

Il fattore K può così riprodurre un coefficiente correttivo della magnitudo del rischio che può rappresentare le diverse variabilità umane, tenendo anche conto della possibile presenza simultanea delle variabili medesime, con conseguente incremento del Rischio, come di seguito rappresentato:

Correttivo K						
	Genere	Età	Contratto	Lingua	Capacità di apprendimento	Etc.
	R	R ¹	R ²	R ³	R ⁴	R ⁱ
R= PxD	4	K= 1,2				
		4,8	K= 1,3			
			6,24	K= 1,5		
				9,36	K= 1,7	
					15,912	
					...	
				
						...
						...

Con l'I.A. si potrebbe riprodurre, dunque, una valutazione dei rischi che considera anche come i fattori della variabilità umana s'intersechino tra loro e influenzino il rischio, supportare l'organizzazione ad individuare criticità ma anche evidenziare le necessità di adattamento in termini di misure di Prevenzione e protezione.

Un indirizzo di modalità di intendere la tutela, quello sopra delineato, che mette al centro le persone, i lavoratori, in linea anche con il paradigma dell'«Industria 5.0», che indirizza verso una ricerca e innovazione che possa guidare la transizione verso un ambiente sostenibile, umano-centrico e un'industria europea resiliente con l'obiettivo di mettere i bisogni ed interessi umani al centro del processo produttivo, ma anche di una tecnologia utilizzata nella produzione adattata alle esigenze ed alla diversità degli individui e di ambienti di lavoro più inclusivi.

Una prospettiva di adattabilità soggettiva del lavoro e delle misure di tutela già avviata in alcuni settori, dove la progettazione è indirizzata a postazioni di lavoro più idonee e flessibili alle esigenze degli operatori di linea, permettendo loro di svolgere le mansioni, oltre che in sicurezza, anche in condizioni confortevoli, favorendo il benessere e il miglioramento della performance. Il riferimento è, ad esempio, alle pedane auto-adattative dell'industria automobilistica, che ha introdotto postazioni di lavoro che si adattano alle misure antropometriche dei lavoratori: il sistema legge e identifica con badge personale attraverso totem adiacente alla postazione, i dati antropometrici del lavoratore e modifica l'altezza della postazione in base al percentile di riferimento del lavoratore.

2.1.5 Esempi applicativi

L'utilizzo dell'I.A. nell'ambito della gestione in sicurezza delle risorse umane può essere il più disparato. Alcune grandi realtà industriali, ad esempio, stanno iniziando ad adottare buone prassi per utilizzare l'Intelligenza Artificiale per accelerare l'organizzazione del lavoro, in relazione al task, nel rispetto delle idoneità, prescrizioni e limitazioni risultanti dalla sorveglianza sanitaria. Il sistema si basa sostanzialmente sulla valutazione del rischio effettuata con la metodologia OCRA (Occupational Repetitive Actions), legata alle varie postazioni di lavoro, e sui giudizi di idoneità alla

mansione, che sono espressi dal medico competente in relazione ai vari distretti dell'arto superiore sulla scorta dei colori dettati dall'analisi OCRA.

I dati di input comprendono la mappatura di tutte le postazioni di lavoro (operazioni/compiti lavorativi) analizzate con il metodo OCRA completo, poiché l'analisi del rischio comprende ogni singolo distretto (mano, polso, gomito e spalla), ed i giudizi di idoneità espressi dal medico competente con l'indicazione puntuale della limitazione (un esempio di limitazione è "idoneo alla mansione di con esclusione di (una o più fasi di disimpegno della mansione)").

Il sistema basato sull'I.A. può così facilmente supportare nel matchare operazioni/compiti lavorativi con le limitazioni soggettiva dei lavoratori in turno, organizzare il lavoro assegnando a ciascun lavoratore la fase operativa. Ovviamente il risultato è poi validato ed eventualmente corretto da un ergonomo che ne monitora il flusso. L'utilizzo dell'I.A. però accelera significativamente tale analisi.

Lo stesso principio si potrebbe adottare per gli altri fattori della variabilità umana che impattano sul rischio. Se ragioniamo, ad esempio, in termini di valutazione dei rischi "adattata alla variabilità umana", inserendo il fattore K illustrato nel precedente paragrafo, un sistema di I.A. potrebbe velocizzare l'analisi dei coefficienti correttivi e restituire un risultato esemplificato come di seguito indicato.

ESEMPIO

Mansione:	Addetto linea di assemblaggio (settore meccanica)		
Fattore di rischio analizzato:	<p>Rischio posturale e movimentazione manuale dei carichi</p> <p>(assunzione di posture incongrue durante il lavoro: stazionamento prolungato in piedi, accovacciati o in ginocchio, braccia tenute sopra l'altezza delle spalle, etc., sollevamento di carichi > 3 kg, movimenti ripetitivi da catena di montaggio, spinta-traino transpallet. etc.).</p>	R= PxD = 2x2	4

Diversità di età:	<ul style="list-style-type: none"> • Diminuzione di forza fisica e capacità di movimento (es. infiammazioni croniche a volta plantare, disturbi alla schiena, ginocchia, gomiti e polsi) e/o incremento dei disturbi muscolo-scheletrici – spesso i danni; • Diminuzione di resistenza ad attività faticose fisicamente o stressanti (necessità di un maggior tempo di recupero). <p>NOTA: spesso i danni subiti sono più gravi e con tempi di recupero più lunghi.</p>	<p>K = 1,5 (età 50-55 anni)</p> <p>K = 2 (età 55-60 anni)</p>
-------------------	---	---

R' (aggravato)	PxDxK = 2x2x1,5	6
	PxDxK = 2x2x2	8

Diversità di genere:	<ul style="list-style-type: none"> • Maggior affaticamento e rischio infortunistico derivanti da limitazioni fisiche (es. corporatura e altezza) contrastanti con l'attività (pesi da movimentare, altezze da raggiungere, etc.). • Diminuzione capacità di movimento derivante dal prolungato stazionamento in posizione eretta (es. vene varicose). 	K = 1,8 (presenza di donne)
R' (aggravato)	PxDxK = 2x2x1,8	7,2

Aggravante per diversità contrattuali:	<ul style="list-style-type: none"> • Maggior affaticamento fisico e rischio infortunistico per attività di manovalanza dirottata sui lavoratori "meno" tutelati e/o su mancate conoscenze in merito alle corrette procedure di lavoro. • Maggior rischio infortunistico per attività "più scomode" dirottate sui lavoratori contrattualmente "più deboli" e/o su mancate conoscenze in merito alle corrette procedure di lavoro. 	K = 1,5 (contratti precari)
R' (aggravato)	PxDxK = 2x2x1,5	6

Dalle risultanze correttive della valutazione dei rischi si potrebbero definire ulteriori misure prevenzione e protezione che, nel caso in esemplificazione, potrebbero comprendere:

- Riorganizzazione del lavoro favorendo una maggior rotazione del personale lungo la linea e/o limitando l'orario di lavoro, in linea, per i lavoratori > 50 anni.
- Riorganizzazione del lavoro favorendo una maggiore rotazione del personale addetto alle attività "più scomode" in modo da diminuire il rischio infortunistico.
- Gestione delle competenze con l'avanzamento dell'età.
- Pianificare puntualmente le lavorazioni con i responsabili di produzione per la distribuzione delle attività tra i lavoratori (particolare attenzione agli interinali e, in generale, ai lavoratori con minore esperienza).
- Coinvolgimento del Medico Competente per implementare controlli sanitari specifici.

Bibliografia

- BECK U. (Ed. 2013), *La società del rischio. Verso una seconda modernità*, Feltrinelli
- BENINI, SORCIONI (2006), *Il fattore umano*, Donzelli
- CHIALASTRI (2012), *Human Factor. Sicurezza & Errore Umano*, IBN Editore
- BISIO (2003) *fattore umano e sicurezza sul lavoro*, Edizioni Unicopli
- D'AVENIA (2018), *Le vere cause degli incidenti*, www.puntosicuro.it
- FEDERICI M.C., ROMEO A. (2017), *Sociologia della Sicurezza*, Mondadori Università
- HAWKINS FRANCK (1987), *Human factor in Flight*, Aldershot Hampshire
- HELMREICH R.L. (1996), *Safety and Error Management: The Role of Crew Resource Management*, University of Texas
- ICAO (1998), *Human Factor Training Manual*, Doc 9683-AN/950
- KOONCE J.M. (2002), *Human Factor in the Training of Pilots*, Taylor & Francis
- ORLADY H.W e ORLADY L.M. (1999), *Human Factor in Multi-Crew Flight Operations*, Ashgate Publishing Limited
- RALLI MARCELLO (1993), *Fattore umano e operazioni di volo*, Libreria dell'Orologio
- REASON J. T., (1990), *"Human error"*, Cambridge university press, trad. it. *"L'errore umano"*, Il Mulino
- SALAS E, MAURINO D. (2010), *Human Factors in Aviation*, Academic Press, Elsevier
- TURNER E PIDGEON, 2001 *Disastri: la responsabilità dell'uomo nelle catastrofi*, Einaudi
- VECCHIONE E, VIOLA M. (2008), *Fattore umano in aviazione*, IBN Editore
- WOODS D., DEKKER S., COOK R., JOHANNESSEN L., SARTER N. (2010), *Behind Human Error*, Ashgate
- ZAMPONI (2022), *l'ergonomia e il benessere organizzativo: Le fasi e i processi di adattamento*, 78Edizioni

Altri contributi accademici e specialistici

- ANGELINI, *Lavori flessibili e sicurezza nei luoghi di lavoro: una criticità da governare*, in *Olympus*, voce *Approfondimenti*, 2007
- D'AVENIA R. (2018), *Investigare sugli incidenti con i modelli causali*, *Ambiente & Sicurezza*, n. 2
- GHERARDI S., NICOLINI D. E ODELLA F., «Dal rischio alla sicurezza: il contributo sociologico alla costruzione di organizzazioni affidabili», *Quaderni di Sociologia*
- GHERARDI S., NICOLINI D. (2000), *The Organizational Learning of Safety in Communities of Practice*. *Journal of Management Inquiry*
- SPADONI DANIELE, *Human factor and non-technical skills: come costruire una cultura del comportamento sicuro*, *Puntosicuro* del 31/01/2017

2.2 La valutazione del rischio e responsabilità: rischi connessi alle interferenze macchina-uomo-ambiente e relative responsabilità

Francesco Costantino

Sapienza Università di Roma, Dipartimento di ingegneria informatica, automatica e gestionale "Antonio Ruberti"

2.2.1 L'evoluzione del lavoro e l'emergere di nuovi rischi

L'interazione tra persone e nuove tecnologie rappresenta oggi uno degli ambiti più interessanti e complessi dell'analisi dei rischi nei contesti lavorativi. Se da un lato l'innovazione tecnologica è spesso accolta con entusiasmo per le promesse di efficienza, flessibilità e in generale di prestazioni migliorate, dall'altro apre scenari di incertezza e preoccupazione che meritano un'attenta riflessione. L'attenzione è rivolta in particolare ai rischi per la persona che si interfaccia con tecnologie emergenti all'interno di un sistema più ampio: l'ambiente operativo in cui tali interazioni si verificano. L'evoluzione del lavoro negli ultimi decenni ci offre una chiave di lettura utile. In passato, il lavoro si configurava come un'attività prevalentemente svolta tra persone, con modalità comunicative, gestuali e organizzative tipiche dell'interazione umana. Con la meccanizzazione prima, e la successiva automazione, il rapporto si è progressivamente spostato verso una relazione persona-tecnologia, nella quale chi opera in un processo si è trovato ad interagire con dispositivi sempre più complessi e performanti.

Oggi siamo di fronte a una nuova trasformazione: il lavoro contemporaneo si svolge sempre più spesso all'interno di sistemi cyber-socio-tecnici. Questa definizione rende conto della convergenza tra tre elementi fondamentali. Le nuove tecnologie, ovvero sistemi meccanici e digitali integrati, rappresentano il primo polo del sistema. Le persone, che interagiscono con tali sistemi e ne orientano le funzioni, costituiscono il secondo elemento. Il terzo fattore è l'ambiente – fisico, organizzativo e sociale – in cui queste interazioni si collocano e assumono significato operativo.

Un esempio emblematico di questo nuovo scenario è rappresentato dai robot collaborativi, o cobot, progettati per operare fianco a fianco con gli esseri umani nei contesti industriali. Questi sistemi segnano una discontinuità rispetto ai robot tradizionali, in quanto sono concepiti per interagire in modo diretto e continuo con l'operatore umano, condividendo spazi, compiti e, in alcuni casi, anche decisioni operative. La loro presenza modifica profondamente non solo le dinamiche di lavoro, ma anche il modo in cui il rischio viene percepito, valutato e gestito.

Questa trasformazione non può essere letta soltanto in termini tecnologici: essa ha una dimensione antropologica, cognitiva e organizzativa, che richiede strumenti interpretativi nuovi. È proprio in questo crocevia tra persona, macchina e ambiente che si collocano alcuni importanti interrogativi: quali sono i nuovi rischi generati da queste interferenze? E soprattutto: come possiamo gestirli in modo efficace, senza rinunciare al contributo umano né cedere a una delega cieca nei confronti delle macchine?

2.2.2 Tecnologie emergenti: tra efficienza e rischio

Come anticipato, l'adozione di nuove tecnologie nei contesti lavorativi è spesso motivata dalla necessità di aumentare la produttività, migliorare l'efficienza operativa o aumentare la flessibilità dei sistemi. Tuttavia, accanto a queste motivazioni economiche e organizzative, si fa sempre più strada anche l'attenzione alla sicurezza delle persone. Le imprese e le organizzazioni, infatti, riconoscono che l'automazione e la digitalizzazione possono offrire strumenti utili anche per ridurre l'esposizione al rischio, alleggerire i carichi fisici e prevenire infortuni.

Un esempio significativo di questo approccio è rappresentato dall'introduzione degli esoscheletri nel settore industriale e logistico. Un esoscheletro è un dispositivo digitale-meccanico indossabile, una

sorta di “armatura” tecnologica che sostiene e amplifica i movimenti dell’operatore. Gli esoscheletri sono progettati per ridurre il carico biomeccanico durante compiti fisicamente impegnativi, ad esempio nel sollevamento di carichi pesanti o nei lavori overhead, cioè sopra la linea delle spalle. Grazie al loro utilizzo, è possibile diminuire l’insorgenza di affaticamento muscolare, strappi o stiramenti, in particolare a livello della colonna vertebrale, delle spalle e delle braccia. Tuttavia, anche quando la finalità principale di una nuova tecnologia è la tutela della salute, emergono nuovi rischi di tipo diverso, spesso meno immediati da identificare. Ad esempio, cosa accade se una persona che indossa un esoscheletro urta inavvertitamente un collega? Oppure se deve allontanarsi in fretta dal luogo di lavoro in caso di emergenza? In entrambi i casi, il dispositivo che in condizioni normali rappresenta un ausilio, può diventare un ostacolo o addirittura una fonte di pericolo.

Questo fenomeno mostra una *tensione evolutiva della tecnologia*, l’evoluzione porta progresso ma anche una destabilizzazione del sistema in cui essa viene inserita, con un *paradosso dell’intento tecnologico*, per cui quello che è progettato per aiutare, talvolta crea nuove difficoltà. Anche le tecnologie puramente digitali, le piattaforme informatiche e i sistemi basati su intelligenza artificiale generano effetti collaterali non trascurabili. Ne è testimonianza il technostress osservato durante la pandemia di Covid-19, quando lo smart working si è diffuso massicciamente e ha reso evidente l’impatto psicologico della pervasività tecnologica. La continua connessione, la necessità di adattarsi a strumenti digitali poco familiari e la difficoltà nel mantenere un confine chiaro tra lavoro e vita privata hanno generato in molti lavoratori disagio, fatica cognitiva e un senso di disorientamento.

In definitiva, *ogni tecnologia introdotta in un contesto lavorativo modifica l’equilibrio preesistente tra persona, macchina e ambiente*. Anche quando l’obiettivo dichiarato è la riduzione del rischio, occorre interrogarsi su quali nuove forme di esposizione possano emergere, sia sul piano fisico sia su quello cognitivo ed emotivo.

2.2.3 Il contesto conta: la tecnologia non è mai neutra se inserita in un sistema

La crescente presenza di tecnologie avanzate nei luoghi di lavoro impone una riflessione profonda non solo sulle caratteristiche intrinseche di tali dispositivi, ma anche e soprattutto sul contesto in cui essi vengono inseriti. Un aspetto spesso sottovalutato è proprio la natura *situata* del rischio: la stessa tecnologia può comportare esiti molto diversi a seconda dell’ambiente fisico, dell’organizzazione del lavoro, della cultura aziendale e del profilo di chi la utilizza. In altre parole, la tecnologia non è mai neutra, ma assume significato e impatto in relazione al sistema in cui viene adottata.

Di fronte a questa complessità, le organizzazioni sembrano oggi muoversi secondo due direttrici principali. La prima consiste nel *trattare le nuove tecnologie come semplici estensioni delle macchine tradizionali*, applicando quindi le stesse normative, regolamenti e metodologie di valutazione del rischio. Questa strategia può rappresentare un primo passo utile, ma presenta limiti evidenti: i dispositivi attuali, infatti, non sono più semplici meccanismi lineari, ma sistemi dinamici e adattivi, spesso controllati da software intelligenti, capaci di apprendere, decidere e interagire con l’ambiente. La seconda direttrice, altrettanto problematica, è quella che porta molti utenti finali ad *affidarsi alle indicazioni dei produttori*. In molti casi, le aziende acquirenti presumono che il costruttore della tecnologia abbia già valutato e previsto tutti i rischi possibili. Tuttavia, i costruttori, per quanto competenti, non possono conoscere nel dettaglio il contesto operativo in cui il loro prodotto verrà effettivamente utilizzato. Non possono prevedere la configurazione specifica degli ambienti, le abitudini lavorative, le caratteristiche delle persone coinvolte, né le interazioni impreviste che potrebbero emergere nel tempo. Un esempio concreto riguarda l’impiego di un cobot in una linea di assemblaggio di piccoli elettrodomestici. Il robot, dotato di una pinza, era programmato per spostare utensili come cacciaviti magnetici da una postazione all’altra. Durante una fase operativa, il cobot ha inavvertitamente lasciato cadere il cacciavite. Secondo le specifiche

del produttore, in simili situazioni l'oggetto avrebbe dovuto atterrare su una superficie antiurto, senza danni. Tuttavia, nel contesto reale, sotto il braccio del robot si trovava temporaneamente una scatola aperta contenente circuiti stampati. Il cacciavite è caduto proprio all'interno della scatola, danneggiando i componenti e causando un'interruzione della produzione. In un altro caso, un operatore si era chinato proprio sotto il cobot per raccogliere un pezzo: se la caduta fosse avvenuta in quel momento, avrebbe potuto subire una ferita seria. Questo mostra come anche eventi prevedibili, come il rilascio di un oggetto, possano avere conseguenze molto diverse a seconda delle condizioni specifiche e imprevedute dell'ambiente operativo, confermando che le valutazioni del produttore, per quanto accurate, non possono sostituire un'analisi contestuale dei rischi.

Queste due tendenze, l'applicazione di approcci tradizionali da un lato e l'esternalizzazione della responsabilità dall'altro, finiscono per generare una pericolosa sottovalutazione del rischio contestuale. Il risultato è una valutazione della sicurezza incompleta, che non tiene conto delle nuove variabili introdotte dalla presenza di sistemi digitali e intelligenti nei luoghi di lavoro. Diventa dunque fondamentale superare la visione lineare e deterministica della tecnologia, per abbracciare una logica più sistemica, più attenta alla variabilità e alla complessità delle interazioni.

2.2.4 Complessità e imprevedibilità nei sistemi contemporanei

Il ricorso agli approcci tradizionali per la valutazione e la gestione dei rischi nei luoghi di lavoro, quelli sviluppati in epoca di meccanizzazione e poi di automazione, rappresenta ancora oggi una prassi diffusa. Questi approcci si basano sull'idea che il sistema tecnico sia analizzabile in modo lineare, attraverso la scomposizione in elementi discreti, la previsione di scenari di pericolo e la definizione di misure preventive o correttive. Ma quando si ha a che fare con sistemi contemporanei, questi strumenti mostrano rapidamente i propri limiti. Le nuove tecnologie evolvono a una velocità tale da rendere difficile il loro inquadramento normativo tempestivo. La legislazione fatica a stare al passo con l'innovazione e spesso si basa su logiche superate, non in grado di cogliere le implicazioni di sistemi autonomi, intelligenti, connessi in rete. Di fronte a questo disallineamento tra innovazione tecnologica e aggiornamento normativo, è fondamentale non assumere un atteggiamento attendista. Non è necessario né consigliabile aspettare che le normative recepiscano pienamente i nuovi scenari per iniziare a lavorare sulla sicurezza. È già possibile (e auspicabile) utilizzare le metodologie esistenti che si sono dimostrate efficaci, adattandole ai contesti emergenti con intelligenza e flessibilità. Inoltre, esistono approcci consolidati nella letteratura tecnico-scientifica, come la Resilience Engineering, la Safety-II o i modelli ibridi di analisi del rischio, che pur non essendo ancora completamente integrati nel quadro normativo, offrono strumenti concreti per migliorare la comprensione e la gestione della complessità. Adottare questi strumenti, anche in assenza di obblighi di legge, significa scegliere un atteggiamento proattivo e responsabile, orientato alla qualità e alla sostenibilità dei sistemi di lavoro.

Anche le competenze interne alle aziende fanno fatica ad aggiornarsi con la stessa rapidità: molte organizzazioni si trovano a utilizzare strumenti di cui non comprendono pienamente il funzionamento, né tantomeno le implicazioni di sicurezza. Ma è soprattutto l'aumento delle interazioni tra persone, tecnologie e ambiente operativo a generare una nuova dimensione di complessità. Il lavoro non è più un processo lineare, ma un intreccio dinamico soggetto a un numero crescente di variabili. In termini sistemici, si può dire che il lavoro contemporaneo avviene dentro sistemi complessi, ovvero sistemi nei quali non è possibile identificare relazioni di causa-effetto pienamente controllabili, che non si prestano a una scomposizione lineare e che sono caratterizzati da una tale variabilità da renderli difficilmente prevedibili. Ciò non significa che il lavoro tra due persone, senza l'intermediazione della tecnologia, sia di per sé semplice. Anche in un contesto apparentemente "artigianale", la complessità può essere elevata, ad esempio quando il compito

richiede un alto grado di coordinamento, quando è soggetto a interruzioni improvvise o quando si svolge in ambienti non strutturati. Tuttavia, in questi casi la comunicazione si fonda su modelli innati nell'essere umano, su segnali verbali e non verbali, su un'intelligenza sociale sviluppata sin dalla nascita attraverso le esperienze quotidiane. L'essere umano è naturalmente attrezzato per interpretare questo tipo di segnali, sia quando discute con un collega in ufficio, sia quando ordina un caffè al bar. Diversamente, quando la persona si interfaccia con sistemi digitali, intelligenti, meccanici, entra in un territorio molto più incerto. Le fonti di complessità si moltiplicano: si parla di *opacità algoritmica*, ovvero l'incapacità di comprendere come "ragiona" il sistema; è attestato un rischio di *cognitive overload*, per la quantità di informazioni da elaborare; esistono difficoltà di interpretazione dei dati e delle interfacce; infine, si manifesta un problema crescente di delega eccessiva, che porta le persone ad affidarsi alla tecnologia, rinunciando alla propria capacità critica. Tutto questo genera una nuova ambiguità, quella della responsabilità: dove finisce il controllo umano? Chi prende realmente le decisioni operative? Chi risponde di un errore? Queste domande diventano centrali, soprattutto in ambiti dove è forte l'adozione di intelligenza artificiale o automazione avanzata.

Un esempio può chiarire il concetto. Si pensi a due artigiani che costruiscono un oggetto in legno: usano scalpelli, seghe, le mani, e coordinano le proprie azioni parlando, osservandosi, leggendo gesti e intenzioni. In questo caso, la complessità dipende dal compito, dal contesto, dal grado di esperienza e dalla capacità di comunicazione. Ora immaginiamo, invece, un operatore industriale che gestisce una linea produttiva mediante una piattaforma digitale con AI predittiva, manutenzione automatica, controllo remoto. In apparenza, il lavoro è semplificato, ma in realtà la complessità non è scomparsa: si è semplicemente spostata sull'interfaccia tra l'operatore e i sistemi tecnologici, che diventa il nuovo centro di gravità del rischio.

2.2.5 Superare i modelli tradizionali: da Safety-I a Safety-II

Di fronte all'aumento della complessità nei sistemi socio-tecnici contemporanei, diventa evidente che i tradizionali modelli di gestione della sicurezza non sono più sufficienti. Per decenni, la sicurezza è stata intesa come "assenza di incidenti" e misurata in termini di frequenza e gravità degli eventi negativi. Questo approccio, definito retrospettivamente come *Safety-I*, si fonda sull'idea che ogni incidente derivi da un malfunzionamento, un errore umano o una deviazione da una norma o da una procedura prestabilita. La logica conseguente è quella della riduzione dell'errore: progettare sistemi resilienti rimuovendo il fattore umano, standardizzando le attività, limitando la variabilità. Tuttavia, questa visione presenta un limite strutturale: presuppone un sistema prevedibile, stabile, lineare. Ma come abbiamo visto, i sistemi in cui operiamo oggi sono tutto fuorché lineari. Sono ambienti in continua trasformazione, in cui l'incertezza è la regola e la variabilità non è solo inevitabile, ma spesso anche necessaria. È in questo scenario che si è affermato un nuovo paradigma, noto come *Safety-II*, che propone un cambiamento di prospettiva tanto radicale quanto necessario. La *Safety-II* non si concentra su ciò che va storto, ma su ciò che normalmente va bene. Invece di analizzare solo gli incidenti, essa si interroga su *come il sistema riesca ogni giorno, nella stragrande maggioranza dei casi, a raggiungere i propri obiettivi in modo sicuro ed efficace*, nonostante le pressioni, i vincoli, gli imprevisti. Si tratta di un approccio proattivo, che riconosce nella persona non un fattore di rischio, ma una risorsa preziosa. Questa visione si deve principalmente al lavoro di Erik Hollnagel, uno dei principali teorici della Resilience Engineering. Secondo la *Safety-II*, la sicurezza emerge dalla capacità del sistema, persone comprese, di adattarsi, apprendere, anticipare e rispondere. È un cambiamento profondo di mentalità: non si tratta più di prevenire gli errori eliminando la variabilità, ma di gestire la variabilità in modo intelligente, riconoscendo che l'adattamento umano è spesso ciò che evita l'incidente. Adottare la *Safety-II* significa anche cambiare lo sguardo sulla persona nel sistema. Un buon modo per comprendere il senso della *Safety-II* è ricorrere a un esempio semplice ma efficace.

Se vogliamo capire perché un matrimonio funziona, non possiamo limitarci a intervistare solo chi ha divorziato. È certamente utile analizzarne gli errori, ma se non ascoltiamo anche le coppie insieme da decenni rischiamo di perdere i "segreti" del successo. Lo stesso vale per la sicurezza nei sistemi complessi: non basta indagare gli incidenti, bisogna osservare e comprendere anche tutto ciò che consente al sistema di funzionare ogni giorno, nonostante le pressioni, le deviazioni e gli imprevisti. Questo approccio allarga lo sguardo, includendo la normalità operativa come oggetto di analisi e fonte di apprendimento. In termini di valutazione del rischio, significa studiare anche come le persone riescano a gestire la variabilità senza incorrere in errori, facendo emergere le strategie efficaci, spesso informali, che garantiscono la sicurezza nelle attività quotidiane. È una logica che mette al centro l'adattamento, la resilienza e la competenza distribuita sul campo, valorizzando l'esperienza reale degli operatori. L'essere umano non è più visto come l'elemento debole, l'anello incerto, il potenziale colpevole. Al contrario, è considerato una risorsa strategica, in grado di percepire segnali deboli, di improvvisare soluzioni non previste dalle procedure, di riconfigurare in tempo reale la propria attività in funzione del contesto. È in questo senso che si parla di "*human as hero*", contrapposto alla vecchia idea dell'"*human as hazard*". Gestire i rischi in sistemi di interazione uomo-tecnologia secondo l'approccio Safety-II significa dunque accettare la complessità come condizione naturale del lavoro contemporaneo. Significa osservare i sistemi non solo dall'alto, con modelli prescrittivi e regole standardizzate, ma anche dal basso, ascoltando l'esperienza diretta degli operatori, valorizzando ciò che essi fanno per mantenere il sistema in equilibrio.

2.2.6 La resilienza come chiave di lettura e le domande finali

Per affrontare i rischi nei sistemi complessi in modo coerente con il paradigma della Safety-II, si è sviluppata negli ultimi anni una nuova prospettiva metodologica nota come *Resilience Engineering*. Questo approccio parte dal riconoscimento che non è possibile eliminare del tutto l'incertezza, l'imprevisto e la variabilità nei contesti operativi. Piuttosto, occorre sviluppare la capacità di convivere con questi elementi, rendendo il sistema capace di rispondere in modo flessibile e adattativo. Secondo la Resilience Engineering, un sistema è resiliente quando possiede quattro capacità fondamentali. La prima è la *capacità di monitoraggio*, ovvero l'abilità di percepire in anticipo segnali deboli, cambiamenti nel contesto, deviazioni rispetto alla norma, anche quando non costituiscono ancora un pericolo manifesto. La seconda è la *capacità di risposta*, cioè l'abilità di reagire in modo tempestivo e pertinente quando si verifica un evento inatteso. La terza è la *capacità di apprendimento*, che consiste nel saper riflettere sull'esperienza, integrarla nella pratica, migliorare continuamente a partire dagli esiti concreti dell'attività. Infine, la *capacità di anticipazione* permette di immaginare scenari futuri e prepararsi a potenziali minacce o cambiamenti, anche in assenza di segnali diretti.

Queste capacità sono fortemente radicate nell'intelligenza umana. Le persone, in quanto agenti cognitivi, sono in grado di gestire situazioni complesse perché fanno ricorso non solo a competenze tecniche, ma anche a intuizioni, a conoscenze implicite, a modelli mentali costruiti con l'esperienza. *Quando si affidano interi task alla macchina o a un sistema automatico, si rischia di perdere questi elementi di valore*, delegando attività che magari appaiono semplici, ma che nascondono in realtà una ricca componente cognitiva e relazionale che ha un valore importante ai fini della salute e sicurezza sul lavoro. Bisogna dunque iniziare a ragionare su *quello che viene perso quando il lavoro umano viene automatizzato*. Il modello SRK di Jens Rasmussen aiuta a comprendere questa dinamica. Secondo tale modello, l'agire umano può essere classificato in tre livelli. Il primo livello prevede azioni di tipo *Skill-based*, ovvero azioni automatiche, routinarie, apprese, svolte in maniera quasi istintiva. Prendiamo l'esempio di un magazziniere che in prossimità di uno spazio ristretto vicino a un'area di passaggio pedonale riduce la velocità in maniera automatica, grazie alla sua abilità consolidata nella guida del veicolo. Il secondo livello riguarda le azioni *Rule-based*, che sono guidate

da regole note o procedure. Nell'esempio del magazziniere, la presenza di una regola che impone di suonare il clacson in caso di mancanza di visibilità è stabilita dall'azienda e viene seguita dal guidatore. Il terzo livello considera le azioni *Knowledge-based*, fondate sull'analisi, sull'interpretazione, sull'elaborazione cognitiva complessa, sulla capacità di mischiare azioni routinarie e regole note in maniera originale creando azioni non normate o codificate, ma utili per la gestione dei rischi quando si presentano le variabilità di cui si è parlato. Nell'esempio del magazziniere, di fronte a un bancale di merce stoccato in maniera inappropriata, a fronte di una valutazione personale del rischio che esula da quanto già visto in passato, nonché dalle regole fornite dall'organizzazione, il guidatore preferisce fermare il mezzo e comunicare con il supervisore per garantire le condizioni di sicurezza.

Le tecnologie odierne sono molto efficaci nel riprodurre compiti skill-based e rule-based, ma faticano ad affrontare situazioni knowledge-based, in cui servono intuito, flessibilità e giudizio. Nell'esempio del magazziniere, sostituendolo con un sistema a guida autonoma, esso può essere programmato per riconoscere la vicinanza di persone e diminuire la velocità, così come la mancanza di completa visibilità e il suono del clacson, ma difficilmente si riuscirebbe a contemplare la capacità di accorgersi di un bancale male impilato.

Va riconosciuta dunque una zona grigia, tra regola e intuizione, tra automatismo e consapevolezza, dove si colloca gran parte del valore umano nel lavoro. Quando si automatizza un compito senza comprenderne appieno la natura cognitiva, si corre il rischio non solo di abbassare il livello di sicurezza, ma anche di compromettere la capacità del sistema di apprendere, anticipare e adattarsi. Ecco perché il passaggio alla tecnologia non deve mai essere inteso come una sostituzione integrale, ma come un nuovo patto di collaborazione tra l'uomo e la macchina.

In conclusione, il tema delle interferenze tra tecnologie, persone e ambiente operativo non si risolve con l'introduzione di nuovi strumenti, ma richiede una trasformazione culturale e organizzativa profonda che riconosca di guardare ai rischi partendo da nuovi punti di vista: i sistemi persona-tecnologia sono complessi e non devono essere analizzati come sistemi deterministici (causa→effetto); le persone sono una risorsa da valorizzare in ottica di gestione dei rischi, come sentinelle in grado di intervenire con capacità cognitive inimitabili dalla tecnologia; serve un'attenzione al contesto, alla complessità e alle molteplici dinamiche reali dell'attività quotidiana.

2.3 La necessità di conoscere la logica che sottende la progettazione al funzionamento delle tecnologie applicate, funzionale alla individuazione dei rischi nonché agli aspetti manutentivi

Alessandro Palla*, Antonio Baldassarre**

*Senior staff machine learning engineer & AI Researcher, Intel Corporation

**Prof. Medicina del Lavoro- Università degli studi Firenze

Introduzione

L'Intelligenza Artificiale (IA) rappresenta una delle forze trainanti più significative della trasformazione tecnologica contemporanea, incidendo profondamente e in modo pervasivo su quasi ogni settore dell'attività umana. Dalla sanità alla finanza, dall'automazione industriale alla logistica, l'adozione di sistemi basati sull'IA promette efficienze senza precedenti, capacità analitiche superiori e la possibilità di affrontare problemi complessi che in precedenza erano considerati insormontabili. Tuttavia, la crescente integrazione di queste tecnologie avanzate introduce nuove sfide e complessità, in particolare riguardo alla loro progettazione, al loro funzionamento e, in modo cruciale, alla gestione dei rischi associati e degli interventi di manutenzione necessari. La natura intrinseca di molti algoritmi di IA, in particolare quelli basati su reti neurali profonde e apprendimento automatico, spesso li rende opachi, trasformandoli in vere e proprie "scatole nere". Questa opacità implica che, pur essendo capaci di generare risultati eccezionali, il processo decisionale interno e la logica sottostante che conducono a tali risultati non sono immediatamente comprensibili o interpretabili dagli esseri umani. Tale mancanza di trasparenza solleva questioni fondamentali in termini di responsabilità, affidabilità e sicurezza, specialmente in contesti critici in cui le decisioni dell'IA possono avere conseguenze significative sulla vita delle persone, sulla sicurezza operativa o sulla stabilità economica. Il presente capitolo si propone di esaminare l'urgenza di una comprensione approfondita della logica che sottende la progettazione e il funzionamento delle tecnologie IA. Tale conoscenza non è solo un requisito accademico o teorico, ma una condizione essenziale per l'individuazione proattiva e la gestione efficace dei rischi emergenti, nonché per la pianificazione e l'esecuzione di interventi di manutenzione mirati e funzionali. Attraverso l'analisi di casi specifici, in particolare nel campo della manutenzione predittiva, e l'esame delle sfide legate alla trasparenza e all'interpretabilità dell'IA, si intende dimostrare come una maggiore consapevolezza dei meccanismi interni dell'IA sia fondamentale per sfruttarne appieno il potenziale, minimizzando al contempo le vulnerabilità e garantendo un'implementazione sicura, etica e sostenibile.

Funzionamento e progettazione dell'Intelligenza Artificiale

L'IA si fonda su un insieme di tecniche matematiche e computazionali volte a permettere alle macchine di apprendere dai dati ed eseguire compiti complessi senza essere rigidamente programmate in ogni dettaglio. Per chi opera in ambito medico e della salute occupazionale, comprendere i principi di funzionamento e le logiche di progettazione di questi sistemi è cruciale non solo per sfruttarne le potenzialità, ma anche per valutarne limiti, rischi e implicazioni pratiche.

In passato, i programmi erano costruiti attraverso regole esplicite definite dall'uomo. Con l'avvento dell'approccio *data-driven*, l'attenzione si è spostata dal programmare regole all'addestramento automatico: i sistemi di IA imparano riconoscendo pattern e relazioni all'interno di grandi quantità di dati senza che questa capacità sia stata definita a priori dal programmatore.

Il dataset con cui viene addestrato un modello di IA riveste dunque un ruolo cruciale nella progettazione ed è diviso in tre componenti:

- Dataset di training: serve per l'apprendimento vero e proprio del modello, che adatta i propri parametri per minimizzare l'errore.
- Dataset di validazione: utilizzato durante l'addestramento per regolare l'architettura e prevenire fenomeni come l'*overfitting*, ovvero il fatto che il modello ricalca perfettamente i dati usati per addestrarlo ma non è in grado di generalizzare su dati mai visti prima.
- Dataset di test: impiegato a posteriori per valutare in modo indipendente le prestazioni del modello.

La dimensione, la qualità e la rappresentatività dei dati sono determinanti: un modello allenato con dati incompleti, distorti o contraddittori produrrà risultati poco affidabili.

Machine Learning, Deep Learning e Reinforcement Learning

L'addestramento dell'IA può assumere forme diverse. Nel *machine learning* (apprendimento automatico) classico, i modelli individuano relazioni tra variabili sulla base di funzioni statistiche o matematiche relativamente semplici. Fanno parte di questa categoria i modelli di regressione lineare e logistica, *decision-tree* (alberi decisionali), *random forest* (foreste casuali), *support vector machine* (macchine a vettori di supporto) e altri algoritmi che, pur con diversi gradi di complessità, si basano su regole esplicite e interpretabili.

Con l'avvento del *deep learning* (apprendimento profondo), invece, l'addestramento si è spostato verso reti neurali profonde capaci di apprendere rappresentazioni complesse e non lineari dei dati, arrivando a gestire immagini, testi e segnali con un livello di astrazione molto superiore. Mentre i metodi tradizionali richiedono spesso che l'esperto estragga manualmente le caratteristiche rilevanti dai dati, il deep learning è in grado di apprendere automaticamente rappresentazioni gerarchiche a partire da informazioni grezze come immagini, segnali o testi.

Un'altra importante branca è il *reinforcement learning* (apprendimento per rinforzo), che si distingue da entrambe le precedenti per il suo approccio dinamico e interattivo. In questo paradigma, l'agente non apprende da un insieme statico di dati, bensì interagendo con un ambiente: compie delle azioni, osserva gli effetti prodotti e riceve ricompense o penalità. L'obiettivo è massimizzare la ricompensa cumulativa nel tempo, sviluppando strategie (policy) ottimali attraverso un processo iterativo di esplorazione ed esperienza. Questo approccio ha trovato applicazioni particolarmente rilevanti nei sistemi di controllo, nella robotica, nei giochi (come gli algoritmi che hanno battuto i campioni di Go e scacchi) e più recentemente nell'ottimizzazione di processi complessi o nella gestione di risorse.

L'elemento comune a gran parte delle innovazioni più recenti in IA è l'impiego delle reti neurali, che prendono il nome dall'analogia con il cervello umano:

- Nei neuroni biologici, i dendriti ricevono segnali, il corpo cellulare li integra e, se viene superata una soglia, il neurone si attiva trasmettendo un impulso attraverso l'assone verso altre cellule tramite sinapsi.
- Nei "neuroni" artificiali, gli input numerici vengono moltiplicati per pesi che rappresentano l'importanza di ciascun segnale, sommati e trasformati da una funzione di attivazione: se la soglia viene superata, il neurone "spara" un output verso i livelli successivi.

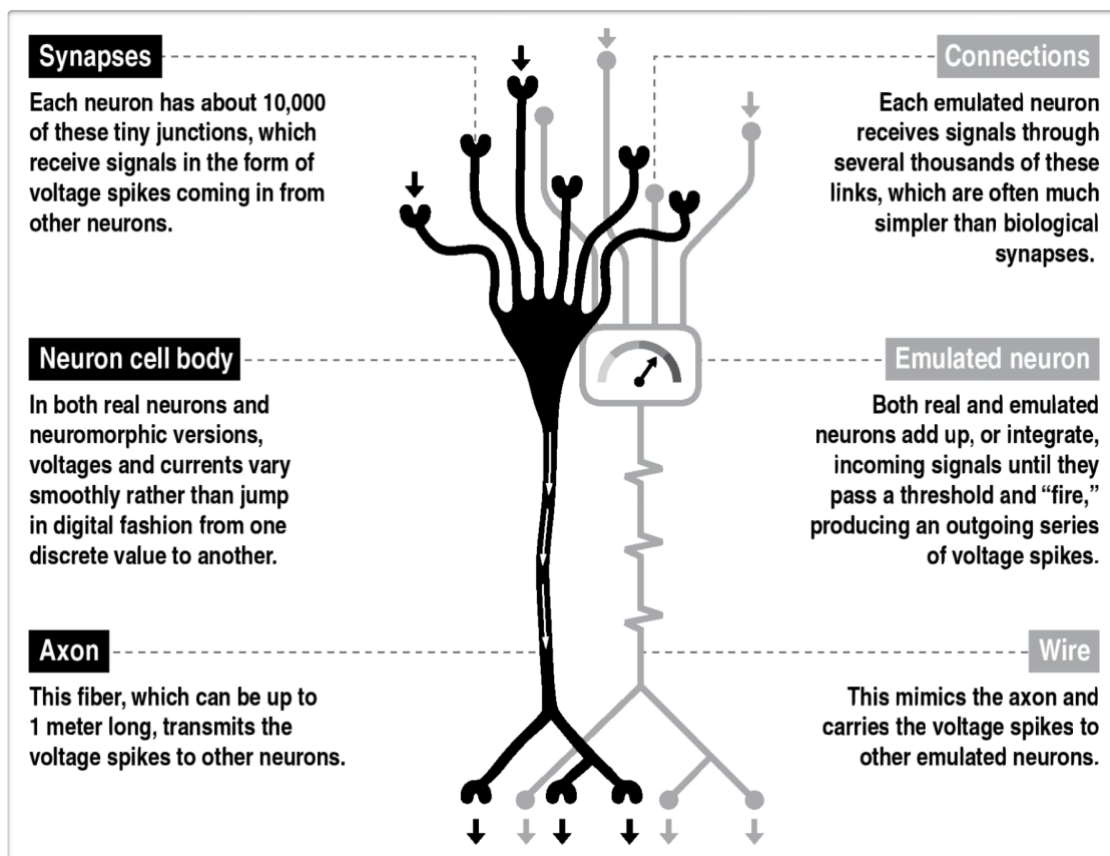


Figura 1 – Comparazione tra neuroni biologici ed artificiali, tratto da The homology between biological neurons and artificial neurons. Source: Adapted from M. Waldrop, “Neuroelectronics: Smart Connections,” Nature News (2013): 503(7474), 22–24

Questa analogia, pur semplificata, ha un valore concettuale: come nel cervello, l’IA non deriva da una singola regola esplicita, ma dall’interazione distribuita di molte unità semplici. Le reti neurali artificiali riescono così a riconoscere schemi complessi, ad esempio in immagini o sequenze temporali, senza istruzioni programmate passo dopo passo.

Va tuttavia sottolineato che si tratta di una somiglianza parziale. I neuroni biologici sono molto più complessi e l’apprendimento del cervello si fonda su processi elettrochimici e plasticità sinaptica, mentre le reti artificiali utilizzano algoritmi matematici. Nonostante ciò, il termine “reti neurali” rimane appropriato perché evidenzia l’ispirazione biologica che ha guidato lo sviluppo di questi modelli.

I Large Language Models (LLM) ad esempio sono, reti neurali di dimensioni estremamente elevate, addestrate su vastissimi corpora testuali. Questi modelli non comprendono il linguaggio come farebbe un essere umano, ma imparano a predire la parola successiva più probabile sulla base del contesto. Tale meccanismo statistico, se supportato da un addestramento su dati eterogenei e di qualità, permette loro di generare testi coerenti, rispondere a domande complesse, sintetizzare documenti o assistere in processi decisionali.

Progettazione delle Intelligenze Artificiali

In generale la progettazione di un sistema di IA segue un percorso metodico che parte dalla definizione del task e delle specifiche funzionali. Prima di procedere è necessario chiarire:

- quale problema il modello deve risolvere (classificazione, previsione, generazione di contenuti, ecc.);
- quali metriche di prestazione saranno utilizzate (accuratezza, sensibilità, precisione, AUC, ecc.);

- quali vincoli pratici devono essere rispettati (tempi di risposta, consumo energetico, capacità di scalare a grandi volumi di dati).

Solo dopo aver definito questi parametri si passa alla scelta dell'architettura del modello, che può spaziare da algoritmi più semplici a reti neurali profonde, a seconda della complessità del compito e della disponibilità dei dati.

Addestramento e validazione del modello

Ogni rete neurale necessita di un addestramento sul dataset di training, durante il quale i pesi interni vengono progressivamente aggiornati per ridurre l'errore rispetto ai dati osservati. Il cuore matematico di questo processo è l'algoritmo di backpropagation, che calcola come modificare i pesi a partire dalla differenza tra output desiderato e output prodotto. Ci sono tre modalità principali per addestrare le IA:

- **Training:** indica l'addestramento completo di un modello a partire da zero, utilizzando un dataset molto ampio. È la fase più costosa in termini di dati e risorse computazionali.
- **Fine-tuning:** consiste nell'adattare un modello già pre-addestrato a un dominio specifico, ad esempio usando dati di settore. Questa tecnica permette di ottenere modelli specializzati con costi più contenuti.
- **Prompt engineering:** con l'avvento di modelli generalisti come gli LLM, è possibile guidare il comportamento del sistema attraverso istruzioni in linguaggio naturale, "programmando" il modello a svolgere compiti diversi senza doverlo ri-addestrare.

Un nuovo modo di concepire lo sviluppo

L'evoluzione dello sviluppo dei sistemi di IA può essere vista come una sequenza di cambiamenti paradigmatici.

- **Approccio algoritmico:** in origine, i sistemi erano basati su regole esplicite programmate dall'uomo.
- **Approccio data-driven:** con l'introduzione dell'apprendimento automatico, l'attenzione si è spostata sui dati, che guidano direttamente l'apprendimento dei modelli.
- **Modelli generalisti (LLM):** oggi disponiamo di architetture capaci di affrontare compiti diversi, senza la necessità di progettare una rete per ogni singola applicazione.

Questo nuovo paradigma permette di "programmare" i modelli tramite prompt engineering e di sfruttare tecniche come *few-shot* (il modello apprende un nuovo compito a partire da pochi esempi) o lo zero-shot learning (il modello generalizza a compiti non visti senza esempi espliciti), riducendo tempi e costi di sviluppo.

Il passaggio è paragonabile a quello che, nella storia dell'informatica, ha segnato il passaggio dai computer analogici ai computer digitali: i primi erano costruiti su misura per ogni problema, i secondi hanno introdotto un livello di astrazione che ha reso possibile programmare macchine generaliste. Allo stesso modo, gli attuali modelli di IA generalista rappresentano una piattaforma adattabile, in grado di affrontare compiti imprevisti e di evolvere rapidamente con nuove modalità d'uso.

La fase di progettazione deve includere la validazione del modello su dati indipendenti, finalizzata alla regolazione degli iperparametri (*hyperparameters*), ossia quei parametri esterni al processo di apprendimento che influenzano in maniera determinante la complessità e le prestazioni del modello. Tale procedura è inoltre essenziale per monitorare e prevenire fenomeni di *overfitting*,

ovvero la tendenza del modello a adattarsi eccessivamente ai dati di addestramento perdendo capacità predittiva su dati nuovi. Successivamente, il modello deve essere sottoposto a un test finale su un dataset non visto, con l'obiettivo di valutare la sua effettiva capacità di generalizzazione. Un modello ben progettato, infatti, non deve soltanto ottenere buone prestazioni sul training set, ma deve garantire robustezza e affidabilità anche in presenza di dati inediti e potenzialmente eterogenei.

La sfida della "Black Box" nell'IA

Nonostante i numerosi vantaggi e le applicazioni promettenti dell'IA, l'adozione diffusa di queste tecnologie presenta una sfida intrinseca già anticipata nell'introduzione: il problema della "black box". Questo termine si riferisce alla difficoltà, o in alcuni casi all'impossibilità, di comprendere il processo decisionale interno di un modello di IA, ovvero come e perché un algoritmo arrivi a una determinata conclusione o previsione.

Molti dei modelli di IA più avanzati e performanti, come le reti neurali, operano tramite milioni di parametri e complessi strati, rendendo estremamente difficile seguire il percorso logico che porta a un output specifico. Questa mancanza di chiarezza è una conseguenza diretta della loro architettura e del loro metodo di apprendimento dai dati. A differenza dei sistemi basati su regole esplicite, in cui ogni decisione può essere rintracciata a una logica predefinita, i modelli di apprendimento automatico identificano autonomamente schemi e correlazioni nei dati, spesso in modi che non sono intuitivamente comprensibili per gli esseri umani.

La mancanza di trasparenza si manifesta in diverse forme:

- Opacità algoritmica: L'incapacità di spiegare il funzionamento interno di un algoritmo, anche se sono noti i suoi input e output.
- Opacità dei dati: La difficoltà di comprendere come specifici dati di input influenzino l'output, o come i bias presenti nei dati di addestramento possano propagarsi e amplificarsi nelle decisioni del modello.
- Opacità del modello: L'impossibilità di estrarre regole o logiche chiare che governano il comportamento complessivo del sistema.

Conseguenze della "Black Box": difficoltà nell'identificazione di bias, errori e responsabilità

Le implicazioni della logica inaccessibile che sottintende all'IA sono profonde e multifattoriali, interessando elementi tecnici, etici, legali e sociali.

- Difficoltà nell'identificazione dei bias: se un modello di IA è indecifrabile, diventa estremamente complesso identificare e correggere eventuali pregiudizi algoritmici. Tali pregiudizi possono derivare da dati di addestramento non rappresentativi o distorti e possono condurre a decisioni ingiuste o discriminatorie, ad esempio in ambiti come le assunzioni, la concessione di prestiti o le diagnosi mediche.
- Difficoltà nell'identificazione e nella correzione degli errori: quando un sistema di IA individua un errore, la natura della 'black box' rende complicato comprendere la causa principale dell'errore. Ciò ostacola la capacità di debug, il miglioramento del modello e la prevenzione di futuri malfunzionamenti, con potenziali conseguenze gravi in applicazioni critiche, quali i veicoli autonomi o i sistemi di controllo industriale.
- Problemi di responsabilità: In caso di danni o incidenti causati da un sistema di IA, la mancanza di trasparenza rende difficile attribuire la responsabilità. Chi è responsabile se un algoritmo

prende una decisione errata che provoca danni? Il progettista, l'operatore, il produttore? Questa incertezza legale ed etica rappresenta un ostacolo significativo all'adozione su larga scala dell'IA in settori regolamentati.

- Mancanza di fiducia: La fiducia è un elemento cruciale per l'accettazione e l'adozione di qualsiasi tecnologia. Se gli utenti non comprendono il modo in cui un sistema di IA prende le proprie decisioni, è meno probabile che si fidino dei suoi risultati, specialmente in contesti ad alto rischio. Questa mancanza di fiducia potrebbe limitare l'efficacia e la diffusione di questa tecnologia, anche quando i suoi potenziali benefici sono considerevoli.

La necessità di IA Spiegabile (XAI) per una maggiore comprensione e fiducia

Per affrontare queste sfide, è emerso il campo dell'IA Spiegabile (*eXplainable AI - XAI*). L'obiettivo della XAI è sviluppare metodi e tecniche che permettano agli esseri umani di comprendere, interpretare e riporre fiducia nei risultati forniti dai sistemi di IA, senza la necessità di conoscere ogni singolo calcolo interno. Le tecniche di XAI si prefiggono di garantire:

- Trasparenza: Rendere visibile il funzionamento interno del modello o, quanto meno, le sue parti più significative.
- Interpretabilità: La capacità di chiarire in termini comprensibili per gli esseri umani il motivo per cui un modello ha preso una determinata decisione.
- Fiducia: Costruire la fiducia degli utenti nei sistemi di IA, dimostrando che le decisioni sono basate su motivazioni valide e non su correlazioni spurie o pregiudizi latenti.

Esempi di tecniche di XAI comprendono l'analisi dell'importanza delle caratteristiche (*feature importance*), spiegazioni locali (ovvero il perché di una singola previsione) e spiegazioni globali (come il modello si comporta nel complesso). L'implementazione della XAI è fondamentale non solo per motivi etici e legali, ma anche per migliorare la manutenzione e il debug dei sistemi di IA, consentendo agli ingegneri di identificare e risolvere più facilmente eventuali problemi.

La questione della spiegabilità non resta confinata al piano teorico o etico: trova applicazioni immediate nel mondo industriale. Un esempio concreto è la manutenzione predittiva, dove algoritmi complessi analizzano dati provenienti da macchinari e impianti per anticipare guasti. In questo contesto, la mancanza di trasparenza può tradursi non solo in difficoltà di interpretazione, ma anche in rischi operativi ed economici significativi.

L'IA e la Manutenzione Predittiva

La manutenzione predittiva è un approccio proattivo che mira ad anticipare i guasti prima che si verifichino. A differenza del passato, quando si ricorreva soprattutto alla manutenzione preventiva o addirittura reattiva, oggi l'IA consente di analizzare grandi quantità di dati in tempo reale, rilevando segnali di anomalie e stimando con maggiore precisione il momento ottimale per intervenire.

Differenze con la manutenzione preventiva

È di fondamentale importanza distinguere tra manutenzione preventiva e manutenzione predittiva, in particolare nel contesto dell'IA. La manutenzione preventiva si basa su programmi fissi, spesso delineati dalle raccomandazioni del produttore o da dati storici generali, senza considerare il reale stato di usura dell'apparecchiatura. Ciò può comportare interventi eccessivamente frequenti o, al contrario, insufficienti.

Al contrario, la manutenzione predittiva si fonda sui dati e sullo stato attuale dell'apparecchiatura. Attraverso l'uso dell'IA, i sistemi monitorano costantemente le condizioni operative e analizzano i

dati per prevedere il momento esatto in cui un componente potrebbe guastarsi. Questo approccio dinamico e basato su evidenze risulta nettamente più efficiente e preciso rispetto alla manutenzione preventiva.

Grazie all'IA è possibile avvalersi di sensori IoT (*Internet of Things*) installati sulle apparecchiature per la raccolta continua di dati riguardanti parametri operativi quali temperatura, vibrazioni, pressione e consumo energetico. Questi ampi flussi di dati vengono successivamente analizzati da algoritmi di IA e machine learning, i quali apprendono dai dati storici e in tempo reale per sviluppare modelli predittivi. L'obiettivo è identificare segnali premonitori di potenziali guasti, anche minimi, che potrebbero sfuggire all'osservazione umana o a metodi di analisi tradizionali. L'importanza di tale approccio è duplice. In primo luogo, consente una riduzione significativa dei tempi di inattività non pianificata, che possono causare perdite economiche rilevanti per le aziende. Le fabbriche, ad esempio, possono subire una perdita compresa tra il 5% e il 20% della loro capacità produttiva a causa di guasti imprevedibili. In secondo luogo, ottimizza l'allocazione delle risorse di manutenzione, permettendo interventi mirati solo quando e dove sono realmente necessari, evitando così sprechi e prolungando la vita utile delle apparecchiature.

Vantaggi dell'IA nella manutenzione

Integrare l'IA nei processi di manutenzione significa quindi ottenere benefici tangibili su più livelli. Le previsioni accurate dei guasti permettono, anzitutto, di ridurre in modo significativo i costi legati a interventi emergenziali, fermi non programmati e sostituzioni premature di componenti. Questo approccio contribuisce anche a prolungare la vita utile delle attrezzature: intervenendo quando i problemi sono ancora agli inizi, si prevengono danni più gravi e si assicura un funzionamento stabile nel tempo. L'efficienza operativa ne risulta notevolmente migliorata, poiché diventa possibile pianificare le attività in maniera mirata, riducendo le interruzioni della produzione e aumentando la continuità dei processi. In settori delicati come l'energia o i trasporti, dove un guasto può mettere a rischio la sicurezza di lavoratori e cittadini, l'IA offre un ulteriore vantaggio: contribuisce a prevenire incidenti e a creare ambienti di lavoro più sicuri.

Gli utilizzi dell'IA non si limitano alla semplice previsione dei guasti. I sistemi intelligenti, ad esempio, possono ottimizzare i percorsi dei tecnici, calcolando in tempo reale il tragitto più efficiente in base alle priorità, ai vincoli temporali e alla posizione geografica degli impianti. Allo stesso modo, l'IA è in grado di analizzare dati storici e sintomi per proporre diagnosi precise, suggerendo le probabili cause di un malfunzionamento e le azioni correttive più adatte, riducendo così l'errore umano e accelerando la risoluzione dei problemi.

Un altro contributo rilevante riguarda l'automazione dei rapporti di intervento: i dati raccolti sul campo e le osservazioni dei tecnici possono essere trasformati automaticamente in report standardizzati e accurati. Anche la manutenzione preventiva trae vantaggio dall'IA, che analizza lo storico degli interventi e i cicli di vita delle attrezzature per pianificare in autonomia il momento più opportuno per un controllo, evitando sprechi e riducendo l'usura. Sul fronte logistico, i modelli predittivi aiutano a gestire le scorte di ricambi, prevedendo le necessità future e impedendo sia carenze sia accumuli inutili in magazzino.

Infine, l'IA supporta i manager con dashboard analitiche e report che mettono in evidenza indicatori chiave di prestazione, favorendo decisioni strategiche basate su dati affidabili. Può anche interagire direttamente con i clienti tramite chatbot, gestendo richieste di routine, organizzando interventi e migliorando così la qualità del servizio. Non meno importante è il suo ruolo nella formazione: strumenti intelligenti offrono tutorial personalizzati e simulazioni immersive, permettendo ai tecnici di acquisire competenze in modo più rapido ed efficace.

Gestione dei rischi e interventi manutentivi nell'era dell'IA

L'integrazione diffusa dell'IA nei settori industriali rende la gestione dei rischi un aspetto centrale della progettazione e dell'implementazione tecnologica. Non si tratta più di un'attività accessoria, ma di un requisito imprescindibile. L'adozione di soluzioni basate sull'IA comporta rischi specifici, diversi da quelli tradizionalmente associati alle tecnologie informatiche. Un errore di progettazione o un dataset inadeguato possono generare decisioni sbagliate o comportamenti imprevisti del sistema, con conseguenze gravi se l'IA è usata per la manutenzione predittiva. La mancanza di trasparenza, già discussa nella sfida della "black box", complica l'individuazione di bias e rende più difficile attribuire responsabilità in caso di malfunzionamenti. A ciò si aggiunge il rischio di una dipendenza eccessiva dagli algoritmi: affidarsi ciecamente alle loro raccomandazioni può ridurre la capacità critica degli operatori e portare a errori di valutazione. Anche la vulnerabilità alla cybersecurity è un problema rilevante, poiché un attacco ai dati o agli algoritmi può compromettere l'affidabilità dell'intero sistema. Infine, non vanno dimenticate le questioni etiche e legali: la tutela della privacy, la prevenzione della discriminazione algoritmica e la necessità di un quadro normativo chiaro sono temi ancora aperti.

Per affrontare queste criticità è necessario un approccio integrato. I sistemi devono essere sottoposti a test e validazioni rigorose prima dell'adozione e monitorati costantemente anche dopo l'implementazione, così da correggere tempestivamente errori, bias o comportamenti inattesi. La supervisione umana rimane un pilastro irrinunciabile: un modello in cui l'essere umano mantiene l'ultima parola nelle decisioni critiche garantisce sicurezza e offre un'occasione preziosa di apprendimento reciproco tra uomo e macchina. In parallelo, è fondamentale investire nella formazione e nella riqualificazione del personale: gli operatori devono comprendere non solo i vantaggi dell'IA, ma anche i suoi limiti e i modi migliori per interpretarne i risultati.

Come abbiamo visto un ulteriore passo verso la riduzione dei rischi può essere rappresentato dallo sviluppo di tecniche di IA spiegabile. In prospettiva, anche il rafforzamento dei quadri normativi e degli standard etici sarà determinante per assicurare un utilizzo responsabile e sicuro di queste tecnologie, soprattutto nei settori regolamentati e ad alto impatto.

In un sistema di manutenzione predittiva, la capacità di un tecnico di diagnosticare correttamente un guasto dipende anche da quanto comprende i criteri con cui il modello ha generato un'allerta. Se l'IA viene percepita come una scatola nera, le sue indicazioni rischiano di apparire arbitrarie. In questo scenario, il manutentore potrebbe eseguire diagnosi parziali o errate, oppure compiere interventi costosi e superflui in caso di falsi positivi. La mancanza di comprensione complica anche l'ottimizzazione del sistema stesso: senza conoscere come l'IA elabora i dati, diventa difficile affinare i modelli o adattare i parametri operativi.

Al contrario, un tecnico che possiede almeno una conoscenza di base dei principi con cui l'IA prende decisioni non è più un semplice esecutore, ma un collaboratore attivo del sistema. Questo gli consente di intervenire in modo più mirato, di contribuire al miglioramento continuo dei modelli e di garantire una manutenzione più precisa, sicura ed efficiente.

Aspetti etici e legali

L'evoluzione dell'IA solleva inevitabilmente questioni etiche e legali. Una delle più delicate riguarda la responsabilità: chi risponde se una decisione automatica provoca un danno? Il progettista, l'operatore, il produttore o l'utente finale? L'assenza di chiarezza dei modelli complica ulteriormente questo nodo, rendendo difficile distinguere tra errori di progettazione, malfunzionamenti tecnici o usi impropri.

Dal punto di vista etico, è essenziale che l'IA sia sviluppata e utilizzata nel rispetto dei diritti fondamentali, della privacy e della dignità delle persone. Occorre prevenire discriminazioni algoritmiche e garantire che l'IA operi nell'interesse del benessere umano. Ciò richiede un approccio multidisciplinare che coinvolga non solo tecnologi, ma anche giuristi, esperti di etica e rappresentanti della società civile.

Parallelamente, la regolamentazione dell'IA è un campo in rapido sviluppo. Governi e organizzazioni internazionali stanno lavorando per stabilire leggi e linee guida che bilancino innovazione e protezione dei diritti. I principi chiave su cui si concentrano queste normative riguardano trasparenza, responsabilità, sicurezza, tutela della privacy e supervisione umana.

Conclusioni

La comprensione della logica alla base dell'IA è cruciale non solo per sfruttarne i benefici, ma anche per ridurre i rischi e migliorare gli interventi manutentivi. La manutenzione predittiva rappresenta un esempio emblematico: qui l'IA offre vantaggi rivoluzionari, ma il suo processo intrinseco non interpretabile può diventare un ostacolo significativo se non viene accompagnata da strumenti di interpretabilità, da un'attenta supervisione umana e da un quadro normativo solido.

Per il futuro, sarà necessario progettare sistemi più trasparenti e interpretabili fin dalle prime fasi di sviluppo, implementare protocolli rigorosi di test e validazione e garantire un monitoraggio costante delle prestazioni. Anche la formazione interdisciplinare dei professionisti, capace di unire competenze tecniche, etiche e legali, sarà un fattore chiave. Infine, la collaborazione tra istituzioni, industria e ricerca potrà portare alla definizione di standard condivisi e di strumenti che rendano l'IA più accessibile anche a operatori non esperti.

La piena realizzazione del potenziale dell'IA dipenderà dalla nostra capacità di guardare oltre la superficie dei suoi risultati e di comprendere i meccanismi che li generano. Solo così sarà possibile costruire un futuro in cui l'IA non sia soltanto potente, ma anche sicura, etica e davvero al servizio della società.

3 Intelligenza artificiale e partecipazione dei lavoratori

3.1 The Filipino workers at the sharp end of AI

Théophile Simon

Sul #29 (Winter 2024) della rivista HesaMag di ETUI è stato pubblicato l'articolo "The Filipino workers at the sharp end of AI" di Théophile Simon, giornalista, che proponiamo in questa raccolta. La rivista può essere scaricata [a questo link](#). L'articolo è a pag.18.

3.2 Documenti EU OSHA: la partecipazione dei lavoratori

Rocco Vitale

Sociologo del lavoro, già docente universitario, fondatore e presidente onorario di Aifos.

3.2.1 Apprendimenti concreti per l'implementazione della gestione dei lavoratori tramite intelligenza artificiale

L'uso dell'intelligenza artificiale (IA) nella gestione dei lavoratori (AIWM) può avere impatti diversi sulla sicurezza e salute sul lavoro (SSL) dei lavoratori, a seconda delle modalità di implementazione e gestione. Esaminare casi di studio di applicazioni reali aiuta a comprendere meglio come questi sistemi vengono utilizzati nella pratica e offre indicazioni per un'implementazione efficace, riducendo al minimo i rischi associati al loro utilizzo.

Grande casa automobilistica: l'importanza del coinvolgimento dei lavoratori

Una grande casa automobilistica belga analizzata nello studio impiega circa 7.000 lavoratori, una parte significativa dei quali con contratti a tempo determinato. È stato introdotto un sistema di gestione dei lavoratori basato sull'intelligenza artificiale per migliorare l'efficienza sulla linea di montaggio attraverso la sincronizzazione delle attività. Il sistema segnalava anche gli operatori che non lavoravano da molto tempo in una determinata posizione, sollecitando la riassegnazione e la formazione.

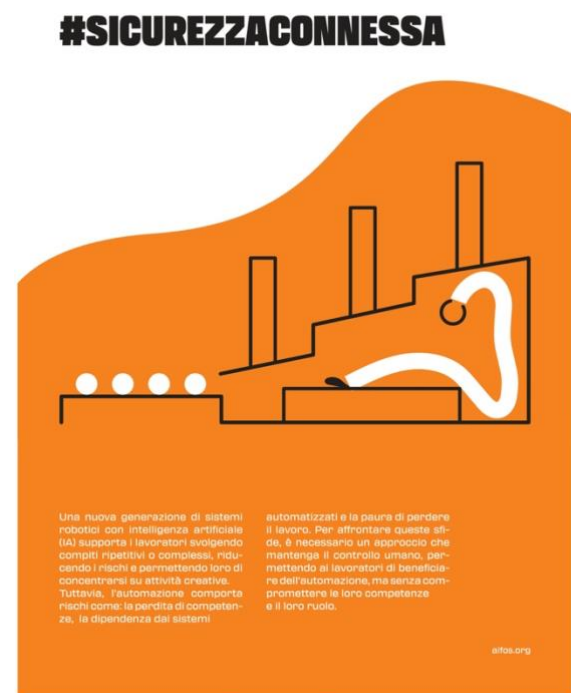
La tecnologia è stata implementata secondo un approccio gerarchico top-down, che ha ridotto al minimo le opportunità di input dei lavoratori. A seguito dell'implementazione, l'azienda ha registrato un aumento della produttività e una riduzione degli incidenti di qualità. Ciononostante, il sistema AIWM ha ridotto l'autonomia dei lavoratori e aumentato il carico di lavoro, due importanti fattori di rischio psicosociale che possono portare a stress e burnout. L'intensità di lavoro era elevata e gestita tramite rotazione delle mansioni.

Inoltre, la mancanza di supervisione umana nei processi basati sull'intelligenza artificiale ha contribuito a creare un ambiente di lavoro più ostile, in cui i lavoratori si sentivano eccessivamente monitorati e isolati. Ciò ha portato a un elevato tasso di turnover all'interno dell'azienda.

Questo caso evidenzia l'importanza di coinvolgere i lavoratori nello sviluppo e nell'implementazione di sistemi di gestione dell'ambiente di lavoro (AIWM). Un approccio dall'alto verso il basso può esacerbare i rischi psicosociali e ridurre la soddisfazione lavorativa.

Piccolo fornitore automobilistico: partecipazione e proattività sono fondamentali.

Un piccolo fornitore automobilistico italiano con 49 dipendenti ha implementato soluzioni AIWM in tutti i reparti e ruoli. Tra queste, sistemi per l'assegnazione delle attività, la comunicazione e la



condivisione delle informazioni, i controlli di qualità e sicurezza e la logistica, volti a creare flussi di lavoro più efficienti.

La tecnologia è stata progettata e sviluppata internamente, con il coinvolgimento attivo dei lavoratori in ogni fase del processo. L'azienda ha inoltre adottato un approccio proattivo in materia di SSL, consultandosi con istituti di ricerca e organizzazioni nazionali specializzate nel settore.

I sistemi AIWM hanno supportato i lavoratori nella gestione dei processi e nella risposta alle sfide utilizzando dati in tempo reale, migliorandone l'autonomia. L'approccio partecipativo ha creato un maggiore senso di appartenenza e coinvolgimento tra i dipendenti, con conseguente maggiore soddisfazione lavorativa, aumento della produttività e maggiore empowerment dei lavoratori. In definitiva, questa strategia ha contribuito a ridurre i livelli di stress, creando un ambiente di lavoro più sano.

Fornitori di servizi di ristorazione: modelli alternativi per un migliore equilibrio tra lavoro e vita privata.

Due cooperative spagnole di servizi di ristorazione a domicilio hanno adottato fin dall'inizio un approccio AIWM incentrato sul lavoratore. Le consegne vengono coordinate utilizzando uno di questi sistemi sviluppati da e per le cooperative, progettato per promuovere relazioni sindacali di supporto piuttosto che di controllo.

Grazie al coinvolgimento attivo dei lavoratori nei processi decisionali, il sistema AIWM consente un'equa distribuzione del lavoro, inclusa la possibilità di rifiutare le consegne senza penali. Questo contribuisce a mitigare i comuni rischi psicosociali del lavoro su piattaforma digitale, garantendo un'equa distribuzione del carico di lavoro, rispettando la disponibilità e le preferenze dei lavoratori e limitando lo sforzo fisico quotidiano, il tutto contribuendo a un migliore equilibrio tra lavoro e vita privata e a condizioni più sicure.

Grande azienda manifatturiera: il dialogo sociale è essenziale.

Una grande azienda manifatturiera danese, caratterizzata da alti livelli di sindacalizzazione dei lavoratori, ha gradualmente introdotto le tecnologie AIWM nelle sue linee di produzione e nelle attività amministrative. Queste tecnologie, integrate in dispositivi come smartwatch e tablet, sono state progettate per semplificare i flussi di lavoro, allocare i compiti e facilitare la comunicazione tra lavoratori e macchine.

L'azienda ha coinvolto i lavoratori e i loro rappresentanti durante l'intero processo di implementazione. Questo impegno al dialogo sociale ha contribuito ad affrontare le preoccupazioni, ridurre lo stress e garantire che i sistemi AIWM fossero introdotti in modo da supportare attivamente la salute e la sicurezza dei lavoratori.

In allegato il documento originale EU OSHA: [Digital technologies for worker management: implications for safety and health. A comparative study of two automotive companies in Belgium and Italy](#)

3.2.2 Verso sistemi di gestione dei lavoratori basati sull'intelligenza artificiale e algoritmici per luoghi di lavoro più produttivi, sicuri e sani

La scheda informativa esplora l'ascesa di Sistemi di gestione dei lavoratori (AIWM) basati su algoritmi che migliorano la produttività automatizzando le decisioni e ottimizzando l'organizzazione delle attività. Oltre ai vantaggi offerti, l'AIWM viola la privacy dei lavoratori e genera rischi psicosociali legati al lavoro, stress e una serie di altri effetti negativi sulla sicurezza, la salute e il benessere dei lavoratori.

Un approccio incentrato sull'uomo, la partecipazione dei lavoratori e un solido sistema di prevenzione e gestione della salute e sicurezza sul lavoro sono essenziali per bilanciare i vantaggi della tecnologia con la sicurezza, la salute e il benessere dei lavoratori, creando ambienti di lavoro più sicuri, più sani e più produttivi.

In allegato il documento originale EU OSHA: [Verso sistemi di gestione del personale basati su intelligenza artificiale e algoritmi per luoghi di lavoro più produttivi, più sicuri e più sani](#)

3.2.3 Intelligenza artificiale per la gestione dei lavoratori: implicazioni per la sicurezza e la salute sul lavoro

La relazione evidenzia i rischi e le opportunità in materia di sicurezza e salute sul lavoro correlati a Sistemi di gestione dei lavoratori basati sulla sicurezza (AIWM). La ricerca e i risultati sono supportati dall'analisi dei dati della Terza Indagine Europea delle Imprese sui Rischi Nuovi ed Emergenti e da interviste approfondite con esperti.

Lo studio esplora anche le possibili misure di prevenzione, sottolineando la necessità di approcci incentrati sulla persona e basati sulla "prevenzione attraverso la progettazione" per garantire la salute, la sicurezza e il benessere dei lavoratori. Viene presentata una serie di raccomandazioni per affrontare i rischi legati all'utilizzo di sistemi AIWM sul posto di lavoro.

In allegato il documento originale EU OSHA: [Artificial intelligence for worker management: implications for occupational safety and health](#)

3.2.4 Partecipazione e rappresentanza dei lavoratori: l'impatto sulla prevenzione dei rischi dei sistemi di gestione dei lavoratori dell'IA

Il rapporto analizza sistemi di gestione dei lavoratori basati sulla violenza (AIWM) in relazione ai rischi psicosociali dei lavoratori e al ruolo delle strutture di rappresentanza dei lavoratori nella prevenzione di tali rischi. Si basa sulla letteratura esistente per esaminare le conseguenze derivanti dall'AIWM e indaga su come i rappresentanti dei lavoratori possano prevenire e mitigare gli effetti indesiderati. Tuttavia, la rappresentanza dei lavoratori può incontrare ostacoli dovuti alla natura potente ma enigmatica dell'AIWM, nonché all'equilibrio di potere tra datori di lavoro e dipendenti per settore, aspetti che richiederebbero ulteriori ricerche per trovare soluzioni.

In allegato il documento originale EU OSHA: [Worker participation and representation: the impact on risk prevention of AI worker management systems](#)

Allegati

- Allegato 1: [Digital technologies for worker management: implications for safety and health. A comparative study of two automotive companies in Belgium and Italy](#)
- Allegato 2: [Verso sistemi di gestione del personale basati su intelligenza artificiale e algoritmi per luoghi di lavoro più produttivi, più sicuri e più sani](#)
- Allegato 3: [Artificial intelligence for worker management: implications for occupational safety and health](#)
- Allegato 4: [Worker participation and representation: the impact on risk prevention of AI worker management systems](#)

3.3 La partecipazione degli attori aziendali della prevenzione nella progettazione, valutazione e gestione dei rischi: criticità, opportunità, ruolo della *line* aziendale

Sonia Fagotti

Tecnico della Prevenzione

3.3.1 Premessa

La salute e sicurezza sul lavoro è oggi una dimensione strategica dell'organizzazione, che va oltre il mero adempimento normativo, diventando indicatore di maturità gestionale e capacità d'integrare sostenibilità, innovazione e competitività all'interno dei propri processi. In questo contesto, la prevenzione si configura come leva culturale per garantire continuità operativa, benessere organizzativo e affidabilità reputazionale.

L'evoluzione normativa e tecnologica ha favorito il passaggio da un approccio documentale a una cultura organizzativa della prevenzione. In tale scenario, il coinvolgimento della "*line* aziendale" – ovvero chi presidia operativamente i processi produttivi – è prerequisite fondamentale per politiche efficaci di tutela della salute e sicurezza dei lavoratori.

L'intelligenza artificiale (IA) rappresenta una trasformazione che incide sulla struttura del lavoro, sulla valutazione del rischio e sulle relazioni organizzative. L'IA si configura come strumento di supporto per la gestione della sicurezza – tramite analisi predittiva, automazione e tracciamento – ma introduce anche rischi emergenti: opacità decisionale, riduzione dell'autonomia, stress da sorveglianza. Serve quindi una governance partecipata che valorizzi le competenze di RSPP/ASPP, dirigenti, preposti, medici competenti e HSE manager, promuovendo una mediazione tra innovazione e tutela.

Il compito delle figure della prevenzione si evolve così da applicazione prescrittiva a mediazione progettuale tra innovazione e tutela, tra trasformazione tecnologica e sostenibilità organizzativa.

La progettazione, la valutazione e la gestione dei rischi richiedono oggi una partecipazione consapevole e sistemica, capace di integrare l'intelligenza umana con quella artificiale in modo critico e responsabile. La partecipazione richiede strutture chiare, strumenti condivisi e una visione trasversale, adeguata alla complessità crescente degli ecosistemi produttivi contemporanei.

3.3.2 Opportunità e criticità dell'intelligenza artificiale dal punto di vista della *line* aziendale

La transizione digitale offre strumenti che, se utilizzati con consapevolezza, possono rafforzare il lavoro operativo. Automatizzazione, analisi predittiva, monitoraggio intelligente: tali tecnologie promettono efficienza e offrono molteplici opportunità di strutturare un sistema di gestione della salute e sicurezza efficace, favorendo il passaggio da una logica reattiva a una proattiva. Tuttavia, queste tecnologie, se non governate, introducono nuove criticità ed aree di rischio, non sempre evidenti né regolamentate in modo chiaro.

3.3.2.1 Criticità dell'adozione dell'IA nei contesti lavorativi

L'introduzione dell'IA nei luoghi di lavoro impone nuove responsabilità in materia di salute, sicurezza, etica e privacy, richiedendo una revisione attenta delle modalità di valutazione dei rischi. In aderenza al D.Lgs. 81/2008, art.18 co.1 lett. z, il datore di lavoro deve aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi e all'evoluzione tecnologica, integrando nel DVR i rischi legati all'uso di sistemi intelligenti.

Inoltre, il Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, c.d. AI ACT, recentemente approvato, classifica come “ad alto rischio” quei sistemi IA che hanno un impatto significativo su sicurezza, salute e diritti delle persone (come algoritmi per l’assunzione, selezione, valutazione e licenziamento dei lavoratori, o IA per la gestione dei turni o la sorveglianza dei dipendenti), che potrebbero rappresentare proprio i sistemi di intelligenza artificiale utilizzati nel contesto SSL, obbligando alla conformità con rigorosi requisiti di trasparenza, valutazione dei rischi, supervisione umana e audit periodici.

Gli algoritmi predittivi, i sistemi di monitoraggio automatizzato e le interfacce uomo-macchina evolute possono generare rischi inediti: dalla perdita di controllo operativo in caso di malfunzionamento, alla diffusione di *bias* decisionali, fino a effetti psicosociali come ansia da sorveglianza o dequalificazione del ruolo umano.

La posta in gioco non è solo l’efficienza, ma la qualità del lavoro, la fiducia nei sistemi digitali e la tenuta etica del contesto produttivo. È quindi fondamentale che chi opera nella prevenzione non assista passivamente alla transizione tecnologica, ma ne assuma un ruolo di guida.

Le Linee Guida del Ministero del Lavoro e delle Politiche Sociali per l’implementazione dell’IA nel mondo del lavoro (v.0.7, 2024)²² offrono un primo orientamento per imprese e professionisti: definiscono principi generali per un uso responsabile dell’IA e raccomandano specifiche misure a tutela dei lavoratori. La sicurezza, oggi, non riguarda solo l’ambiente fisico, ma anche il modo in cui i dati vengono trattati, le prestazioni monitorate e le decisioni gestite dagli algoritmi.

La *line* aziendale ha un ruolo cruciale in questo processo: può rilevare tempestivamente le criticità derivanti dall’uso dell’IA, fungere da interfaccia tra i lavoratori e i progettisti dei sistemi, proporre correttivi di natura organizzativa e promuovere una cultura della trasparenza algoritmica.

Le sopra citate Linee Guida del Ministero del Lavoro prevedono l’istituzione di referenti per l’etica tecnologica e la formazione su aspetti giuridici e tecnici dell’uso dell’IA, in aderenza al AI ACT Reg. UE 2024/1689 che ha stabilito l’obbligo per datori di lavoro e formatori di garantire un livello adeguato di alfabetizzazione in materia di IA per tutto il personale coinvolto. Questa indicazione impone di formare la *line* aziendale all’uso consapevole degli strumenti di IA impiegati nei processi operativi, stimolando una maggiore comprensione dei rischi e delle responsabilità connesse all’affidamento alle tecnologie intelligenti.

Queste indicazioni si inseriscono nel quadro delle raccomandazioni di EU-OSHA²³ e ILO, le quali sottolineano l’urgenza di affrontare queste problematiche con strumenti tecnici, normativi e culturali adeguati.

Le stesse pubblicazioni, indicano chiaramente che automatizzazione, analisi predittiva e sistemi di sorveglianza comportano nuovi rischi, tra cui:

- **Stress psicosociale**, l’introduzione dell’IA può incidere negativamente sul benessere dei lavoratori, generando fenomeni di alienazione, perdita di significato e percezione di controllo a causa della sorveglianza costante. Ulteriori fattori di rischio includono la diminuzione dell’autonomia decisionale (soprattutto quando i lavoratori non sono coinvolti nei processi), l’ansia da prestazione e l’incremento del ritmo lavorativo imposto dalla cosiddetta “frusta digitale”²⁴).

²² MLPS - Linee Guida IA v0.7

²³ EU-OSHA (2023), invita a includere i “nuovi rischi emergenti” derivanti dalla digitalizzazione – tra cui anche bias algoritmici, sorveglianza e perdita di controllo umano – nei documenti di valutazione dei rischi (DVR).

²⁴ EU-OSHA (2023), Foresight on new and emerging OSH risks associated with digitalisation by 2025, p. 31.

- **Opacità decisionale**, sistemi IA che non siano monitorati o correttamente addestrati possono fornire indicazioni scorrette nei casi in cui le scelte algoritmiche non siano trasparenti o comprensibili, con impatto diretto sulla sicurezza.
- **Bias sistemici**, alcuni sistemi predittivi possono produrre discriminazioni, ad esempio nei modelli di sorveglianza del comportamento o nella valutazione delle performance, dovute all'uso di dati storici distorti o parziali.
- **Deskilling**, l'affidamento eccessivo all'automazione può determinare una progressiva perdita di competenze da parte dei lavoratori, ciò impoverisce il patrimonio operativo dell'organizzazione e genera vulnerabilità nei momenti critici in cui è indispensabile l'intervento umano.
- **Rischi etici**, inclusa la discriminazione nei sistemi di sorveglianza o nelle valutazioni di performance.
- **Perdita di controllo da parte della linea aziendale e dei lavoratori**, alcuni sistemi IA automatizzano i processi e conseguentemente anche la direzione del lavoro, togliendo autonomia sia ai lavoratori che ai supervisor. Questo riduce il ruolo attivo del *middle management* nella valutazione del contesto, nel sostegno al lavoratore e nel trasferimento della cultura della sicurezza.

Le figure per la sicurezza della *line* aziendale si trovano quindi ad affrontare le seguenti implicazioni per contrastare le criticità da IA:

- **integrare i rischi associati all'IA nel DVR aziendale**, ogni introduzione significativa di tecnologia IA richiede una nuova valutazione dei rischi, compresi quelli indiretti; in particolare, l'esposizione prolungata a strumenti digitali può influire in modo differenziale sulle funzioni cognitive dei lavoratori in base all'età, incidendo su carico mentale, capacità attentiva e percezione del controllo operativo.
- **Formazione e coinvolgimento**: i preposti e capi reparto devono essere formati non solo all'uso dello strumento, ma anche alla sua comprensione critica, sia su competenze tecniche, sia sui diritti connessi all'uso dei dati. Il fine è fornire le competenze affinché la *line* aziendale possa contrastare l'impatto culturale e organizzativo, scongiurando la riduzione del ruolo decisionale ed il conseguente indebolimento della leadership operativa nella gestione partecipata della SSL.
- **Sorveglianza dinamica**: i sistemi intelligenti vanno contestualizzati e monitorati nel tempo, istituendo referenti o comitati etici interni per il monitoraggio delle tecnologie intelligenti, per evitare che vengano percepiti come "scatole nere" incontestabili.
- **Partecipazione**: i lavoratori devono essere parte del processo attivo di co-progettazione, per promuovere accettabilità e sicurezza integrata.

L'introduzione dell'IA nel mondo del lavoro incontra resistenze culturali e barriere strutturali. Da un lato la gestione della salute e sicurezza nei luoghi di lavoro è ancora troppo spesso percepita come responsabilità esclusiva del datore di lavoro o dell'RSPP, invece che come valore condiviso. Dall'altro, pressioni produttive, rigidità organizzative e frammentazione operativa (es. subappalti e supply chain) ostacolano la circolazione delle informazioni e limitano la partecipazione effettiva delle diverse componenti aziendali, rendendo più difficile un'integrazione efficace delle tecnologie intelligenti nei processi di prevenzione.

La *line* aziendale, pertanto, svolge un ruolo chiave nell'affrontare questa sfida e fungere da interfaccia tra i sistemi intelligenti e l'esperienza operativa, a partire dall'individuazione delle anomalie fino alla proposta delle azioni correttive. È quindi indispensabile interpretare in modo

critico le decisioni automatizzate, guidandone l'applicazione sia sotto il profilo etico sia gestionale. Questa capacità riflessiva deve essere strutturalmente integrata nella cultura organizzativa e nel ciclo continuo della prevenzione.

In definitiva, nell'era dell'intelligenza artificiale è necessario promuovere un cambio di paradigma nella sicurezza sul lavoro: l'IA deve essere progettata tenendo conto della realtà operativa e della soggettività umana, dove tecnologia, competenze e diritti devono procedere insieme.

3.3.2.2 Opportunità: l'IA come leva per una prevenzione distribuita

Accanto alle criticità, l'adozione di tecnologie intelligenti può rappresentare un'opportunità concreta per favorire la partecipazione e il miglioramento continuo nella prevenzione. Sistemi digitali per il reporting dei *near-miss*, sensori indossabili (cd. *wearable*), dashboard condivise in tempo reale: tutte queste soluzioni, se ben progettate, permettono di ridurre il tempo tra rilevazione e azione, ampliando il coinvolgimento di tutti gli attori della salute e sicurezza. La vera innovazione da apportare ed accrescere, tuttavia, non sta solo nella raccolta del dato, ma nella sua interpretazione condivisa. È qui che entra in gioco la *line* aziendale in quanto l'efficacia di tali strumenti dipende sempre dalla maturità della condizione organizzativa e dalla reale volontà di integrare la sicurezza nelle logiche decisionali.

In questo senso, l'IA può abilitare una prevenzione:

- continua, grazie al monitoraggio in tempo reale,
- mirata, tramite la personalizzazione degli interventi,
- scientifica e **data-driven**, fondata sull'analisi di evidenze oggettive.

3.3.3 Monitoraggio e prevenzione dei rischi attraverso l'IA

A supporto della prevenzione dinamica, l'adozione di sistemi di IA per il monitoraggio dei comportamenti e delle condizioni di lavoro offre strumenti avanzati per l'identificazione precoce dei rischi. In particolar modo, le principali funzioni sono:

- **Sorveglianza ambientale:** attraverso sensori IoT²⁵, o sistemi e apparecchiature combinate con IA, è possibile monitorare in tempo reale condizioni pericolose (ad es. variazioni di temperatura, umidità, presenza di gas tossici, fumo, sversamenti, assenza DPI, presenza di persone in aree vietate). Generalmente i dati raccolti vengono analizzati in tempo reale per garantire che l'ambiente di lavoro rimanga sicuro. Inoltre, tecnologie IoT possono essere montate su mezzi di movimentazione merci (es. caricatori frontali, transpallet, doppiatori, etc) in grado di rilevare la presenza di pedoni, ostacoli, di rallentare o arrestare il mezzo in caso di necessità, o di effettuare lo *zoning* intelligente al fine di regolare automaticamente le velocità dentro e fuori o in zone indicate.
- **Monitoraggio in tempo reale:** sistemi di IA possono monitorare continuamente le condizioni fisiologiche del lavoratore e inviare allarmi in caso di situazioni pericolose. Ad esempio, sensori collegati a dispositivi indossabili possono rilevare segni di affaticamento e stress nei lavoratori e avvisare i preposti o colleghi.
- **Tracciamento della posizione:** dispositivi indossabili come smartwatch o braccialetti intelligenti possono tracciare la posizione dei lavoratori, facilitando i soccorsi in caso di

²⁵ IoT, l'Internet of Things, ovvero definita come una rete di dispositivi fisici connessi a Internet che possono raccogliere e scambiare dati senza intervento umano. Tali dispositivi sono anche definiti "oggetti intelligenti" e generalmente si compongono di sensori, sistemi di connessione, sistemi di elaborazione dati ed interfaccia utente. Essendo la definizione molto ampia, tra queste tecnologie troviamo un'ampia gamma di dispositivi, dagli smartwatch ai simulatori, dagli esoscheletri ai sensori industriali.

emergenza. Ad esempio, i dispositivi tag Rfid²⁶ integrati nelle divise o nelle attrezzature possono monitorare la presenza e i movimenti dei lavoratori.

- **Equipaggiamento protettivo e accessi del personale autorizzato:** attraverso i sistemi di riconoscimento facciale e biometrico si può garantire che solo il personale autorizzato possa accedere a determinate aree e che i lavoratori indossino correttamente i dispositivi di sicurezza prima di entrare in ambienti ad alto rischio.
- **DPI IoT - Dispositivi di Protezione indossabili intelligenti (smart DPI):** dispositivi indossati dai lavoratori integrati con IA, come caschi, tute o badge connessi, possono monitorare la postura rilevando quella scorretta, le esposizioni prolungate, lo sforzo fisico, i segnali vitali, le anomalie termiche e quelle acustiche. Il valore aggiunto di questi sistemi non sta solo nella rilevazione, ma nella capacità predittiva, che consente di attivare contromisure prima che l'incidente si verifichi.
- **Manutenzione predittiva:** sensori connessi e algoritmi IA sono in grado di rilevare segnali di degrado su impianti e macchinari, prevenendo guasti che potrebbero causare infortuni.
- **Analisi predittiva degli incidenti:** l'IA è in grado di consentire l'elaborazione grandi volumi di dati storici (infortuni, *near-miss*, anomalie) per individuare con accuratezza e puntualità pattern ricorrenti e prevedere situazioni a rischio.

Nell'ambito della prevenzione aziendale, il monitoraggio continuo rappresenta la base di partenza per predire, o comunque per rilevare tempestivamente, le condizioni critiche, segnali deboli e variazioni anomale nei parametri di rischio, e su questo campo l'IA può rappresentare un enorme vantaggio integrando il ruolo della *line* aziendale. Quest'ultima, in genere, costituisce l'avamposto del monitoraggio: osserva dinamiche, comportamenti, guasti incipienti e deviazioni dalle procedure. In questo quadro, l'IA non sostituisce, ma integra il ruolo dei datori di lavoro, dirigenti e preposti alla sicurezza nel monitoraggio dei rischi, amplificando il loro contributo e riducendo l'errore umano. L'IA può accrescere questa sensibilità attraverso sistemi di monitoraggio dinamico, manutenzione predittiva o clustering degli incidenti, ma la qualità e l'utilità del sistema dipendono dal ruolo delle figure aziendali gestionali nella progettazione, nella raccolta e nella validazione dei dati.

In tal senso, i datori di lavoro, dirigenti e preposti, sono chiamati a svolgere un duplice ruolo: essere sensori umani, capaci di cogliere i segnali premonitori, e catalizzatori dell'azione preventiva, attraverso segnalazioni strutturate, micro-interventi correttivi e proposte di miglioramento, completando il dato digitale con la conoscenza esperienziale.

Un'interessante conferma della necessità di integrare monitoraggio tecnologico e osservazione umana proviene da uno studio sperimentale condotto da Aloini et al. (2021)²⁷ in un hub logistico italiano. La ricerca ha impiegato sensori indossabili per raccogliere, in tempo reale, dati ambientali, fisiologici e comportamentali relativi ai lavoratori impegnati in attività di movimentazione merci. L'obiettivo era comprendere l'impatto delle condizioni operative sul benessere e sulle performance, e individuare pattern ricorrenti utili alla prevenzione. Dal punto di vista manageriale, lo studio suggerisce l'adozione di una gestione individualizzata del personale logistico. È utile considerare le caratteristiche psicofisiche e comportamentali di ciascun operatore per ottimizzare i risultati, progettare turni e ambienti di lavoro adeguati e migliorare il benessere dei lavoratori. Lo studio ha

²⁶ Rfid, Radio Frequency Identification, è una tecnologia di riconoscimento, di identificazione e di memorizzazione automatica digitale. I dispositivi con questa tecnologia consentono la rilevazione del tag grazie alla capacità di rispondere a chiamate di prossimità da parte di dispositivi attivi.

²⁷ ALOINI, D., FRONZETTI COLLADON, A., GLOOR, P., GUERRAZZI, E., & STEFANINI, A. (2022). Enhancing operations management through smart sensors: measuring and improving well-being, interaction and performance of logistics workers.

dimostrato infatti che le prestazioni lavorative e il benessere percepito non sono determinati solo da carichi fisici o ambienti ostili, ma anche da variabili “soft”, come lo stato emotivo, la qualità dell’interazione tra colleghi o il tipo di attività svolta. Tali fattori, spesso invisibili alla mera strumentazione tecnologica, diventano intelligibili solo se letti con il contributo della *line* operativa. Il monitoraggio intelligente non può prescindere da una gestione partecipata e dal coinvolgimento diretto di chi, sul campo, traduce il dato in azione. Infatti, come lo studio suggerisce, per rendere il monitoraggio una leva efficace di prevenzione, è necessario passare dalla raccolta passiva alla costruzione condivisa del dato. Solo la sinergia tra sensori e supervisor può trasformare la raccolta di informazioni in un reale strumento di governo della sicurezza operativa. Solo chi vive quotidianamente il processo può definire quali variabili osservare, con quale frequenza, e quali soglie rappresentano realmente condizioni anomale.

Il monitoraggio partecipato non solo migliora la capacità predittiva del sistema aziendale, ma rafforza anche la cultura della responsabilità diffusa e della sicurezza come valore condiviso. La formazione della *line* su strumenti di reporting, audit di processo e principi di ergonomia cognitiva rappresenta quindi un investimento strategico.

In particolare, il coinvolgimento dei preposti può rappresentare uno snodo essenziale. La loro posizione intermedia tra i vertici aziendali e la base operativa li rende figure chiave ai fini del compimento delle misure di prevenzione. Ma per far sì che il loro ruolo sia davvero efficace, devono essere formati non solo sugli obblighi giuridici, ma anche su aspetti di leadership, gestione del rischio dinamico e comunicazione organizzativa. La recente giurisprudenza, così come le modifiche normative introdotte dopo il D.L. 146/2021²⁸ ed il recente Accordo Stato – Regioni in tema di percorsi formativi in materia di salute e sicurezza²⁹, vanno in questa direzione, attribuendo al preposto un ruolo centrale e attivo nella prevenzione.

La partecipazione, in definitiva, non è solo uno strumento, ma una postura organizzativa. È la capacità di vedere nella pluralità degli sguardi un valore e non un ostacolo. L’intelligenza artificiale si affianca a quella collettiva che si attiva quando le persone si sentono coinvolte, riconosciute, responsabilizzate. E in un mondo del lavoro che cambia rapidamente, quest’ultima forma di intelligenza delle organizzazioni è la vera risorsa per affrontare le nuove sfide della sicurezza.

3.3.2.3 Caso studio: due aziende, due diversi impatti dell’IA

È particolarmente utile richiamare i risultati del recente studio EU-OSHA (2024)³⁰ per analizzare il diverso impatto che le tecnologie di gestione del lavoro basate sull’IA, hanno avuto sulla salute e sicurezza dei lavoratori appartenenti a due aziende del settore automobilistico, una in Belgio e una in Italia.

Dallo studio emerge come un approccio partecipativo all’introduzione delle tecnologie digitali, come nel caso studio italiano, favorisca una percezione positiva dell’innovazione, migliorando il benessere lavorativo, l’ergonomia e la comunicazione tra reparti. L’adozione di stazioni di lavoro automatizzate e di strumenti digitali condivisi è risultata efficace nel ridurre il carico fisico e lo stress da prestazione, grazie anche a una maggiore autonomia operativa e al coinvolgimento attivo dei lavoratori nella progettazione.

Al contrario, l’adozione di un approccio decisionale organizzativo di tipo *top-down* (ovvero dall’alto verso il basso), come osservato nel caso belga, ha determinato un aumento dei livelli di sorveglianza, una riduzione del controllo decisionale e un maggior turn-over, con effetti negativi sul clima

²⁸ Decreto Legge 21 ottobre 2021, n. 146, convertito con modificazioni dalla Legge 17 dicembre 2021, n. 215.

²⁹ Rep. atti n. 59/CSR del 17 aprile 2025.

³⁰ EU-OSHA, (2024). Digital technologies for worker management: implications for safety and health. A comparative study of two automotive companies in Belgium and Italy.

organizzativo e sulla salute psicosociale. In quest'ultimo caso, la rigidità degli strumenti di assegnazione automatizzata delle mansioni e la limitata trasparenza sui dati raccolti hanno alimentato sensazioni di alienazione e incertezza.

La ricerca sottolinea come i rischi psicosociali – ansia da monitoraggio, perdita di autonomia, deskilling – non siano effetti collaterali inevitabili, ma conseguenze di scelte organizzative. La governance dell'IA in azienda deve quindi essere ispirata a criteri di trasparenza, inclusività e precauzione, con un ruolo attivo delle figure della prevenzione, delle rappresentanze sindacali e della *line* aziendale. In questo modo l'innovazione può tradursi in un reale progresso per la sicurezza, la qualità del lavoro e la sostenibilità organizzativa.

3.3.3 Analisi dei dati infortunistici con tecniche di clustering (raggruppamento automatico)

L'applicazione di algoritmi di machine learning per l'analisi dei dati infortunistici rappresenta oggi una concreta opportunità operativa per il Servizio di Prevenzione e Protezione e per la *line* aziendale. In particolare, le tecniche di "clustering non supervisionato" consentono di individuare pattern ricorrenti nei dati anche in assenza di etichette predefinite (di cui quindi non si conosce a priori la categorizzazione, o l'appartenenza a classi specifiche³¹), organizzando gli eventi in gruppi omogenei (cluster) in base a caratteristiche simili o condivise, come tipo di evento, orario, mansione, esperienza o condizioni ambientali.

Algoritmi come K-Means e DBSCAN permettono di rilevare correlazioni tra fattori di rischio eterogenei, fornendo una base analitica per azioni preventive mirate. Tuttavia, la loro efficacia dipende fortemente dalla qualità, completezza e contestualizzazione dei dati raccolti. È qui che il ruolo della *line* aziendale diventa cruciale: grazie alla sua prossimità ai processi produttivi, può garantire una raccolta dati accurata e tempestiva, arricchita da elementi qualitativi spesso invisibili all'analisi automatica.

Tuttavia, l'efficacia di questi strumenti dipende in larga parte dalla qualità e dalla granularità dei dati raccolti, elemento su cui la *line* aziendale gioca un ruolo determinante, in quanto deve poter garantire una raccolta dati accurata, tempestiva e contestualizzata. La conoscenza approfondita del ciclo operativo, delle anomalie ricorrenti e dei near-miss da parte delle figure aziendali della prevenzione, consente di inserire nel sistema informativo elementi qualitativi che arricchiscono l'analisi statistica. In molti casi, la rilevazione di eventi a basso impatto ma ad alta frequenza (quasi incidenti, microtraumi, situazioni borderline) è possibile solo se promossa e valorizzata da chi è presente quotidianamente in reparto. Questi strumenti, accessibili anche tramite software open-source (es. Orange, KNIME), consentono agli RSPP/ASPP o HSE Manager, di rivelare pattern non evidenti all'analisi tradizionale e superare le consuete aggregazioni descrittive, avviando azioni mirate su gruppi di rischio emergenti e ridefinendo le priorità del DVR.

Questo tipo di strumento è funzionale solo se la *line* aziendale viene coinvolta non come mero esecutore, ma come co-analista e co-interprete dei dati. Inoltre, il feedback che la linea operativa fornisce all'RSPP è essenziale per validare o rivedere le ipotesi generate dagli algoritmi. In questo senso, l'IA non sostituisce l'esperienza, ma ne amplifica la portata, trasformando l'intuito operativo in conoscenza strutturata.

Resta fondamentale dotare la *line* aziendale delle competenze digitali minime per interagire con dashboard, strumenti di *data entry* e piattaforme di reportistica, nonché promuovere una cultura

³¹ INAIL, (2024) Quaderni di Ricerca, RECKON: Tecnologie abilitanti per il monitoraggio degli elementi di contesto (Operatore-Macchina Ambiente) per la prevenzione di incidenti sul lavoro, p.33.

della segnalazione e dell'apprendimento basato sui dati. Solo così l'analisi predittiva può trasformarsi in prevenzione proattiva.

3.3.4 L'intelligenza artificiale come spinta per orientare comportamenti

Un ambito emergente e strategico in cui la *line* aziendale può esercitare un ruolo trasformativo è l'applicazione del *nudging* supportato da algoritmi predittivi e tecnologie di intelligenza artificiale al fine di orientare comportamenti sicuri. Le *smart nudges* (letteralmente "spinte intelligenti" o "gentili") in ambito di tutela della salute e sicurezza dei lavoratori, si realizzano attraverso micro-interventi ambientali o digitali (anche appunto con applicazioni di IA) che orientano il comportamento dei lavoratori, inducendoli a scelte più sicure senza limitare la libertà individuale.

Ad esempio, negli ambienti industriali è possibile attivare segnali visivi dinamici (come luci LED o messaggi digitali) che, tramite sensori IoT e modelli predittivi, segnalano automaticamente condizioni di rischio (come livelli eccessivi di rumore o prossimità a macchinari in movimento), inducendo il lavoratore a spostarsi o a indossare i DPI corretti. Allo stesso modo, nei cantieri, badge intelligenti o dispositivi indossabili possono attivare alert personalizzati quando un lavoratore entra in un'area riservata o ad alto rischio, senza ricorrere a interventi coercitivi. Un esempio di applicazione in ambito logistico è quello dei sistemi di *zoning* applicati ai mezzi di movimentazione merci, che regolano dinamicamente la velocità del veicolo in funzione della presenza di pedoni, spingendo l'operatore a mantenere comportamenti più prudenti.

In tutti questi casi, la chiave di successo sta nell'adattività e nella trasparenza degli strumenti: i lavoratori devono percepire l'intervento tecnologico come un supporto e non come un controllo invasivo.

Per essere efficaci e accettabili, queste *nudges intelligenti* devono essere integrate nella strategia di prevenzione con il contributo attivo della *line* aziendale, che dovrebbe provvedere in particolare ai seguenti aspetti:

- **contestualizzazione dei dati:** attraverso il filtro dei *false positive* algoritmici e validazione della rilevanza dei segnali in base alla reale dinamica di lavoro;
- **mediazione della comunicazione uomo-macchina:** evitando sovraccarico informativo, ansia da sorveglianza o percezione punitiva dei feedback;
- **individuare soluzioni localizzate:** sfruttando le informazioni di campo per personalizzare le soglie di attivazione delle *nudges*, rendendole culturalmente e operativamente efficaci;
- **valutazione dell'impatto sul clima di sicurezza:** mediante osservazioni o *safety walks* congiunti tra RSPP, preposti e lavoratori.

L'impiego consapevole dell'IA nei meccanismi di *nudging* può rappresentare un potente strumento per orientare i comportamenti verso una sicurezza proattiva. Il *nudging* supportato dall'intelligenza artificiale può diventare una leva trasformativa per la prevenzione aziendale quando integrato con intelligenza relazionale e operativa. La sua efficacia non risiede tanto nella sofisticazione tecnologica, quanto nella capacità della *line* aziendale di mediare tra gli output digitali e la realtà quotidiana del lavoro, trasformando l'informazione in azione concreta, accettata e sostenibile. In particolare, alcuni soggetti della *line* aziendale come dirigenti e preposti, grazie alla loro posizione intermedia tra il datore di lavoro ed i reparti, possono agire da facilitatori e garanti di prossimità, avendo la possibilità di osservare, testare e personalizzare questi micro-interventi, ad esempio monitorando l'efficacia delle strategie di *nudging*, correggendone gli effetti indesiderati (come il rischio di stress o percezione di sorveglianza), e promuovendo una diffusione coerente.

3.3.5 Conclusioni

Tecnologie emergenti di IA e nuove metodologie mettono oggi a disposizione strumenti potenti per la prevenzione. Tuttavia, la differenza continua a farla il fattore umano. Infatti, l'IA non porta risposte definitive e preconfezionate, ma solleva nuove domande su cosa intendiamo per rischio, su chi lo definisce, su come lo si affronta. L'adozione dell'IA nel campo della sicurezza sul lavoro può generare benefici concreti – in termini di prevenzione, efficienza e benessere – solo se accompagnata da un'evoluzione del modello organizzativo, che preveda, in particolare, la partecipazione della *line* aziendale nella progettazione, valutazione e gestione dei rischi.

L'efficacia delle tecnologie intelligenti non dipende solo dalla loro precisione tecnica, ma dalla capacità di inserirsi in un sistema vivo, fatto di relazioni e cultura. La sicurezza, dunque, non si automatizza: si costruisce nel dialogo tra dati e persone, tra modelli e contesti, tra previsioni e giudizi esperti.

La sfida non è adottare l'IA, ma imparare a governarla nel concreto delle pratiche quotidiane perché sia efficace nella prevenzione dei rischi per la salute e sicurezza e affinché i rischi da questa indotti vengano mitigati. E questo è possibile solo se la conoscenza esperienziale della linea operativa entra nei processi decisionali, diventando parte integrante del ciclo della prevenzione. È in questa alleanza tra tecnologia e responsabilità distribuita che si gioca il futuro della sicurezza sul lavoro.

Bibliografia

- INAIL, (2025). *Piano delle attività di Ricerca 2025-2027*. [https://www.google.com/search?q=INAIL%2C+\(2025\).+Piano+delle+attivit%C3%A0+di+Ricerca+2025](https://www.google.com/search?q=INAIL%2C+(2025).+Piano+delle+attivit%C3%A0+di+Ricerca+2025)
- MLPS, (2024). *Linee Guida IA v0.7*. <https://partecipa.gov.it/processes/LineeGuidaIALavoro>
- AI ACT – REGOLAMENTO UE 2024/1689 (13/06/2024). *Regolamento sull'intelligenza artificiale*. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689
- INAIL, (2024) Quaderni di Ricerca, RECKON: Tecnologie abilitanti per il monitoraggio degli elementi di contesto (Operatore-Macchina Ambiente) per la prevenzione di incidenti sul lavoro. https://olympus.uniurb.it/index.php?option=com_content&view=article&id=31496:reckon24&catid=98&Itemid=126
- EU-OSHA, (2024). *Digital technologies for worker management: implications for safety and health. A comparative study of two automotive companies in Belgium and Italy*. <https://osha.europa.eu/it/publications/digital-technologies-worker-management-implications-safety-and-health-comparative-study-two-automotive-companies>
- EU-OSHA, (2023). *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025*. European Agency for Safety and Health at Work. https://osha.europa.eu/sites/default/files/Event%20summary_23.pdf
- EU-OSHA, (2022). *Artificial intelligence for worker management: implications for occupational safety and health*. <https://osha.europa.eu/it/publications/digital-technologies-worker-management-implications-safety-and-health-comparative-study-two-automotive-companies>
- EU-OSHA, (2022). *Artificial intelligence for worker management: an overview*. <https://osha.europa.eu/it/publications/artificial-intelligence-worker-management-overview>
- EU-OSHA, (2022). *L'intelligenza artificiale per la gestione del personale: misure di prevenzione*.

- <https://osha.europa.eu/it/publications/artificial-intelligence-worker-management-prevention-measures>
- RAPPORTO TECNICO UNI TR 11858:2022. *Tecnologie IoT nell'impiego dei DPI – Indicazioni relative all'integrazione di sistemi elettronici nella gestione e nell'utilizzo dei dispositivi di protezione individuali.*
- ILO, (2025). *Rivoluzionare la salute e la sicurezza sul lavoro. L'intelligenza artificiale e la digitalizzazione nel mondo del lavoro*, Roma: Ufficio internazionale del lavoro. https://www.ilo.org/sites/default/files/2025-04/rivoluzionare_la_salute_e_la_sicurezza_sul_lavoro.pdf

Altri contributi accademici e specialistici

- MELE, CRISTINA & RUSSO SPENA, TIZIANA & KAARTEMO, VALTTERI & MARZULLO, MARIA LUISA, (2021). *Smart nudging: come le tecnologie cognitive abilitano architetture di scelta per la co-creazione di valore*, Journal of Business Research , Elsevier, vol. 129(C), pagine 949-960.
- ALOINI, D., FRONZETTI COLLADON, A., GLOOR, P., GUERRAZZI, E., & STEFANINI, A. (2022). *Enhancing operations management through smart sensors: measuring and improving well-being, interaction and performance of logistics workers*. The TQM Journal, 34(2), 303–329.
- KAHNEMAN, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux.
- THALER, R.H., & SUNSTEIN, C.R. (2008). *Nudge: Improving Decisions About Health, Wealth and Happiness*. Yale University Press.
- LI, G., BAI, J. (2008). *Cluster analysis on occupational injury data*. Safety Science, 46(9)

3.4 La partecipazione degli attori aziendali della prevenzione nella progettazione, valutazione e gestione dei rischi. Criticità, opportunità, ruolo dei lavoratori e dei loro rappresentanti

*Cinzia Maiolini **

*Alessio De Luca ***

** Segretaria nazionale Filctem Cgil*

*** Responsabile Ufficio 4.0 CGIL nazionale*

Lo sviluppo e la diffusione di nuove tecnologie portano con sé la necessità di ricercare continuamente un equilibrio tra i rischi che esse possono introdurre e gli innegabili benefici, con la consapevolezza che le utilità prodotte non sempre sono proporzionali al rischio.

Il tema della salute e sicurezza nell'epoca delle implementazioni digitali è centrale ma l'approccio all'analisi del rapporto tra salute e la sicurezza sul lavoro e uso di strumenti digitali deve essere bivalente.

1) Da un lato è indubbio che l'utilizzo integrato delle nuove tecnologie possa consentire una miglior tutela di lavoratori e lavoratrici. A questo tema è infatti dedicato il nuovo Rapporto mondiale dell'Organizzazione Internazionale del Lavoro (OIL), intitolato "Rivoluzionare la salute e la sicurezza sul lavoro. L'intelligenza artificiale e la digitalizzazione nel mondo del lavoro". (Aprile 2025)

I sistemi utilizzabili per garantire maggiore sicurezza possono essere sia proattivi che reattivi.

Si possono utilizzare TIC - tecnologie dell'informazione e comunicazione- come, ad esempio, computer o dispositivi mobili, ma anche cobot, ossia robot collaborativi, videocamere, dispositivi indossabili, droni, microfoni, esoscheletri, realtà virtuale e realtà aumentata e ancora l'identificazione a radio frequenza, sistema che utilizza onde di radiofrequenza per automatizzare la raccolta dei dati.

Esiste insomma una complessità di sistemi che possono o meno essere supportati da IA e consentono una implementazione certa della sicurezza in ambito lavorativo.

Proviamo a fare qualche esempio concreto di possibilità di applicazione di nuove tecnologie al fine di evitare rischi:

- In primo luogo parliamo dei DPI (dispositivi di protezione individuale). La sensorizzazione dei DPI consentirebbe, in prima battuta, di verificare che i lavoratori li stiano indossando ma se ne può monitorare anche il corretto utilizzo e il possibile deterioramento. Si potrebbe dunque pensare ad ambienti di lavoro il cui accesso sia consentito solo previa rilevazione di corretta dotazione di DPI. Esistono già sperimentazioni in merito che prevedono la sensorizzazione di indumenti, scarpe antinfortunistiche e caschi che sono in grado di produrre un alert anche in caso di non corretto posizionamento.
- Dispositivi tecnologici che possono, in generale, monitorare tutti i fattori ambientali di un qualsiasi luogo di lavoro. Temperature, luminosità, rumore, radiazioni, vibrazioni, salubrità dell'aria sono monitorabili: esistono ad esempio tecnologie wearable come quella che, mettendo insieme sistemi di localizzazione wireless, tecniche di intelligenza artificiale a basso costo energetico, connessione al cloud e sensori innovativi, è utilizzabile per rilevare gas nocivi e polveri sottili. Un progetto di multi sensore per il monitoraggio degli ambienti di lavoro (SALVO) è stato implementato a partire dal 2020 da ENEA, Università di Catania e STMicroelectronics. Il dispositivo può essere applicato ai DPI.
- Nel 2019 è terminato anche il progetto BRIC ID 12/2016, il cui obiettivo era lo sviluppo di nuovi sensori per composti organici volatili (COV), intesi come componenti di strumenti di

lettura diretta per poter misurare in tempo reale la concentrazione di sostanze chimiche pericolose nell'aria dei luoghi di lavoro in modo affidabile

- Body cameras e smart glasses possono consentire al lavoratore di ricevere un supporto da remoto nello svolgimento di una attività lavorativa.
- Riproducendo virtualmente ambienti di lavoro (digital twin) si possono testare possibili interventi manutentivi prima di esporre gli esseri umani a rischi evitabili
- Esistono poi innumerevoli applicazioni di sistemi wearable "uomo a terra" in grado di segnalare la mancanza di movimento e la posizione non eretta di operatori/trici che lavorino in ambienti isolati.

L'elenco potrebbe continuare ma ciò che ci interessa è indicare come, già oggi, siano molteplici le possibilità di combinazione delle tecnologie esistenti per garantire maggiore sicurezza in ambito lavorativo.

A questo é bene aggiungere che, in Europa, si è avviata una campagna di EU-Osha sulla salute e sicurezza sul lavoro nell'era digitale. Come è noto l'Agenzia europea per la sicurezza e la salute sul lavoro è nata nel 1994 e ha come missione è rendere i luoghi di lavoro più sicuri, sani e produttivi.

Il documento EU-OSHA (<https://osha.europa.eu/it/publications/smart-digital-monitoring-systems-occupational-safety-and-health-implementation-workplace>) include alcune raccomandazioni chiave per le aziende per implementare e integrare i possibili sistemi di monitoraggio in modo efficace. Nello specifico:

1. comprendere le reali esigenze del luogo di lavoro. Questo si deve tradurre in **una consultazione continua con i lavoratori ed i loro rappresentanti**, per capire le reali necessità, problemi di sicurezza e le misure da adottare per affrontarli. E questo è un elemento di primaria rilevanza perché il tema della salute e sicurezza prevede necessariamente il coinvolgimento attivo e la informazione di tutti gli attori coinvolti.
2. **mettere i lavoratori al centro del processo**. I lavoratori vanno dunque coinvolti nella sperimentazione, attuazione ed ottimizzazione di tali sistemi, ne devono comprendere il funzionamento, debbono essere formati.
3. **favorire il dialogo e la comunicazione**, ossia va mantenuto un canale di comunicazione aperto tra lavoratori e professionisti della SSL anche in itinere, per discutere di eventuali problemi e possibili miglioramenti. Inoltre, **i lavoratori devono essere informati sui loro diritti e responsabilità in relazione ai sistemi digitali di monitoraggio**.

Qui dunque si propone un importante elemento di valutazione, che attiene il necessario rispetto delle norme vigenti a riguardo della tutela della privacy, della necessaria informativa sulla raccolta e conservazione dei dati, sulla finalità di utilizzo, la loro gestione condivisa con enti preposti alla valutazione e tutela della salute e della sicurezza e con gli RLS, e l'indicazione specifica di diritti ed obblighi in capo a lavoratori/ lavoratrici e datori di lavoro. Questo aspetto a nostro avviso è il tema che obbliga al coinvolgimento delle rappresentanze sindacali unitarie e delle OO.SS.

Del resto su questo aspetto abbiamo già le norme di riferimento cui appellarsi per un ruolo attivo delle rappresentanze dei lavoratori:

- art 4 e art 8 della legge 300/70 (Statuto dei lavoratori)
- GDPR, meglio noto come Regolamento sul trattamento dei dati personali
- IA act (in vigore da febbraio 2025)

Fermi restando i disposti della legge 300/70, che implicano il principio di non discriminazione (art 8) e indicano le fattispecie di coinvolgimento OBBLIGATORIO delle RSU (art 4) il Regolamento sulla

protezione dati (GDPR) specifica infatti che il datore di lavoro, nell'effettuare i controlli sui lavoratori, è obbligato a rispettare i principi generali in materia di tutela dei dati personali:

- [principio di necessità](#): il controllo deve risultare necessario o indispensabile rispetto ad uno scopo determinato ed avere il carattere della eccezionalità, limitato nel tempo e nell'oggetto, mirato e mai massivo;
- [principio di finalità](#): il controllo deve essere finalizzato a garantire la sicurezza o la continuità aziendale, o a prevenire e reprimere illeciti;
- [principio di trasparenza](#): il datore di lavoro deve [informare](#) preventivamente i dipendenti sui limiti di utilizzo degli strumenti e delle sanzioni previste nel caso di violazione di tali limiti;
- [principio di proporzionalità](#): il datore di lavoro deve adottare forme di controllo strettamente proporzionate e non eccedenti lo scopo della verifica;
- [principio di sicurezza](#): i dati raccolti devono essere protetti in modo adeguato

Dunque, è del tutto evidente che il sindacato e gli RLS non possono prescindere dal richiedere le informazioni di cui sopra all'atto della implementazione di sistemi che, anche ai fini di maggiore sicurezza sul luogo di lavoro, raccolgano dati di lavoratrici e lavoratori. Questo ci riguarda specificamente rispetto ai vari accordi proposti e sottoscritti in tema di prevenzione rischi.

L'IA ACT stabilisce poi come siano da considerarsi ad ALTO RISCHIO tutti i sistemi di IA applicati al lavoro. Se infatti sono vietati i sistemi per identificare o desumere emozioni nel contesto lavorativo, viene considerata ad alto rischio l'intelligenza artificiale applicata alle assunzioni, alle decisioni relative alle condizioni lavorative, al monitoraggio del lavoro e nell'assegnare mansioni o promozioni. Il Regolamento, inoltre, all'art 4 pone un obbligo di alfabetizzazione in materia di intelligenza artificiale.

Pare dunque chiaro che il mero richiamo all'art 4 della Legge 300/70 sia indispensabile ma NON sia sufficiente in caso di accordi di implementazione di tecnologie digitali che rilevino dati dei lavoratori.

Del resto tra le attività che [L'art. 33 del D. Lgs. 81/08](#) specifica debbano essere effettuate dal SPP, troviamo il garantire che lavoratori e lavoratrici siano informati e informate sulla prevenzione degli infortuni (e dunque, diremmo noi, degli strumenti utilizzati a tal fine) e sulla corretta gestione delle situazioni di emergenza. Sul versante di salute e sicurezza, vi è una connessione diretta tra valutazione dei rischi predisposta dal Regolamento UE sulle applicazioni di IA e la normativa del D.lgs. n. 81/2008 (DVR).

Proprio in tale ambito le linee guida della Commissione Europea individuano una eccezione al divieto nell'uso di IA con riconoscimento emotivo nei luoghi di lavoro, se questa è utilizzata per la salvaguardia della salute del lavoratore, ma questa predisposizione non può che essere frutto di confronto sindacale per escludere diverse finalità. È chiaro che su questa fattispecie è necessaria la contrattazione e la definizione di un accordo per quanto chiaramente stabilito dall'art. 4 della legge 300, oltre l'azione prevista sempre nella legge 300, per quanto riguardo il ruolo centrale del medico competente. Il ruolo delle RLS diviene centrale e la formazione adeguata strumento imprescindibile per esercitare i connessi diritti/doveri.

Non vi è dubbio poi che, grazie al combinato disposto delle diverse norme citate e dei CCNL applicati, che sempre più ampliano il diritto dei lavoratori e delle loro rappresentanze ad essere informati e coinvolti (vedi da ultimo CCNL elettrici e CCNL chimico farmaceutici), la richiesta di un sempre maggior coinvolgimento dei rappresentanti dei lavoratori nell'utilizzo di tecnologie finalizzate alla protezione dei rischi per la salute e la sicurezza è supportata da norme solide.

Nel momento in cui viene consegnato questo contributo è stato licenziato un disegno di legge cd "DDL semplificazioni" che intende modificare nuovamente l'art 4 della legge 300/70 inserendo nel comma 2 "gli strumenti, i dispositivi e le attrezzature funzionali a garantire la tutela della salute e sicurezza sul lavoro". Dunque, secondo la proposta, anche per questi strumenti e dispositivi NON sarebbe più richiesto il preventivo accordo collettivo stipulato con le RSU/RSA.

È del tutto evidente, per tutto quanto sopra scritto, che escludere l'accordo preventivo all'utilizzo di questi dispositivi, che per loro stessa natura raccolgono dati relativi all'attività lavorativa svolta e consentono un controllo pervasivo, impedirebbe di fatto l'esercizio di un ruolo negoziale di tutela e controllo da parte di lavoratrici e lavoratori coinvolgendo gravemente tutele e garanzie.

2) L'altra faccia della medaglia attiene invece i rischi correlati **all'utilizzo di tecnologie digitali**. Da un canto vi è il tema della responsabilità, da intendersi come cattivo funzionamento del sistema digitalizzato, quando non dovuta a dolo, colpa grave o negligenza dell'utilizzatore.

Dall'altro i rischi per la salute, materiali ed immateriali: vi sono rischi legati all'uso della **robotica** ed alla **automazione del lavoro per malfunzionamento o eccessiva intensificazione delle attività**, e specifiche fattispecie di esposizione ad alcune tipologie di rischio quali quelli derivanti dalla **presenza di campi elettromagnetici, disturbi muscolo-scheletrici** legati all'utilizzo di specifici supporti, **disturbi visivi, disturbi dell'udito, disturbi del sonno**.

Vi è poi una ampia gamma di rischi di tipo **psico-sociali** emergenti in ambito lavorativo già riportati da diversi studi, rischi derivanti dalla sempre maggiore autonomia delle componenti tecnologiche, dal deficit di trasparenza degli algoritmi, dal funzionamento del processo decisionale della tecnologia, dalla maggiore difficoltà di concentrazione conseguente all'utilizzo prolungato di alcune tecnologie, dalla perdita di autostima. In particolare sul tema dei rischi si sono già approfonditi studi sul lavoro agile.

Anche in questo ambito è in corso una campagna europea che si basa su cinque temi prioritari di attenzione specifica: lavoro su piattaforma digitale, robotica avanzata e intelligenza artificiale, telelavoro, sistemi digitali intelligenti e gestione dei lavoratori tramite l'intelligenza artificiale.

La Cgil, nelle diverse Federazioni e a livello Confederale, ha svolto e svolge percorsi di formazione specifica. Ma gli stessi contratti collettivi nazionali ed il richiamo alle disposizioni della Direttiva sul lavoro in piattaforma, utilizzabili in modo estensivo anche in contesti di lavoro non specificatamente di piattaforma, consentono di prevedere una formazione continua e un coinvolgimento ex ante dei rappresentanti dei lavoratori/trici.

Qualche esempio di buona contrattazione lo abbiamo nei recenti rinnovi del Contratto del settore elettrico 2025-2027, laddove si prevede la costituzione di un Osservatorio sui temi delle transizioni, compresa quella digitale, cui possano partecipare anche esponenti del mondo accademico o esperti: uno dei compiti dell'Osservatorio sarà esaminare l'applicazione dell'IA ACT. Parimenti sono previsti incontri preventivi di confronto e consultazione in merito agli impatti dell'IA.

Anche nel più recente CCNL chimico farmaceutico si sono individuate linee guida specifiche in tema di IA, che ribadiscono la centralità della persona e le azioni necessarie per la responsabilizzazione nell'utilizzo di sistemi di IA, attraverso regole chiare e adeguata formazione ed informazione. Inoltre, vi si prevede tra le altre cose la necessità di un utilizzo etico inclusivo e sostenibile, che passa da una valutazione ex ante degli impatti conseguenti ad implementazioni di IA e la promozione della dignità, dei diritti e delle libertà della persona. E infine, come elementi necessari per la gestione di strumenti di IA, si prevede la necessaria informazione preventiva alle

RSU sull'introduzione di sistemi di IA con coinvolgimento dei lavoratori perché possano comprenderne scopi e funzionamento.

Dunque, coinvolgimento, informazione e formazione.

Per fare formazione è importante il coinvolgimento anche di docenti ed esperti sia sui temi di SSL sia anche su normazione europea, su IA act, sui temi attinenti alla tutela della privacy, necessitando il tema, come sempre accade in questo ambito, di un approccio multidisciplinare.

La Filctem Cgil ha già implementato, proprio sfruttando le potenzialità date dall'utilizzo di strumenti digitali anche come supporto fruibile da lavoratrici e lavoratori, Rsu ed RLS, una app su salute e sicurezza (<https://www.collettiva.it/copertine/lavoro/salute-e-sicurezza-le-trovi-sullapp-i6qfo3gd>) costantemente aggiornata, che si pensa di implementare con tutti i materiali relativi all'utilizzo possibile di nuove tecnologie in questo ambito ed alla contrattazione dell'implementazione delle stesse, proprio al fine di provare a fornire una sorta di vademecum normativo ed una serie di casi di specie capaci di agevolare una corretta negoziazione.

Come più volte abbiamo sostenuto il quadro regolatorio esistente consente già un esercizio importante, sia a monte che a valle delle nuove implementazioni tecnologiche, del ruolo delle rappresentanze dei lavoratori anche e soprattutto in ambiti, come questo, determinanti per le condizioni di vita di ciascuno. In particolare, sui temi della salute e sicurezza è necessario utilizzare al meglio le opportunità offerte dalle nuove tecnologie senza violare i diritti dei cittadini/lavoratori e prevenendo già i rischi materiali ed immateriali che possiamo sia ragionevolmente sia scientificamente prevedere.

4 La formazione per la sicurezza con l'intelligenza artificiale per gestire il cambiamento

4.1 Intelligenza Artificiale al servizio della Formazione: quale approccio efficace per la Sicurezza sul Lavoro alla luce degli scenari attesi.

Matteo Cozzani

CEO securON® - esperto di safety e security e consulente di direzione

L'approccio alla formazione applicata alla sicurezza sul lavoro richiede sensibilità e responsabilità in relazione alla funzione etica e sociale connessa alla tutela della salute e dell'incolumità dei Lavoratori. Questo principio non va mai dimenticato per non incorrere nel rischio che ogni approfondimento su questioni tecniche, normative o formali correlate, induca a perdere di vista lo scopo ultimo che resta quello della prevenzione.

Per tale ragione, la formazione applicata alla sicurezza sui temi della salute e sicurezza deve essere

opportunamente ed eticamente orientata all'efficacia e al pragmatismo.

Perseguendo tale principio, si anticipa una digressione preliminare per tentare di correggere i limiti di un approccio che troppo spesso si focalizza unicamente sulla funzione educativa, o conoscitiva, della formazione rispetto ad obiettivi effettivi di salute e prevenzione dei lavoratori.

Molto spesso si attribuisce all'errore umano la causa principale degli incidenti (diverse fonti autorevoli indicano una incidenza compresa tra l'80 ed il 90 %).

Per questo, nel tempo si sono sviluppate dottrine e metodi incentrati sullo sviluppo del comportamento sicuro (si pensi ad esempio alla BBS) ed è un metodo diffuso, se non consolidato, quello di finalizzare la formazione al cambiamento dei comportamenti attraverso le nozioni e i concetti trasmessi.

Tuttavia, pur tenendo presente la rilevanza dei comportamenti, bisogna considerare la formazione una opportunità di potenziamento dell'individuo piuttosto che uno strumento di regole formali di mera applicazione.



Il lavoro su piattaforma digitale offre nuove opportunità, facilitando così l'incontro tra la domanda e l'offerta. Tuttavia, i lavoratori affrontano rischi, come il basso potere contrattuale, l'alto controllo e la mancanza di protezione, andando, però, incontro alla possibilità di isolamento,

stress e sorveglianza digitale. Essendo generalmente autonomi, sono responsabili della loro sicurezza sul lavoro e le piattaforme non sono obbligate a fornire misure di protezione.

aiifos.org

La capacità di attenzione e la consapevolezza situazionale sono abilità individuali importantissime per un sistema di prevenzione e svilupparli attraverso una attività formativa evoluta. Per questo, all'affacciarsi di nuovi e potenti strumenti, non va persa l'occasione di considerare e potenziare questi fattori.

A titolo di paradigma, cito il noto studio di Abraham Wald, un ungherese esperto di statistica che collaborava con la RAF durante la II Guerra Mondiale, coinvolto nell'analisi dei fori dei proiettili sugli

aerei rientrati dalle missioni in territorio nemico. L'intento dello studio era quello di individuare i punti della carlinga da rinforzare in modo da rendere gli aerei meno vulnerabili.³²

Fu quindi determinante il contributo di Wald che propose un contro-intuitivo "ragionamento in negativo", suggerendo di proteggere le parti illese perché probabilmente erano quelle che, se colpite, avrebbero causato l'abbattimento impedendo ovviamente il rientro.

Analogamente, secondo un approccio di "ragionamento in negativo", quando un incidente viene correlato al fattore umano è probabile che ciò sia dovuto al mancato funzionamento della capacità correttiva normalmente attuata dal lavoratore, ovvero che si tratti probabilmente di un'eccezione a un sistema o un processo progettato male, ma umanamente compensato.

Come osservava Platone, "L'istruzione è l'accensione di un fuoco, non il riempimento di un recipiente"

Per questo, se pensiamo agli scopi perseguiti dalla formazione per la sicurezza sul lavoro l'Intelligenza Artificiale deve contribuire ad accendere tale fuoco.

Quale ulteriore esempio divergente: Hans Monderman, pioniere del "shared space", insegnava che rimuovere vincoli apparenti (strisce pedonali, semafori, segnaletica) eleva la soglia di attenzione dei conducenti e riduce gli incidenti, perché restituisce la responsabilità all'individuo (approccio adottato da sette Comuni in Germania, Belgio, Olanda, Danimarca e Gran Bretagna).

In sintesi, Monderman riteneva che per cambiare il comportamento delle persone si deve cambiare il contesto ambientale.

Analogamente, nella formazione alla sicurezza sul lavoro, le procedure lineari possono contribuire a ridurre i comportamenti non sicuri e quindi il rischio, riducendo le probabilità di accadimento dell'incidente, ma una seria politica di prevenzione necessita anche e soprattutto di motivazione e di un pensiero laterale, che, ad oggi, è proprio il "tallone d'Achille" della rigorosa e algoritmica Intelligenza Artificiale.

Si aggiunga inoltre che la formazione alla sicurezza deve comprendere anche la capacità di reagire alle situazioni di emergenza, contesto che richiede abilità di preparazione con un allenamento (esercitazioni pratiche) ed il giusto mind setting.

Queste premesse sono ancor più necessarie se ci proiettiamo negli scenari prossimi futuri del lavoro dove gli umani verranno impiegati in attività residuali, rispetto a tutti i processi che saranno oggetto di automazione e "robotizzazione" nei quali si rende indispensabile la peculiare capacità umana del fare ed adattarsi, oltre al fatto che non siamo culturalmente e normativamente pronti (giustamente!) per delegare alle macchine le fasi decisionali critiche.

Uno scenario insieme avveniristico e sorprendentemente vicino, ma allo stesso tempo inquietante, nel quale dobbiamo immaginare gli umani sempre più dedicati a funzioni critiche ed apicali per le quali necessiteranno quindi di grandi ed affinate capacità che richiederanno sostanziali upskilling e reskilling.

Si aggiunga nel contempo una riflessione opposta e preoccupante rispetto a queste prospettive, ovvero che si realizzi invece il rischio di una assuefazione determinata da questi "ADAS" (sistemi di assistenza alla guida - metaforicamente parlando) che l'Intelligenza Artificiale apporterà al lavoro ed in conseguenza alle azioni di Sicurezza, attraverso i quali potrebbero in qualche modo atrofizzarsi le

³² Questo metodo fu perfezionato dagli statunitensi che operavano in Algeria, sempre durante la Seconda guerra mondiale, che portò un notevole contributo alla teoria della probabilità e che, negli anni successivi portò Nobert Wiener alla pubblicazione del primo studio informativo relativo alla cibernetica.

preziose capacità peculiari e creative dell'essere umano la cui reattività e plasticità necessitano appunto di allenamento e stimoli.

Ma allora, come l'Intelligenza Artificiale può collocarsi ed essere correttamente implementata per diventare un alleato prezioso per la formazione dedicata alla sicurezza sul lavoro, alla luce di questi scenari?

Oggi è necessario tener conto che l'insegnamento a tutti i livelli e per tutte le fasi evolutive, deve competere con le diffuse forme di intrattenimento digitale che sono capaci di potenti ed ammalianti stimolazioni.

Partendo dall'esperienza maturata sul campo non dobbiamo dimenticare che stiamo generalmente trattando una didattica applicata ad adulti ormai lontani dai banchi di scuola, talvolta con un livello di educazione medio, per questo il docente/formatore ha oggi la necessità di rendere la formazione fruibile, attrattiva e coinvolgente (vanno bene i giochi d'aula, il role playing, i video di Napo, però nell'attuare la formazione in materia di salute e sicurezza è necessario mantenere un adeguato rigore formale e sostanziale per non rischiare di svilire il tema in termini di credibilità ed autorevolezza).

Ecco quindi, che le potenzialità dell'intelligenza artificiale possono costituire un ausilio determinante a patto che il docente/formatore od ente formativo la impieghino in modo appropriato, usando creatività e insieme buon senso, ancor meglio se scevro da tentazioni commerciali "catchy" e sensazionalistiche.

D'altro canto, l'intelligenza artificiale ha in sé le potenzialità di risolvere vari vincoli e problemi connessi alla consueta attività didattica:

- È in grado di valutare il livello di conoscenza e di misurare costantemente la capacità di adattarsi a nuovi stimoli e a nuovi livelli di competenza dei discenti.
- Consentirebbe di realizzare l'insegnamento personalizzato "one to one"
- Può attingere da una conoscenza praticamente totale rispetto allo scibile umano ed è virtualmente a prova di errore, sempre che vi sia un uso corretto delle fonti
- Non è inficiata da transfer emotivo negativo o condizionante
- Non perde mai la pazienza...
- È disponibile all'interazione 24 ore su 24, consentendo così pause affinché la mente umana elabori ed interiorizzi, ma è pronta a rispondere e ad alzare l'asticella degli stimoli in qualsiasi momento.
- Può "ascoltare" il discente a tempo indeterminato
- Valuta con obiettività gli output del discente.

Insomma, rischiando di essere banali, vale la pena ribadire che nell'implementare l'Intelligenza Artificiale dobbiamo usare prudenza, misura e responsabilità, rinunciando alla tentazione di abusarne col rischio di abusarne troppo correndo il rischio o di "buttare via il bambino insieme all'acqua sporca" perdendo cioè quel "mestiere" di cui dispongono solo i formatori ed i docenti preparati.

Presto capiremo che l'Intelligenza Artificiale è uno strumento potente che tra le regolamentazioni attese (colmando le gravi lacune oggi esistenti) dovrebbe servire, chiamiamola, una "patente" almeno per chi la usa per realizzare applicazioni sensibili o almeno che venga definito un serio codice etico e linea guida per l'applicazione responsabile nella formazione, soprattutto se tratta di sicurezza sul lavoro!

I formatori, ovvero coloro che poi sono chiamati a formare le persone ed a coinvolgere i lavoratori devono essere i soggetti principalmente coinvolti in queste azioni.

In concreto l'intelligenza artificiale può offrire una serie di Vantaggi applicativi nella formazione che si possono così riassumere:

1. Supporto in fase di macro-progettazione del progetto formativo e nella personalizzazione dei percorsi
 - Può aiutare nell'analisi del contesto e del bisogno formativo
 - Può implementare algoritmi di adaptive learning che profilano il singolo utente e modulano contenuti e ritmo in base alle sue competenze e lacune.
2. Supporto al docente in fase di micro-progettazione e predisposizione del materiale didattico
 - Può proporre al docente delle micro-progettazioni alternative affinché lo stesso ragioni criticamente e selezioni la migliore combinazione
 - Può aiutare il docente nella ricerca dei contenuti.
 - Può generare immagini ed animazioni ad hoc
3. Consente l'integrazione di simulazioni immersive e realtà virtuale (utili per la formazione e l'addestramento simulato alla risposta emergenziale).
 - L'Intelligenza Artificiale integrandosi con ambienti realtà virtuale offrirebbe l'opportunità di esercitazioni realistiche di situazioni ad alto rischio, riducendo i costi rispetto alle esercitazioni tradizionali (spesso cartacee o solo illustrate) e aumentando l'impatto emotivo ed il coinvolgimento dei discenti.
4. Offre l'accessibilità multilingue e on-demand
 - Chatbot e traduttori automatici possono rendere i materiali fruibili in diverse lingue, garantendo omogeneità di standard formativo.
5. Consente una verifica dell'apprendimento più approfondita ed efficace rispetto ai metodi tradizionali
 - Grazie all'analisi semantica consentita dall'Intelligenza artificiale, si potranno superare i limiti intrinseci dei test a risposte multiple, implementando interazioni e domande aperte per una verifica più approfondita e allo stesso tempo oggettiva dell'apprendimento, offrendo inoltre uno stimolo supplementare ai discenti consapevoli dell'efficace vaglio finale.
6. Consente una verifica dell'efficacia dell'apprendimento in fasi successive
 - Attraverso "cold test" o, meglio ancora, integrandosi con sistemi di analisi comportamentale, consentirebbe di monitorare nel tempo l'efficacia della formazione, offrendo un feedback prezioso per modulare interventi correttivi.

La premessa ed una prima conclusione di questi aspetti consistono nella verifica delle fonti. Navigare sul web sarà la cosa più disastrosa in quanto gli aspetti commerciali, farlocchi e del tipo "clicca qui e la formazione è fatta", sono in agguato. Naturalmente a nessuno sfugge che le potenzialità di automazione del lavoro possa servire a ridurre il carico di lavoro connesso alle fasi operative pericolose, monotone e ripetitive.

Lo stesso vale anche per l'organizzazione e lo sviluppo dell'attività formativa. L'Intelligenza Artificiale potrà contribuire a soluzioni di aspetti burocratici ed amministrativi, solo formali e non sostanziali, liberando così più risorse per lo sviluppo e l'incremento degli aspetti con maggiore valore aggiunto, come la valutazione dei rischi, l'analisi del fabbisogno e la stesura di seri progetti formativi.

Si deve quindi scongiurare la possibilità che la l'Intelligenza Artificiale venga speculativamente impiegata solo per automatizzare e ridurre i costi complessivi, ma possa invece essere impiegata per offrire agli operatori della formazione l'opportunità di concentrarsi sugli aspetti qualitativi.

L'adozione efficace dell'Intelligenza Artificiale nella formazione per la sicurezza sul lavoro richiede un prezioso equilibrio tra innovazione tecnologica, etica e rispetto delle persone, considerando i limiti e i pericoli suddetti in caso di impiego sconsiderato o abuso.

Aristotele affermava che «La vera saggezza consiste nel conoscere i limiti della propria intelligenza». Per questo l'Intelligenza artificiale, affinché serva sul serio a potenziare l'individuo, deve costituire uno strumento di supporto al formatore, che rimane quindi il vero custode dell'esperienza e dell'empatia nel processo didattico, senza perdere di vista l'elemento umano quale ingrediente essenziale per una cultura della sicurezza e un approccio al lavoro attento e responsabile.

4.2 Le ricadute formative previste dall'accordo Stato-Regioni con l'utilizzo dell'intelligenza artificiale

Carlo Zamponi * e Rocco Vitale**

*Responsabile Ufficio Formazione e Referente SGQ Arta Abruzzo, Consigliere Nazionale Aifos, Docente a contratto presso Università degli Studi dell'Aquila.

**Sociologo del lavoro, già docente universitario, fondatore e presidente onorario di Aifos.

L'introduzione dell'intelligenza artificiale (AI) nei luoghi di lavoro rappresenta un ulteriore passo verso l'evoluzione delle metodologie formative in quanto attraverso l'utilizzo di algoritmi avanzati capaci in breve tempo di analizzare i dati raccolti consente, fra l'altro, di valutare l'efficacia formativa misurando l'impatto della formazione sui lavoratori e sull'organizzazione.

L'utilizzo di questi sistemi restituisce al *management* aziendale *feedback* personalizzati poiché i dati e le informazioni processati danno modo di monitorare in tempo reale i progressi dei lavoratori e facilitano, pertanto, l'individuazione delle aree di miglioramento. Tutto questo al fine di facilitare la pianificazione, la progettazione e la programmazione di eventi formativi adattati alle esigenze individuali e assicurare all'organizzazione stessa che le conoscenze, le competenze e le abilità acquisite dai singoli collaboratori siano applicate e rese disponibili nello specifico contesto lavorativo.

Questo approccio personalizzato non solo aumenta l'efficacia della formazione, ma contribuisce anche a migliorare la motivazione e l'*engagement* dei lavoratori che vedono riconosciute e valorizzate le loro peculiarità e i loro bisogni formativi. Inoltre, facilita il lavoro del *management* aziendale, dato che questo processo di valutazione *work in progress* permette di apportare eventuali correttivi in tempo reale ottimizzando così l'investimento formativo e garantendo il raggiungimento degli obiettivi prefissati.

4.2.1 La valutazione di impatto

Il tema della valutazione degli impatti sugli eventi formativi è attualmente, purtroppo, una delle attività meno esplorate. La stessa, tuttavia, rappresenta una componente essenziale per attribuire un valore e un peso oggettivo in termini di efficacia e di appropriatezza alle attività formative erogate.

Sul posto di lavoro, i comportamenti e i cambiamenti organizzativi sono influenzati da molte variabili quali il clima, inteso come benessere organizzativo, la *leadership*, la comunicazione, le risorse strumentali e le tecnologie utilizzate. Queste variabili, se non gestite preventivamente in modo partecipato tra tutti gli attori del sistema aziendale, possono vanificare gli effetti della formazione erogata.

Pertanto, per le aziende è importante verificare che i propri dipendenti siano soddisfatti della formazione cui hanno partecipato, considerando che un aspetto è la verifica delle conoscenze acquisite e della soddisfazione dei partecipanti, un altro è la valutazione degli impatti delle competenze e della soddisfazione dei lavoratori sulle *performance* aziendali.

Difatti, se la formazione aziendale mira a migliorare la produttività, gli impatti misurano, attraverso i cambiamenti negli indicatori di produttività, l'efficacia nel tempo delle attività formative.

Alla base di queste considerazioni, il recente Accordo Stato Regioni³³, finalizzato alla individuazione della durata e dei contenuti minimi dei percorsi formativi in materia di salute e sicurezza, richiede al *management* aziendale di valutare l'efficacia della formazione non solo alla fine dell'evento formativo, ma anche a distanza di tempo per verificare le ricadute nell'organizzazione.

³³ ASR del 17 aprile 2025 in GU Serie Generale n.119 del 24.05.2025.

4.2.2 L'intelligenza artificiale dalla produzione alla formazione

L'AI consente (o dovrebbe consentire) attraverso l'utilizzo di algoritmi avanzati capaci in breve tempo di analizzare i dati raccolti, di valutare l'efficacia formativa misurando l'impatto della formazione sui lavoratori e sull'organizzazione.

Nei settori produttivi, l'uso e l'integrazione di sistemi per la gestione dei lavoratori basati sull'intelligenza artificiale (*AI-based worker management - AIWM*) è in aumento, specialmente nei settori industriali con processi produttivi complessi. Una ricerca dell'Agenzia Europea per la Sicurezza e la Salute sul Lavoro³⁴ (EU-OSHA) ha analizzato le implicazioni di tali sistemi su fattori relativi a sicurezza e salute in ambito lavorativo sottolineando come si evidenzia una differente organizzazione del lavoro in relazione al benessere dei lavoratori e la salute e la sicurezza in diversi contesti organizzativi.

Gli stessi sistemi, nel migliorare la produttività e semplificando le operazioni possono, se non opportunamente gestiti, influire sull'autonomia dei lavoratori, sulla qualità del lavoro e, non ultimo, sui rischi psicosociali e sulla sicurezza e sulla salute.

La nuova dimensione del lavoro comporta inevitabilmente nuovi modelli di valutazione dei rischi e conseguentemente nuovi modelli e strumenti di formazione.

Di tutto ciò vi è ben poca evidenza e scarsa innovazione nel recente Accordo Stato Regioni che, oltre all'accorpamento degli accordi esistenti, doveva individuare due specifici aspetti:³⁵

- a) modalità della verifica finale di apprendimento obbligatoria per i discenti di tutti i percorsi formativi e di aggiornamento obbligatori in materia di salute e sicurezza sul lavoro;
- b) modalità delle verifiche di efficacia della formazione durante lo svolgimento della prestazione lavorativa

In relazione alla verifica finale dell'apprendimento è dedicato un capitolo dell'Accordo che però si conclude con una semplicistica tabella che prevede le modalità di verifica tramite un colloquio o un test, precisando che i test a risposte multiple sono costituiti da un numero minimo di 30 domande da svolgersi al di fuori delle ore di formazione.

Di fatto si è ricopiato tale quale il sistema di verifica previsto per il Modulo A del corso per RSPP dell'Accordo del 7 luglio 2016 con la differenza che nel 2016 "si consigliava di somministrare i test in itinere" mentre nel nuovo Accordo "i test sono somministrabili anche in itinere".

Resta il fatto che se un test di 30 domande su un corso di 24 ore può avere una motivazione³⁶, allorquando il corso è di 4, 6 o 8 ore non può valere la medesima regola. Peraltro, lo stesso nuovo Accordo si contraddice in relazione ai corsi per gli operatori addetti alla conduzione delle attrezzature di cui all'art. 73, c. 5 del D. Lgs. 81/2008.

³⁴L'EU-OSHA è l'Agenzia dell'Unione Europea nel campo della sicurezza e della salute sul Lavoro.

³⁵ Decreto Legge 21 ottobre 2021, n. 146, convertito dalla legge 17 dicembre 2021, n. 215 che ha modificato l'art. 37, comma 2 del D. Lgs. 81/2008.

³⁶ La formazione, che non può comportare oneri economici a carico dei lavoratori si svolge durante l'orario di lavoro (art. 37, c.12). Ciò significa che al termine di una mezza giornata di corso/lavoro di 4 ore svolto presso un ente formatore è necessario rientrare in aula per il tempo di effettuare il test, la correzione da parte del docente e l'individuazione dei singoli lavoratori che ne hanno superato, con esito positivo, almeno il 70% delle domande. Quanto tempo sarà necessario? Il tempo che serve è la risposta esatta! Invece assisteremo ad un silenzio "concordato" che prevede le firme sul registro per 4 ore, le fotocopie dei test fatti e corretti (senza sapere né quando né dove si sono svolti). Non era più semplice scrivere che le ore di formazione sono comprensive della verifica finale lasciando al docente, nella propria responsabilità, la responsabilità della verifica e della formazione!

In relazione alle verifiche finali per detti corsi è prevista solamente una prova pratica mentre entrando nel dettaglio di ogni singola attrezzatura è prevista una verifica intermedia, dopo il modulo teorico-tecnico, consistente in un questionario a risposta multipla. Ma non è lo stesso questionario di 30 domande (!).

In questo quadro laddove la legge demandava all'Accordo di definire "modalità di verifica" vi è abbastanza confusione o meglio chi l'ha scritto pensava alla stesura di domande da fotocopiare su un foglio da consegnare ai partecipanti, poi correggerli con un pennarello rosso e segnare con il blu la percentuale delle domande esatte.

Era troppo chiedere di pensare all'intelligenza artificiale considerato che già le moderne piattaforme informatiche hanno superato il concetto della carta stampata.

Con l'utilizzo dell'intelligenza artificiale le "30 domande" dovranno essere inserite e caricate su dispositivi smartphone con app dedicate con verifica percentuale immediata che assolve a due problematiche:

- a) adempimento normativo della verifica finale di apprendimento
- b) raccolta dei dati per la successiva verifica dell'efficacia.

Basandoci sui dati dei questionari (ed altri dati) iniziamo a costruire il profilo dell'utente che sarà fondamentale nella successiva verifica dell'efficacia.

4.2.3 Efficacia della formazione

Una, purtroppo stringata, paginetta su 138 dell'Accordo Stato Regioni indica le modalità con le quali verificare l'efficacia dell'attività formativa nei confronti dei lavoratori durante lo svolgimento della prestazione lavorativa³⁷.

Le modalità da utilizzare possono essere:

1. analisi infortunistica aziendale;
2. questionari da somministrare al personale;
3. *check list* di valutazione.

Anche in questo caso l'intelligenza artificiale ci consente di andare oltre alla lettura semplicistica delle modalità previste che, assieme, possono concorrere alla verifica dell'efficacia senza porsi il falso problema di quale metodo scegliere tra quelli indicati.

La raccolta dei dati sugli infortuni aziendali è importante unitamente ai *near miss* e l'applicazione della A.I. consente una analisi non solo aziendale ma di reparto, di ambienti di lavoro, di mansioni, di età, e via dicendo.

I questionari da somministrare al personale devono tener conto della formazione svolta, delle analisi dei test di apprendimento e degli eventuali corsi di aggiornamento.

Queste metodologie consentono di elaborare una scheda per ogni singola persona che costituisce la base della successiva valutazione dell'efficacia, effettuata dopo 6 mesi/un anno, ad esempio dal preposto, sulla base di una attenta osservazione dei comportamenti messi in atto a seguito della formazione svolta.

Anche in questo caso i dati dovranno essere raccolti e costituiranno, con l'intelligenza artificiale, una base di analisi dei fabbisogni derivati che rappresentano una solida base delle conoscenze acquisite per progettare un successivo corso di formazione o di aggiornamento.

³⁷ Parte IV, punto 7 ASR, G.U. Serie Generale n° 19 del 24.05.2025

Nello specifico nelle differenti modalità:

a) Analisi infortunistica aziendale

Raccolta dati ed informazioni:

- verbali di infortuni, near miss, formazione, addestramento, verbali ispezioni, sorveglianza sanitaria, gestione qualità conformità/non conformità.

b) Questionari da somministrare al personale

Raccolta dati per la redazione del questionario:

- risultati test pregressi, programma dei corsi svolti, aggiornamento DVR e riunioni periodiche;
- una apposita sessione del questionario dovrà essere dedicata alle proposte e suggerimenti per migliorare il benessere organizzativo aziendale.

c) Check list di valutazione

Redazione di singole schede individuali, per reparto, per mansioni:

- l'osservazione, da effettuarsi durante l'attività lavorativa deve essere focalizzata sugli aspetti tecnici, procedurali ed organizzativi.

Per far sì che l'esito scaturito dall'analisi delle modalità proposte risulti significativo e riferito allo specifico contesto organizzativo è necessario avere a disposizione una notevole mole di dati e di informazioni che possono essere ricavati attraverso la predisposizione di appositi e appropriati questionari e *check list* capaci tutti di aiutare il *management* aziendale a verificare, in modo oggettivo, se a distanza di un tempo breve, medio – lungo dalla fine dell'evento formativo in seno all'organizzazione sono stati raggiunti gli obiettivi prefissati.

Come detto, i sistemi dotati di intelligenza artificiale utilizzano algoritmi e modelli matematici per analizzare i dati e supportare il *management* aziendale nel processo di revisione al fine di adottare le appropriate misure correttive.

Questi dati e questi algoritmi non sono frutto di macchinazioni esterne ma, piuttosto l'analisi dei dati che abbiamo inserito nel sistema che vogliamo utilizzare.

4.2.4 Lo studio delle ricadute formative con l'intelligenza artificiale

La significativa quantità di dati e informazioni raccolte attraverso le modalità sopra descritte può essere elaborata e analizzata utilizzando sistemi equipaggiati con intelligenza artificiale (AI).

Dall'analisi dei dati inseriti, corrispondenti a specifiche azioni, in tempo reale, si possono ricavare utili informazioni, ad esempio, per:

- programmare e riorganizzare mansioni, compiti o turni lavorativi, tenendo conto delle caratteristiche del lavoratore;
- correggere eventuali deviazioni confrontando i dati acquisiti con gli indicatori stabiliti durante la fase di progettazione.
- Analizzando e confrontando i dati delle verifiche di apprendimento finali con quelli dell'efficacia al fine di proporre ipotesi per i corsi di aggiornamento.
- Confrontare le performance dei corsi svolti in aula con la formazione in modalità e Learning ai fini della misurazione della loro efficacia.

Tutto ciò consente di:

1. misurare il cambiamento nei comportamenti dei partecipanti nell'uso di conoscenze, abilità e competenze e di valutare a distanza di tempo il permanere delle stesse;
2. misurare in termini oggettivi l'impatto che ha avuto l'attività formativa sul lavoro ordinario;
3. identificare eventuali carenze o necessità di miglioramento/aggiornamento delle attività formative.

La formazione, comprensiva degli aggiornamenti, incontri, partecipazione a convegni e seminari, sta alla base di un sistema che considera la valutazione come un processo continuo anziché come una semplice comparazione tra uno stato attuale e uno precedente. Inoltre, integra la valutazione nella pratica quotidiana, promuovendone una cultura che mira a migliorare il senso di appartenenza e ad aumentare la proattività dei lavoratori, i quali passano da essere spettatori a diventare parte attiva del processo.

4.2.5 Conclusioni

L'integrazione in azienda dei sistemi basati sull'utilizzo dell'intelligenza artificiale richiede un approccio che dia priorità al coinvolgimento dei lavoratori. A tal proposito, comunicazione e trasparenza sono i pilastri fondamentali per evitare possibili fraintendimenti che altrimenti potrebbero trovare resistenze sul piano organizzativo e ingenerare nei lavoratori una possibile mancanza di fiducia nei confronti del *management* aziendale.

Promuovere una cultura partecipativa in Azienda da una parte incrementa la soddisfazione e l'autonomia lavorativa, dall'altra mitiga i potenziali rischi associati all'aumento del carico di lavoro e al conseguente *stress*.

Fondamentale risulta, a tal proposito, la formazione dei lavoratori che va certamente indirizzata anche sugli scopi di utilizzo dell'AI, sottolineando altresì che questi strumenti supportano il lavoro umano senza sostituirlo. L'uso di questi sistemi deve essere chiaro e comprensibile fin dalla fase di rilevazione dei fabbisogni formativi, passando per la definizione degli obiettivi, dei criteri di valutazione sino al raggiungimento e alla condivisione degli indicatori.

“Il successo nella creazione dell'intelligenza artificiale potrebbe essere il più grande evento nella storia umana. Purtroppo, potrebbe anche essere l'ultimo, a meno che non impariamo a evitarne i rischi”³⁸.

Ricordiamo, però, che in Italia più del 95% delle imprese ha meno di 10 dipendenti ed al loro interno sarà difficile trovare i soggetti dotati delle necessarie competenze informatiche.

Bisogna evitare di ripetere gli errori (e gli inganni) fatti per la redazione del DVR laddove con pochi euro ed inserendo alcuni dati il computer stampava 100 o 200 pagine.

Si deve fare ricorso a consulenti e sindacalisti, RSPP e datori di lavoro, docenti e formatori che devono operare con una azione unitaria ed una visione etica dell'uso e dell'applicazione dell'intelligenza artificiale.

³⁸Stephen Hawking (1942-2018), matematico, fisico, astrofisico, cosmologo, divulgatore scientifico e accademico britannico: discorso tenuto nel corso del *Google Zeitgeist* (Londra, 12 Maggio 2015).

4.3 Costruzione di parametri di benchmark per la valutazione obiettiva dell'efficacia e dell'efficienza nella comunicazione del rischio in ambiente di lavoro

Santi Sparta

AIRP, Radiation and Robotic srl

Abstract

Nel panorama sempre più complesso della formazione alla sicurezza sul lavoro, cresce la consapevolezza che la semplice trasmissione delle informazioni non basta. Occorre verificare se i contenuti vengano compresi, assimilati e trasformati in comportamenti concreti. Ma come misurare davvero ciò che accade tra il momento in cui si parla di sicurezza e quello in cui la sicurezza si pratica?

Questo articolo propone un approccio innovativo basato sull'impiego dell'intelligenza artificiale per valutare l'efficacia e l'efficienza della formazione, attraverso indicatori oggettivi e report indipendenti. L'obiettivo non è quello di giudicare il formatore o il lavoratore, ma di fornire strumenti di miglioramento continuo, nel pieno rispetto della dignità e della riservatezza di tutti i soggetti coinvolti.

Proprio il rispetto dei principi etici e della privacy costituisce uno dei punti di forza del metodo proposto: trasparente, non invasivo, partecipativo. Un modello pensato non per sostituire l'uomo, ma per affiancarlo, rafforzando la cultura della sicurezza con la forza discreta dell'analisi intelligente.

4.3.1 Introduzione

La formazione alla sicurezza dei lavoratori rappresenta da sempre un pilastro imprescindibile della prevenzione, non solo perché consente di individuare e riconoscere condizioni di rischio spesso sottovalutate o ignorate, ma soprattutto perché costituisce un'occasione di crescita consapevole, sia individuale che collettiva. Soltanto attraverso la comprensione reale e profonda dei pericoli connessi alle attività lavorative è possibile costruire quella cultura della sicurezza che rappresenta il vero argine contro infortuni e comportamenti pericolosi.

Tuttavia, perché la formazione sia realmente efficace, è necessario che essa riesca a superare un ostacolo tutt'altro che secondario: quello della comunicazione improduttiva. In molte realtà, il linguaggio utilizzato dai docenti è troppo tecnico, astratto o poco aderente al vissuto quotidiano dei lavoratori. In altri casi, la modalità didattica si limita a una trasmissione unidirezionale, scarsamente interattiva, che non favorisce né la comprensione né la memorizzazione.

In parallelo, anche gli strumenti con cui si valuta l'esito della formazione risultano spesso inadeguati. Questionari standardizzati, test a risposta multipla e verifiche sommarie difficilmente permettono di misurare in modo attendibile la reale efficacia dell'apprendimento, ovvero la capacità dei lavoratori di assimilare, interiorizzare e mettere in pratica le conoscenze ricevute.

Valutare in modo rigoroso l'efficienza comunicativa del formatore e l'efficacia formativa sul piano cognitivo e operativo non è solo un dovere etico e normativo. È anche un'esigenza economica: ogni corso di formazione ha un costo per l'impresa, in termini di tempo, risorse umane e produttività sospesa. E il ritorno di questo investimento non può essere misurato soltanto in termini contabili: deve riflettersi concretamente in una maggiore sicurezza, una minore incidenza nel numero e nella gravità degli infortuni, e una consapevolezza diffusa tra i lavoratori che rimanga attiva nel tempo.

Alla luce di queste considerazioni, diventa urgente esplorare nuove metodologie di analisi e valutazione della formazione, capaci di andare oltre le apparenze. In questo ambito, l'Intelligenza Artificiale può offrire uno strumento nuovo: un osservatore imparziale e analitico, in grado di affiancare – non sostituire – il formatore e contribuire a innalzare il livello qualitativo del processo formativo.

4.3.2 Contesto e innovazione

4.3.2.1 Esperienze precedenti: valutazioni tradizionali e modelli di analisi

La valutazione dell'efficacia formativa non è un'esigenza nuova. Esistono da tempo modelli teorici e prassi consolidate che hanno cercato di affrontare questo tema in modo sistematico. Tra i più noti, il **modello di Kirkpatrick** rappresenta una pietra miliare: articolato in quattro livelli (reazione, apprendimento, comportamento e risultati), ha fornito per decenni una struttura di riferimento per molte organizzazioni. Un'evoluzione successiva è rappresentata dal **modello ROI di Phillips**, che aggiunge una dimensione economica alla valutazione, stimando il ritorno dell'investimento in formazione.

Anche in Italia si sono sperimentate pratiche osservazionali e qualitative, soprattutto in contesti aziendali strutturati, attraverso griglie di valutazione, focus group e interviste. Tuttavia, questi approcci, pur preziosi, richiedono tempi lunghi, risorse umane dedicate e possono risultare parziali o soggettivi.

Nel campo della **formazione medica e sanitaria**, si è sviluppata una particolare attenzione alla **validazione dei test di apprendimento**, con l'impiego di strumenti statistici e psicometrici per assicurare l'attendibilità, la coerenza interna e la capacità discriminativa dei quesiti. In molti corsi di aggiornamento (ECM), ad esempio, i test sono oggetto di analisi ex post per garantire che i risultati riflettano effettivamente la comprensione dei contenuti da parte dei discenti.

Queste esperienze, pur non basate su tecnologie di intelligenza artificiale, dimostrano la crescente consapevolezza del bisogno di strumenti di valutazione affidabili, adattivi e significativi. L'IA si propone oggi non come alternativa, ma come naturale prosecuzione di

questa traiettoria: un alleato capace di aumentare la precisione, ridurre i tempi di analisi e trasformare la formazione da evento episodico a processo continuo.



In diversi ambiti professionali, soprattutto nel settore medico-sanitario, sono già state sperimentate metodologie di valutazione dell'apprendimento fondate su criteri oggettivi. In particolare, l'analisi dei test somministrati ai discenti è spesso sottoposta a una valutazione statistica delle risposte, al fine di identificare eventuali criticità nei contenuti o nella didattica. Tuttavia, tali approcci – per quanto validi – si limitano per lo più a fornire una “fotografia” parziale e statica del processo formativo, focalizzandosi sulla correttezza delle risposte più che sulla profondità della comprensione o sulla capacità di applicazione.

Analogamente, anche nel campo della formazione aziendale o scolastica, sono stati introdotti strumenti di osservazione e monitoraggio, ma spesso con risultati frammentari e poco integrati con il contesto reale. Manca, in generale, una visione dinamica, adattiva e continua, capace di cogliere l'evoluzione dell'apprendimento nel tempo e di misurare l'impatto concreto sulla realtà operativa dei lavoratori.

4.3.2.2 Il cambio di passo: l'intelligenza artificiale come leva trasformativa

È in questo scenario che l'intelligenza artificiale segna un punto di svolta. A differenza degli strumenti tradizionali, essa consente **un'analisi integrata, tempestiva e contestuale** dei processi comunicativi e cognitivi, offrendo una mappa ad alta risoluzione dell'intero percorso formativo.

L'AI è in grado di individuare in tempo reale le criticità espositive del formatore, i momenti di calo dell'attenzione, la pertinenza degli esempi forniti e la reazione emotiva dei lavoratori ai contenuti proposti. Ma soprattutto, può **correlare l'efficienza della comunicazione con l'efficacia dell'apprendimento**, tracciando un profilo completo dell'esperienza formativa e suggerendo modifiche puntuali e personalizzate.

Si tratta dunque di un salto di qualità: non una semplice innovazione tecnologica, ma **una trasformazione epistemica**, che consente per la prima volta di coniugare valutazione e miglioramento continuo, su basi scientifiche, etiche e operative.

4.3.3 Due dimensioni da valutare: Efficienza ed Efficacia

Nell'ambito della formazione alla sicurezza sul lavoro, è fondamentale distinguere due concetti spesso confusi o sovrapposti: l'efficienza della comunicazione formativa e l'efficacia dell'apprendimento. Entrambe le dimensioni sono essenziali per comprendere se un intervento formativo ha realmente raggiunto i propri obiettivi, ma essi richiedono strumenti di analisi differenti.

4.3.3.1 L'efficienza comunicativa: superare le barriere

La prima dimensione riguarda la capacità del formatore di comunicare in modo chiaro, accessibile e pertinente. In molte realtà aziendali, soprattutto nei settori a maggiore complessità tecnica o nei contesti multiculturali, si riscontrano difficoltà dovute a barriere semantiche, linguistiche o culturali tra il docente e i lavoratori.

L'efficienza comunicativa si gioca su vari livelli:

- a) la chiarezza espositiva e la coerenza del discorso;
- b) l'uso di esempi pratici, analogie e riferimenti concreti;
- c) la capacità di adattare il registro linguistico all'uditorio;
- d) l'impiego di supporti visivi o multimediali capaci di rafforzare il messaggio.

Una formazione formalmente corretta ma incapace di “parlare” al lavoratore risulta sterile. Eppure, raramente la qualità comunicativa del docente viene monitorata con criteri oggettivi. In questo ambito l'intelligenza artificiale può essere di prezioso ausilio, perché è in grado di analizzare il contenuto e la forma della comunicazione, individuando criticità e suggerendo miglioramenti.

4.3.3.2 L'efficacia dell'apprendimento: comprendere e applicare

La seconda dimensione, altrettanto decisiva, è l'efficacia formativa, ovvero la misura in cui i lavoratori hanno realmente compreso, interiorizzato e sono in grado di applicare i contenuti ricevuti.

La difficoltà qui non sta solo nel "quanto" è stato appreso, ma nel "come" e nel "perché". L'efficacia non si esaurisce nella risposta corretta a un test, ma si riflette nella capacità:

- a) di riconoscere i rischi sul campo;
- b) di adottare comportamenti adeguati;
- c) di ricordare nel tempo le nozioni fondamentali;
- d) di collegare le informazioni teoriche a contesti operativi reali.

Spesso, queste valutazioni sono affidate a strumenti superficiali o non aggiornati, che offrono solo una fotografia parziale del processo. Una valutazione più articolata, continua e adattiva – in grado di intercettare segnali deboli e dinamiche evolutive – è necessaria per trasformare la formazione in un reale strumento di prevenzione.

Un esempio particolarmente significativo, emerso da esperienze recenti, è l'utilizzo dell'intelligenza artificiale generativa per creare immagini e filmati di eventi incidentali o situazioni di rischio ("near misses") altrimenti impossibili da documentare. La possibilità di visualizzare scenari realistici, anche se non realmente accaduti, consente ai lavoratori di confrontarsi in modo diretto ed emotivamente coinvolgente con le conseguenze potenziali di errori, disattenzioni o comportamenti non conformi.

Queste rappresentazioni, rese possibili da strumenti di generazione video e immagini basati su IA, hanno dimostrato una straordinaria efficacia sul piano formativo: rendono tangibile l'astratto, emotivamente viva l'informazione e quindi più facilmente memorizzabile e trasferibile nella pratica quotidiana. In questo senso, la tecnologia non è solo supporto didattico: è simulazione cognitiva, che prepara all'imprevisto senza attendere che si verifichi.

Le neuroscienze ci confermano che l'apprendimento è tanto più profondo quanto più è legato a esperienze emotivamente significative (Damasio, 1994). Anche nel contesto della formazione alla sicurezza, la narrazione visiva di un pericolo può incidere sulla memoria e sul comportamento più di molte lezioni teoriche, come evidenziato anche in recenti studi sull'efficacia delle simulazioni immersive in ambito HSE (Workplace Safety Training Effectiveness, OSHA Research Notes, 2021).

4.3.4 La proposta: un'intelligenza che osserva, analizza, migliora

Per colmare le lacune della valutazione tradizionale della formazione, viene qui proposta l'introduzione di un sistema basato su tecniche di Intelligenza Artificiale in grado di svolgere un duplice ruolo: da un lato, quello di analista della comunicazione formativa; dall'altro, quello di misuratore del risultato cognitivo e operativo del processo formativo.

4.3.4.1 Un'IA al servizio della trasparenza

Il sistema si configura come uno strumento indipendente, non intrusivo e rispettoso della privacy, ma in grado di raccogliere e interpretare dati significativi durante e dopo le sessioni formative. Le fonti possono includere:

- a) trascrizioni vocali e testuali delle lezioni,
- b) slide, immagini e video utilizzati,
- c) risposte fornite a test pre e post formazione,
- d) linguaggio usato dai lavoratori in attività simulate o nelle interazioni spontanee con chatbot formativi.

Attraverso modelli di analisi linguistica, semantica e cognitiva, l'IA elabora due report distinti ma complementari:

- i. un report sull'efficienza della comunicazione formativa, con analisi degli stili espositivi, della comprensibilità del linguaggio, della coerenza argomentativa, del bilanciamento tra teoria ed esempi concreti;
- ii. un report sull'efficacia dell'apprendimento, basato non solo sulla correttezza delle risposte, ma anche sulla profondità della comprensione, sulla capacità di applicazione e sull'evoluzione nel tempo del comportamento dei lavoratori.

4.3.4.2 Non un giudice, ma un supporto

Il sistema non è concepito come uno strumento punitivo, né nei confronti del docente né dei

lavoratori, ma come alleato del miglioramento continuo. I dati non sono utilizzati per attribuire colpe, ma per identificare aree critiche, valorizzare pratiche efficaci, suggerire percorsi di affinamento.

In questo modo, la formazione alla sicurezza può finalmente diventare un processo dinamico, misurabile, adattabile, che risponde ai cambiamenti dell'ambiente di lavoro, all'evoluzione dei rischi e ai bisogni reali delle persone coinvolte.

4.3.5 Indicatori di benchmarking: misurare per migliorare

Per rendere l'analisi dell'intelligenza artificiale concretamente utile, è necessario definire una serie di indicatori di benchmarking, cioè parametri misurabili che permettano di confrontare, valutare e migliorare nel tempo l'efficacia e l'efficienza della formazione.



La distinzione resta quella già esposta: da un lato gli indicatori di efficienza comunicativa, dall'altro quelli di efficacia dell'apprendimento.

Salvaguardia dei valori etici: garanzie per i lavoratori e i formatori

L'utilizzo dell'intelligenza artificiale nella valutazione della formazione alla sicurezza deve fondarsi su precisi criteri etici, che garantiscano trasparenza, rispetto e tutela della persona. Il sistema proposto si ispira a questi principi fondamentali:

Privacy e anonimato

Tutti i dati raccolti vengono trattati nel rispetto della normativa vigente (GDPR e normative nazionali), in forma anonima o pseudoanonimizzata. Nessuna informazione individuale viene usata per scopi estranei alla valutazione formativa.

Assenza di giudizio personale

L'IA non valuta le persone, ma analizza i processi. Il formatore non è soggetto a giudizi soggettivi o penalizzazioni, ma riceve indicazioni oggettive e costruttive per migliorare l'efficacia comunicativa.

Trasparenza degli strumenti

Gli algoritmi impiegati sono verificabili, tracciabili e, dove possibile, spiegabili. Gli indicatori utilizzati sono chiari, condivisi e consultabili da tutte le parti coinvolte.

Finalità esclusivamente formative

I report generati dall'IA non hanno valore disciplinare. Sono strumenti di supporto alla qualità formativa e alla sicurezza, e non possono essere utilizzati per attribuire colpe o responsabilità individuali.

Diritto all'opposizione

I lavoratori e i formatori coinvolti nel progetto hanno diritto a essere informati preventivamente e, se lo desiderano, a opporsi alla raccolta dei propri dati, secondo quanto previsto dalla normativa vigente.

Coinvolgimento partecipativo

Il progetto incoraggia il coinvolgimento di rappresentanze sindacali, RLS e figure di garanzia per assicurare che ogni fase sia condotta con trasparenza e condivisione.

Tutela dei dati sensibili

Ogni dato raccolto è trattato con misure di sicurezza adeguate. Non vengono raccolti dati biometrici, sanitari o sensibili, salvo esplicito consenso e finalità strettamente legate alla sicurezza collettiva.

Centralità dell'essere umano

L'intelligenza artificiale non sostituisce il giudizio umano. Ogni decisione operativa o formativa resta in capo alle figure professionali competenti, che possono integrare o rifiutare le indicazioni dell'algoritmo

4.3.5.1 Indicatori di efficienza comunicativa

Questi indicatori valutano la qualità della trasmissione delle informazioni da parte del docente, analizzando il linguaggio, la struttura del discorso e la capacità di coinvolgimento. Tra i più significativi:

- **Indice di chiarezza lessicale**

È la percentuale di termini tecnici o specialistici non spiegati, rapportata alla totalità del discorso.

Obiettivo: rendere il linguaggio comprensibile anche a chi non ha formazione tecnica.

- **Indice di complessità sintattica**

Misura la lunghezza e la struttura delle frasi utilizzate. Frasi troppo lunghe o articolate tendono a ridurre la comprensione.

Obiettivo: favorire un'esposizione lineare e accessibile.

- **Presenza di esempi concreti**

Frequenza di esempi, casi pratici o analogie per ogni concetto astratto introdotto.

Obiettivo: collegare teoria e pratica.

- **Bilanciamento tra contenuti e pause interattive**

Percentuale del tempo in cui il docente stimola domande, dialoga, o verifica la comprensione.

Obiettivo: trasformare la lezione in un'esperienza attiva.

- **Indice di equilibrio visivo (immagini/testo)**

Rapporto tra contenuti visuali (immagini, schemi, infografiche) e contenuti testuali nelle slide utilizzate durante la lezione. L'IA può rilevare automaticamente la densità di testo per slide, la presenza o assenza di elementi grafici significativi, e segnalare eccessi o carenze.

Obiettivo: promuovere una comunicazione visiva più incisiva e favorire l'attenzione. Una presentazione sovraccarica di testo può risultare opprimente, mentre un uso mirato di immagini facilita la memorizzazione e stimola l'elaborazione cognitiva.

4.3.5.2 Indicatori di efficacia formativa

Questi indicatori sono orientati a valutare quanto i lavoratori abbiano compreso, interiorizzato e siano in grado di applicare i contenuti della formazione. Alcuni esempi:

- **Differenziale pre/post test**

È lo scarto percentuale tra le risposte corrette prima e dopo il corso, ponderato per difficoltà.

Obiettivo: misurare l'apprendimento netto.

- **Indice di riformulazione semantica**

Capacità del lavoratore di spiegare concetti chiave con parole proprie in test aperti o interviste.

Obiettivo: valutare la comprensione profonda, non solo la memorizzazione.

- **Indice di retention a distanza**

Percentuale di concetti mantenuti a 30 o 60 giorni di distanza, valutata con brevi test ripetuti.

Obiettivo: misurare la stabilità dell'apprendimento nel tempo.

- **Comportamenti osservabili post-formazione**

Riduzione (o persistenza) di comportamenti a rischio rilevati tramite osservazione diretta, check-list, audit.

Obiettivo: valutare l’impatto sul comportamento reale.

Tutti questi indicatori non sono esaustivi, ma rappresentano una base strutturata su cui costruire un sistema di analisi adattabile alle diverse realtà aziendali e ai diversi ruoli lavorativi. La loro applicazione, supportata da strumenti di IA, permette non solo di fotografare lo stato della formazione, ma anche di misurare il miglioramento nel tempo, intervenendo con precisione là dove la formazione rischia di fallire.

Gli indicatori possono essere riassunti in due tabelle, e a ciascuno di essi è possibile attribuire un valore di ponderazione che tenga conto del differente contributo fornito al risultato complessivo.

I fattori di ponderazione sono **esemplificativi** e andrebbero tarati in base agli obiettivi del corso, al contesto aziendale e al pubblico.

Tabella 1 – Indicatori di Efficienza Comunicativa

Indicatore	Descrizione sintetica	Ponderazione (%)
Chiarezza del linguaggio	Assenza di tecnicismi non spiegati, lessico comprensibile	20
Coinvolgimento visivo	Uso di immagini/filmati evocativi e pertinenti	20
Equilibrio testo/immagine	Diapositive non sovraccariche, immagini non puramente decorative	15
Ritmo espositivo	Variazione della voce, pause, gestione del tempo	15
Interazione con il pubblico	Stimoli, domande, risposte	10
Accessibilità comunicativa	Attenzione a barriere linguistiche, culturali, cognitive	10
Uso di analogie o esempi	Collegamenti con esperienze reali del pubblico	10

Tabella 2 – Indicatori di Efficacia Formativa

Indicatore	Descrizione sintetica	Ponderazione (%)
Comprensione immediata	Misurata tramite test o domande in aula	25
Ritenzione nel tempo	Valutazione a distanza, memorizzazione concetti chiave	20

Indicatore	Descrizione sintetica	Ponderazione (%)
Applicabilità pratica	Capacità di applicare quanto appreso in contesti operativi reali	25
Riscontro nei comportamenti	Osservazione sul campo, near misses ridotti	15
Coerenza tra obiettivi e risultati	Allineamento tra programma e competenze effettivamente acquisite	15

4.3.6 Sperimentazione in una grande azienda: dal modello al campo

Per validare il modello proposto e verificarne la reale utilità, si propone l'avvio di una sperimentazione controllata in una grande azienda, scelta in modo da garantire:

- una significativa varietà di mansioni e profili professionali;
- una struttura formativa interna o comunque consolidata;
- la disponibilità a cooperare per il miglioramento continuo della formazione.

L'obiettivo non è quello di valutare la qualità di un singolo docente o corso, ma di testare l'efficacia del sistema di indicatori automatizzati e dei report generati da intelligenza artificiale, in confronto ai metodi tradizionali di valutazione.

4.3.6.1 Fasi operative del progetto pilota

a) Selezione del modulo formativo

Si individua un corso già previsto all'interno del piano di formazione annuale, possibilmente dedicato a un rischio specifico (es. movimentazione carichi, rischio elettrico, uso DPI, rischio radiazioni, ecc.).

b) Raccolta dei dati

Il sistema IA elabora:

- trascrizioni e metadati audio/video del docente;
- presentazioni utilizzate (formato slide, immagini);
- risultati dei test pre e post formazione;
- dati di interazione dei partecipanti (domande, commenti, pause riflessive);
- eventuali feedback spontanei.

c) Elaborazione dei report

Il sistema genera:

- un report sull'efficienza comunicativa, con indicatori aggregati e raccomandazioni;
- un report sull'efficacia dell'apprendimento, con valutazioni di comprensione, retention e coerenza tra contenuti e comportamenti.

d) Confronto con la valutazione tradizionale

I risultati vengono confrontati con le modalità di valutazione attualmente in uso (questionari, osservazioni del formatore, audit interni), per evidenziare divergenze, conferme o elementi di arricchimento.

e) Valutazione partecipata

Viene coinvolto un panel di soggetti interni (formatori, RSPP, rappresentanti dei lavoratori, direzione) per esaminare i risultati e riflettere sull'eventuale integrazione stabile del sistema nella pratica formativa aziendale.

4.3.6.2 Risultati attesi

Validazione degli indicatori: si potrà verificare quali parametri risultano più predittivi dell'apprendimento reale e quali meno significativi.

Rilevazione di criticità invisibili: l'IA potrebbe individuare elementi di debolezza comunicativa che sfuggono alla valutazione tradizionale.

Miglioramento continuo: il confronto tra i report generati e i comportamenti osservati nel tempo potrà costituire una base per affinare programmi, linguaggi e metodologie.

Costruzione di un modello replicabile: la sperimentazione potrà costituire il primo passo per un sistema modulare e scalabile, adattabile a settori diversi e contesti multipli.

4.3.7 . Conclusioni – Verso una formazione che lascia il segno

La formazione alla sicurezza non è un atto burocratico, ma un investimento culturale, operativo e umano. E come ogni investimento, merita strumenti adeguati per valutarne l'impatto. Limitarsi a raccogliere firme di presenza e risposte a test chiusi significa accontentarsi della forma, rinunciando a comprendere la sostanza.

Se la formazione alla sicurezza ha finora oscillato tra obbligo formale e tentativi empirici, oggi possiamo dotarla di strumenti oggettivi e trasparenti, capaci di misurarne il valore vero: la capacità di proteggere le persone.

L'introduzione dell'Intelligenza Artificiale come osservatore intelligente e indipendente non nasce dall'idea di sostituire il formatore, ma al contrario dalla volontà di affiancarlo con strumenti di analisi più raffinati, più imparziali, più capaci di leggere ciò che spesso sfugge.

Essa permette di misurare non solo ciò che è stato detto, ma anche come è stato detto e soprattutto quanto è stato compreso, ricordato, trasformato in comportamento.

A fronte dei costi inevitabili legati alla formazione, l'impiego di indicatori oggettivi può rendere il sistema più efficiente, più giusto e più trasparente.

Un docente attento potrà ricevere un feedback utile per migliorare il proprio stile comunicativo, mentre un lavoratore potrà essere messo nella condizione di apprendere davvero, non solo di "seguire un corso". Infine, un'azienda potrà finalmente sapere se la propria formazione produce risultati, o se è solo una voce di bilancio.

Ma, soprattutto, si potrà fare un passo avanti verso quella cultura della sicurezza che non si fonda sul timore della sanzione, ma sulla consapevolezza lucida del rischio e sul rispetto per il lavoro e per la vita.

La tecnologia, se ben orientata, può diventare alleata di questo processo. In tale contesto, essa non serve a spiare, ma a capire; non a giudicare e sostituire, ma a correggere e supportare. E in questo equilibrio sta forse la più autentica forma di prevenzione: quella che nasce non dall'obbligo, ma dalla comprensione.

Appendice. Un esempio di modulo di valutazione del docente.

Un importante contributo alla valutazione dell'efficacia della comunicazione può essere fornito dagli stessi fruitori della formazione, in quanto diretti interessati alla conoscenza del rischio ed alle tecniche di prevenzione e protezione da adottare per la salvaguardia della salute e della sicurezza.

Per tale motivo, un feedback qualitativo 'a caldo' da parte dei lavoratori sulla validità percepita della formazione appena ricevuta può risultare assai utile per lo stesso docente, che può utilizzare tali informazioni al fine di ottimizzare il percorso educativo e renderlo quanto più possibile mirato agli obiettivi di comunicazione prefissati.

A tale scopo, la stessa Intelligenza Artificiale è in grado di predisporre una tabella di valutazione, che può essere sottoposta 'a caldo' ai discenti, inserendo un QR CODE alla fine della presentazione, grazie al quale ciascuno può accedere ad un modulo da compilare in tempo reale con l'ausilio del proprio smartphone.

Un esempio di tale modello viene riportato in allegato.

I vantaggi di tale soluzione sono molteplici. In particolare:

- Il modello non è limitato ad un generico gradimento, ma chiede di approfondire alcuni aspetti di importanza cruciale per il miglioramento della comunicazione
- Il docente che riceve le informazioni può decidere o meno di condividerle con il datore di lavoro, discutendo con lo stesso sul raggiungimento degli obiettivi formativi stabiliti
- I dati vengono automaticamente accorpati in senso statistico, fornendo un quadro immediatamente comprensibile dei risultati
- La valutazione può essere resa anonima, escludendo i dati anagrafici del lavoratore

ALLEGATO. MODULO DI VALUTAZIONE DEL DOCENTE

Il modulo comprende due sezioni principali. La prima si riferisce all'**Efficienza comunicativa**, mentre la seconda riguarda l'**Efficacia formativa**, come riportato nei riquadri che seguono.

In entrambe le sezioni, le risposte possono essere fornite selezionando un valore compreso tra 1 (minimo) e 5 (massimo).

SEZIONE 1. EFFICIENZA COMUNICATIVA

Sezione 1,1 – Efficienza comunicativa : Chiarezza linguaggio *

	1	2	3	4	5
Il linguaggio era chiaro e comprensibile	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 1,2 – Efficienza comunicativa : Leggibilità testi *

	1	2	3	4	5
Il testo delle slide era leggibile e ben equilibrato	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 1,3 – Efficienza comunicativa : Pertinenza immagini *

	1	2	3	4	5
Le immagini erano pertinenti e d'aiuto alla comprensione	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 1,4 – Efficienza comunicativa : Successione logica *

	1	2	3	4	5
I concetti si sono susseguiti in modo logico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 1,5 – Efficienza comunicativa : Mantenimento interesse *

	1	2	3	4	5
Il corso ha mantenuto vivo il mio interesse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

SEZIONE 2. EFFICACIA FORMATIVA

Sezione 2,1 – Efficacia Formativa : Comprensione del rischio *

	1	2	3	4	5
Ho compreso i principali rischi legati alla mansione	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 2,2 – Efficacia Formativa : Comprensione metodi di protezione *

	1	2	3	4	5
So cosa fare per proteggermi correttamente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 2,3 – Efficacia Formativa : Comprensibilità concetti *

	1	2	3	4	5
Ricorderò con facilità almeno 3 concetti chiave	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 2,4 – Efficacia Formativa : Comprensione degli esempi *

	1	2	3	4	5
Le simulazioni o gli esempi mostrati mi hanno colpito	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sezione 2,5 – Efficacia Formativa : Aumento consapevolezza *

	1	2	3	4	5
Il corso ha aumentato la mia consapevolezza generale	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Una Sezione conclusiva è dedicata ad una valutazione globale e ad eventuali commenti da parte del lavoratore

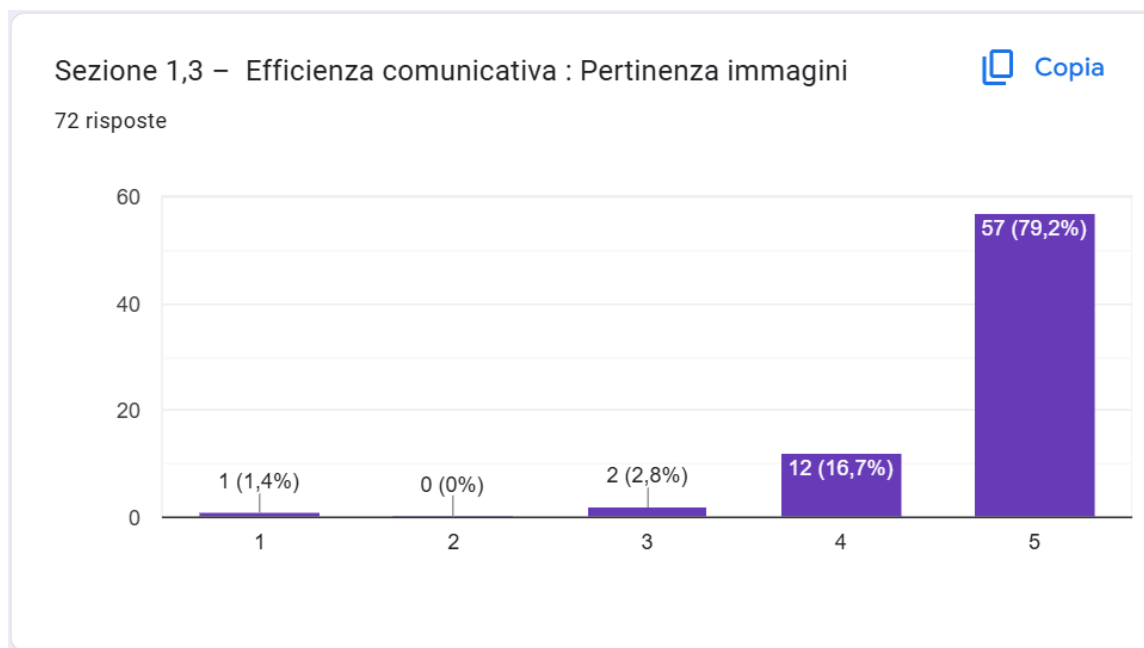
Sezione 3 – Valutazione globale *

	SI	IN PARTE	NO
Hai trovato utile questo ...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vorresti corsi simili in fu...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Commenti o suggerimenti (facoltativo):

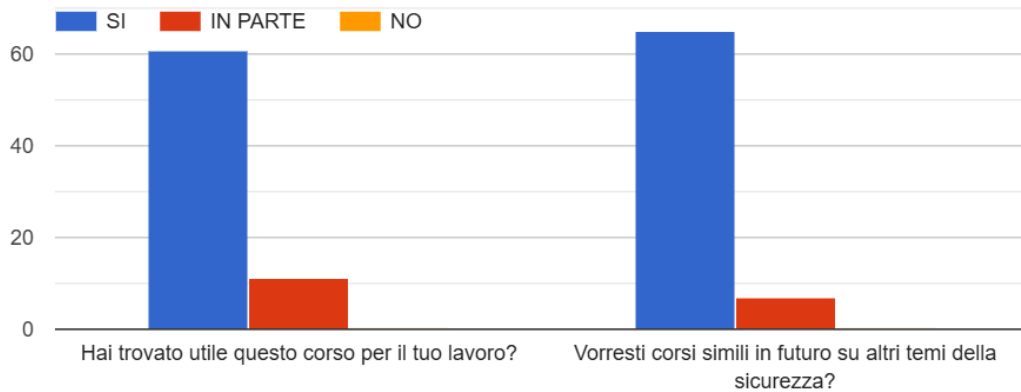
Testo risposta lunga

L'accorpamento statistico dei dati permette di avere una visione sinottica chiara del risultato ottenuto e di migliorare le parti della presentazione che abbiano ricevuto una valutazione modesta o insufficiente.



Sezione 3 – Valutazione globale

Copia



Bibliografia

- Damasio, A. R. (1994). *Descartes' Error: Emotion, Reason, and the Human Brain*. New York: G.P. Putnam's Sons.
- European Agency for Safety and Health at Work. *Artificial intelligence for worker management: an overview Report*. ISSN: 1831-9343
- Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating Training Programs: The Four Levels* (3rd ed.). Berrett-Koehler Publishers.
- Phillips, J. J. (1997). *Return on Investment in Training and Performance Improvement Programs*. Butterworth-Heinemann.
- Mayer, R. E. (2009). *Multimedia Learning* (2nd ed.). Cambridge University Press.
- Morin, E. (2001). *La testa ben fatta. Riforma dell'insegnamento e riforma del pensiero*. Raffaello Cortina.
- Norman, D. A. (2002). *The Design of Everyday Things*. Basic Books.

4.4 L'Accordo Stato Regioni e l'intelligenza artificiale

Rocco Vitale

Sociologo del lavoro, già docente universitario, fondatore e presidente onorario di Aifos.

L'obbligo di formazione per il datore di lavoro è stato definito dalla Legge 215/2021 che ha modificato l'art. 37 del D. Lgs. 81/2008 la cui entrata in vigore veniva demandata ad un successivo Accordo Stato Regioni, approvato il 17 aprile 2025.

Meno nota è la Legge 3 luglio 2023, n. 85 (conversione del D. L. 4/03/2023, n. 48 contenente *Misure urgenti per l'inclusione sociale e l'accesso al mondo del lavoro*) che all'art. 14 prevede una serie di modifiche al D. Lgs. 81/2008.

Nello specifico nella "Formazione dei lavoratori" all'articolo 37, comma 2, dopo la lettera b) è aggiunta la nuova lettera «*b-bis*) *il monitoraggio dell'applicazione degli accordi in materia di formazione, nonché il controllo sulle attività formative e sul rispetto della normativa di riferimento, sia da parte dei soggetti che erogano la formazione, sia da parte dei soggetti destinatari della stessa.*»

Il monitoraggio, dunque, completava le indicazioni della Legge 215/21 che ha affidato all'Accordo l'accorpamento della formazione, durata e contenuti minimi della formazione del datore di lavoro, le modalità dell'obbligo della verifica finale e, appunto, il monitoraggio.

Per questo monitoraggio la parte VI dell'Accordo prevede un "atto successivo". Nel frattempo, la Regione Lombardia, con atto della Giunta di approvazione dell'Accordo, prevede una legge regionale sui "soggetti formatori accreditati" che dovranno inserire dati e notizie sui propri corsi in un portale regionale. Ma siamo sicuri che questo sia il "monitoraggio ed il controllo sulle attività formative"? Ci può anche stare ma si tratta solo di adempimenti amministrativi e zero contenuti sulla formazione.

Forse sarà proprio l'assenza di indicazioni dettagliate sul monitoraggio della formazione svolta che ci potrà spronare a sperimentare modelli e progetti innovativi con l'uso dell'intelligenza artificiale.

I soggetti e le fonti

Dall'Accordo unico Stato Regioni si evidenziano, in modo particolare, tre tipologie di soggetti che sono (possono essere) coinvolti nell'uso dell'intelligenza artificiale ai fini degli adempimenti e delle disposizioni definite dall'Accordo stesso.

- Al primo posto troviamo i soggetti formatori (Organizzazione generale, 1.1, 1.2 e 1.3) che hanno il compito dell'organizzazione dei corsi
- La successiva categoria è rappresentata dai docenti/formatori
- Vi sono poi (anzi prima) i lavoratori coinvolti sia in quanto soggetti cui la formazione viene somministrata sia per un monitoraggio individuale della rispettiva formazione svolta ed in scadenza.

Siamo quindi in presenza di specifiche categorie di soggetti che hanno come compito quello della formazione alla sicurezza sul lavoro.

I soggetti formatori dovranno applicare i sistemi di IA con molta precauzione ed attenzione.

La richiesta di specifici documenti, previsti dall'Accordo, induce alla semplificazione del processo tramite una semplice richiesta all'IA di produrre un determinato documento.

La risposta dell'IA a tale richiesta sarà sicuramente corretta a livello normativo in quanto si basa sulla "Parte IV dell'Accordo" che ne indica le metodologie che verranno pedissequamente descritte.

Attenzione, però, poiché queste metodologie, corrette ma generiche, non si riferiscono al progetto formativo ma alla formalità della norma.

Come superare questo passaggio formale per renderlo sostanziale è compito dei soggetti formatori tramite l'inserimento dei dati anagrafici nonché della macro e micro progettazione.

Se si inseriscono i dati corretti l'IA aiuta alla predisposizione dei documenti.

Uno degli aspetti qualificanti sull'applicazione della IA riguarda i docenti ed i formatori. Due sono le principali modalità di erogazione dei corsi: in presenza o in e-Learning.

Per i corsi in presenza l'IA è utile per produrre testi, sintesi ed immagini. In questo caso non "si appalta" il corso all'IA. Più di una prova pratica, in fase di studio, ha realizzato modelli incompleti, ripetitivi e, spesso, senza il filo logico del corso. E, soprattutto, senza dare alcun valore al ruolo del formatore fornendogli delle slide da leggere recitando a memoria un testo anonimo.

Deve essere il formatore a definire scaletta, argomenti, tempi e l'uso dell'IA non può sostituire il formatore ma lo affianca nella fase di studio, ricerca, analisi e realizzazione.

Certamente l'IA sarà uno strumento utile, ad esempio, per creare immagini e grafici ma, come sempre deve essere il docente che deve conoscere bene cosa chiedere e, non solo, formulare la domanda ma una volta acquisita (es.) una immagine continuare a dialogare per renderla sempre più attinente alla lezione da svolgere.

Pensare di saltare le fasi iniziali e chiedere alla IA di passare alla realizzazione di un prodotto (slide) si avrà un risultato pessimo in termini di formazione.

Più complessa è la formazione in modalità e-Learning laddove l'IA può contribuire alla realizzazione dello strumento formativo.

Scrivere un buon testo e poi affidarlo alla IA chiedendo di leggerlo, fare delle dispersive con testi ed immagini per essere fruito dall'utente non è e-learning ma, tutt'al più sempre che funzioni, un sistema moderno di videocorso (che non è formazione).

I medesimi strumenti quali questionari standardizzati, a risposta multipla, non consentono una reale valutazione dell'efficacia formativa.

Trasformare l'esercitazione passiva in uno strumento attivo vuol dire progettare, nello sviluppo del corso, diversi momenti di esercitazioni e verifiche in itinere che l'IA organizza e valuta per ciascun utente, dando così alla verifica finale momenti di feed-back complessivi e comparativi.

Il Fascicolo del corso

L'intelligenza artificiale sarà sicuramente utile ai fini della realizzazione e conservazione del Fascicolo del Corso. Si tratta di andare oltre le attuali piattaforme di raccolta dei dati e dei fogli di Excel.

Il Fascicolo raccoglie tutta la documentazione relativa ad uno specifico corso e l'Intelligenza Artificiale consentirà alla documentazione amministrativa di trasformarla in documentazione dinamica al fine di consentire le seguenti azioni:

- a) Essere di riferimento per corsi successivi.
- b) Analisi documentale del corso con la verifica di efficacia e, sulla base delle risultanze, individuare soluzioni e modificazioni dei diversi documenti.
- c) Costituire per i singoli partecipanti il (ormai abbandonato) Libretto Formativo del Cittadino³⁹

³⁹ Previsto dall'art. 37, c. 14, D. Lgs. 81/2008 citato e mai attuato in tutti i precedenti Accordi Stato Regioni e, adesso, completamente ignorato.

d) Favorire l'aggiornamento del D.V.R. con l'integrazione del Fascicolo.

Analizziamo alcuni obblighi previsti dal nuovo Accordo Stato Regioni dove l'Intelligenza Artificiale svolgerà un ruolo importante.

L'organizzazione della formazione e l'analisi del fabbisogno

Il "Progetto formativo" meglio definito il "documento progettuale" rappresenta l'intero processo con tutti gli elementi che costituiscono l'azione formativa.

La qualità e l'efficacia della formazione in materia di salute e sicurezza sul lavoro non può prescindere dall'adozione di modelli organizzativi attraverso l'implementazione di un ciclo di garanzia della qualità e di miglioramento della stessa. L'approccio più idoneo, a garantire ciò, è quello basato sulla gestione di qualità dei processi di produzione della formazione, in termini di presidio e governo degli stessi. Il riferimento metodologico e concettuale per la gestione di tali processi, più comunemente e largamente diffuso, è quello basato sul ciclo PDCA di Deming⁴⁰.

La pianificazione è costituita dall'analisi del fabbisogno formativo quale fase iniziale dell'elaborazione di tutto il processo formativo. Una analisi indispensabile per conoscere i dati e le informazioni necessarie alla progettazione formativa.

Domanda semplice e risposta difficile e complessa. Le aziende e le organizzazioni utilizzano spesso più piattaforme differenti tra loro, che non sempre si interfacciano, con duplicazione e differenti sistemi di raccolta dati.

Una seria analisi del fabbisogno formativo comincia con una attenta analisi del Documento della Valutazione dei Rischi. Un DVR completo con i rischi associati alle mansioni ed ai lavoratori. Dati necessari da analizzare nel contesto della sorveglianza sanitaria (ma quando questa è affidata ad una agenzia esterna dove sono i dati correlati con il DVR?).

L'intelligenza Artificiale ci sarà di aiuto, e molto di più, se metteremo a disposizione tutte le fonti e non solamente la normativa di riferimento. Dati, numeri, analisi, processi e valutazioni associati ai nominativi dei lavoratori saranno gli elementi che ci aiutano nell'analisi partendo da quello che è stato fatto, dai risultati raggiunti per un miglioramento continuo.

Il progetto formativo

L'intelligenza artificiale utilizzata nelle analisi del fabbisogno renderà il **progetto formativo** coerente e dettagliato in tutte le azioni che caratterizzano l'azione formativa se verranno considerati gli elementi aziendali essenziali quali la valutazione dei rischi, l'aggiornamento annuale del Documento della Valutazione dei Rischi dopo la riunione periodica, la formazione svolta, l'andamento degli infortuni e della sorveglianza sanitaria.

Tutto ciò (oltre a concorrere all'analisi del fabbisogno) rappresenta una variabile mutevole, in continuo aggiornamento, derivata dalle modificazioni, di qualsiasi genere, del lavoro nel tempo e nello spazio.

Non sarà (o non dovrebbe essere l'intelligenza artificiale) a scrivere semplicemente un progetto formativo che si basa su dati generici, ma – con riferimento alle fonti – verranno poste all'analisi una

⁴⁰ Ciclo PDCA: Plan, Do, Check, Act. Metodo di gestione interattivo con un sistema ciclico, di 4 fasi, fino a raggiungere il miglioramento continuo elaborando un sistema e non i singoli pezzi. Studiato dall'americano W. Edwards Deming trovò la sua più efficace applicazione in Giappone, negli anni '50, dove contribuì notevolmente al miglioramento dei metodi produttivi delle aziende giapponesi rendendole famose per prodotti innovativi e di alta qualità, contribuendo anche al sorgere della sua potenza economica.

serie di domande che per continue e successive fasi di ricerca approderanno alla redazione del progetto riferito al complesso dei lavoratori dell'azienda o a gruppi omogenei.

Questi dati devono essere messi in relazione a specifici requisiti di:

conformità alle norme ed alle leggi

- a) coerenza metodologica
- b) pertinenza per dare risposta alla finalità formativa
- c) efficacia in quanto il progetto deve realizzarsi con i risultati attesi

Certamente le fonti normative saranno indispensabili ma altrettanto lo saranno le indicazioni operative differenti corso per corso derivanti dall'analisi del fabbisogno.

Il progetto formativo costituisce la base per l'analisi e la proposizione del "programma del corso". Gli enti formatori presentano (o dovrebbero presentare) ai datori di lavoro il programma del corso aziendale derivante dalle analisi del fabbisogno ed il relativo progetto formativo.

Sono questi gli elementi che costituiscono il programma del corso destinato ai lavoratori.

Il programma del corso

Se con gli strumenti semplici dell'Intelligenza Artificiale (ChatGPT o Copilot) si chiede di scrivere il programma del corso di formazione generale dei lavoratori avrete in pochi secondi la descrizione della pagina 13 dell'Accordo Stato Regioni del 17 aprile 2025.

La risposta dell'Intelligenza Artificiale è la seguente:

i corsi di formazione di 4 ore per lavoratori coprono argomenti fondamentali come:

- *Normativa sulla sicurezza sul lavoro*
- *Rischi generali e specifici legati all'attività lavorativa*
- *Misure di prevenzione e protezione*
- *Uso corretto dei dispositivi di protezione individuale*
- *Comportamenti sicuri sul luogo di lavoro*

Se, però, viene fatto il passo successivo per chiedere il programma del corso di formazione specifica dei lavoratori, nel rischio medio, la risposta dell'IA è questa:

Ciao! Al momento, non ho accesso a dettagli specifici sul programma del corso di formazione specifica per lavoratori a rischio medio dell'accordo del 17 aprile 2025. Tuttavia, in genere, questi corsi includono moduli su normativa di sicurezza, gestione dei rischi, uso corretto dei dispositivi di protezione individuale, e procedure di emergenza. Ti consiglio di consultare direttamente le fonti ufficiali o il soggetto organizzatore per ottenere il programma dettagliato e aggiornato.

Come mai, nel secondo caso, non ho neppure un elenco degli argomenti da trattare nel corso? Per il semplice motivo che nell'Accordo non sono definite le materie del corso e quindi l'IA non le legge.

In altri casi le materie sono definite e l'IA riporta il testo dell'Accordo.

Ma questo non è il programma del corso! Si tratta di una indicazione sui contenuti minimi.

Si ritorna, allora, all'analisi del fabbisogno che parte dalla valutazione dei rischi.

Però l'intelligenza artificiale non si limita alla produzione di testi ma, ad esempio, la *LinkedIn Learning*

propone contenuti formativi personalizzati ⁴¹ che si basano sui profili degli utenti analizzando le competenze esistenti ed i miglioramenti da acquisire

Vi è una piattaforma *Coursera for Business* per creare percorsi di apprendimento personalizzati che utilizza algoritmi adattati automaticamente in base alle performance dei partecipanti messi in relazione agli obiettivi aziendali. Non ho trovato, però, in questa piattaforma nessun algoritmo che avesse come obiettivo, da parte dell'azienda, della salute e sicurezza ma solo la crescita del business. Questa impostazione, legittima ma commercialistica, ci porta a considerare quanto sia sottovalutata o assente la problematica dei costi e dei mancati investimenti in sicurezza il cui peso economico incide più sui costi sociali che su quelli aziendali.

La formazione senza contenuti

Quando l'analisi è imprecisa o superficiale anche le risposte saranno di difficile applicazione.

La formazione rientra tra le forme più disarticolate dell'analisi e, spesso, i programmi dei corsi ricopiano i testi dell'Accordo e, soprattutto, non presentano i contenuti ma solo titoli.

Non è sufficiente indicare nel programma del corso una lezione per "la movimentazione dei carichi" se non sappiamo se i lavoratori, discenti, operano nelle costruzioni, nella logistica, nell'agricoltura o in una biblioteca. Certo gli aspetti generali sono comuni ma la specificità fa la differenza nell'apprendimento per il cambiamento.

In questo contesto si inserisce il rapporto tra la formazione e l'intelligenza artificiale per realizzare compiti, procedure e contenuti, come il "Fascicolo del corso", scrive il prof. Mazzoleni ⁴² che se lo strumento è utile viene utilizzato ed indirizzato in modo adeguato.

Non sarà, però, solamente l'Intelligenza artificiale il soggetto che viene chiamato "strumento" a compiere le azioni ma, piuttosto dovrà essere al nostro servizio attuando una collaborazione virtuosa tra le due intelligenze: quella umana e quella artificiale, ovvero come dice il prof. Mazzoleni "attraverso lo scambio continuo tra l'umano ed il tecnologico".

Certamente l'uso degli strumenti messi a disposizione dall'intelligenza artificiale ci deve orientare al dialogo ed al confronto e non alla semplicistica ricerca di una soluzione. Il problema cruciale, sostiene il prof. Harari⁴³, è quello di fare in modo che gli umani riescano a fare meglio degli algoritmi.

Nel nostro caso dobbiamo considerare il "Fascicolo del corso" come uno strumento di lavoro per la formazione continua (non tenere in archivio 10 anni in omaggio al formalismo normativo) quale base di partenza per l'aggiornamento ed altre azioni di salute e sicurezza per il monitoraggio della formazione.

⁴¹ Orazio Stangherlin, esperto digital transformation dell'apprendimento, in Direzione del Personale, rivista dell'AIDP, dicembre 2024.

⁴² Mario Mazzoleni, è stato professore associato di Economia Aziendale dell'Università degli studi di Brescia Dal 1992 al 2004 è stato direttore del Master of Business administration della SDA Bocconi. Nel 2018 ha fondato e diretto la Scuola di Management e Alta formazione dell'università degli studi di Brescia.

⁴³ Yuval Noah Harari, Homo Deus, Giunti editore Bompiani, Firenze 2017.

5 Intelligenza artificiale e benessere psicofisico dei lavoratori

5.1 IA e benessere psico fisico dei lavoratori: fattori di rischio, possibili conseguenze e misure di prevenzione

Barbara Gattoni, Sergio Sangiorgi

SIPLO - Società Italiana di Psicologia del Lavoro e delle Organizzazioni

Intelligenza artificiale e benessere psico fisico dei lavoratori ⁴⁴

La rivoluzione digitale sarà in grado di modificare significativamente la natura del lavoro apportando cambiamenti nelle organizzazioni e nelle condizioni occupazionali individuali e collettive, con un impatto sulla salute e sicurezza, sui rischi psicosociali e sulla salute mentale dei lavoratori ad oggi solo parzialmente prevedibile.

I cambiamenti da prendere in considerazione possono essere ricondotti a tre aree, e riguardano: l'automazione e l'uso di sistemi di monitoraggio intelligenti per la pianificazione e il controllo delle

attività; la digitalizzazione dei processi lavorativi (incluse forme di lavoro ibrido); l'utilizzo di piattaforme come ambiente unico di lavoro.

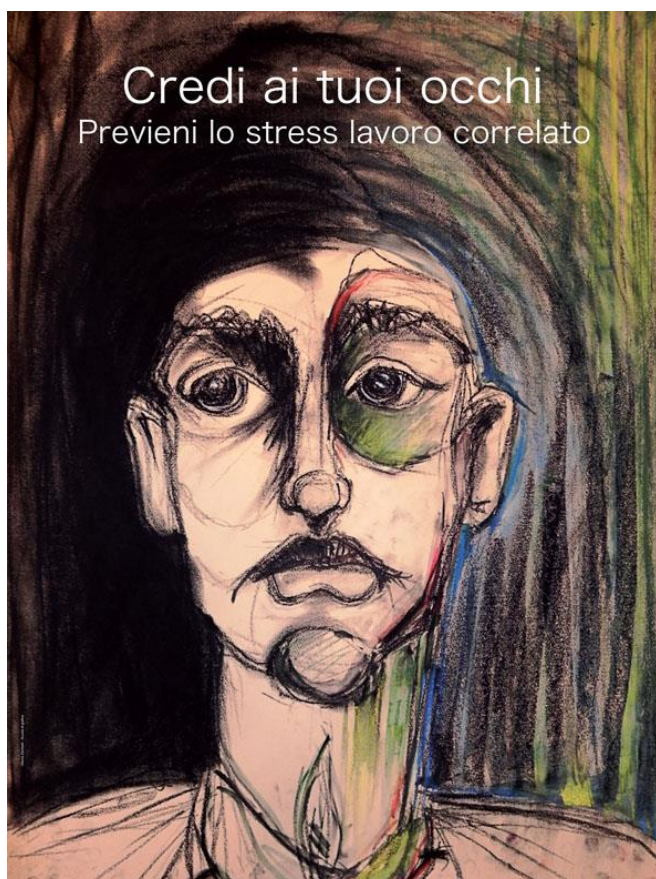
Se non adeguatamente progettati e monitorati, i processi citati saranno in grado di causare nel breve futuro degli effetti indesiderati su benessere organizzativo e individuale.

Sebbene l'automazione e l'introduzione di sistemi di monitoraggio intelligenti favoriscano miglioramenti ergonomici ed una riduzione dello sforzo fisico, possono comportare di fatto la riduzione dell'autonomia dei lavoratori, la dequalificazione, l'intensificazione del lavoro e un conseguente aumento dello stress.

La digitalizzazione dei processi lavorativi può anch'essa portare a miglioramenti delle condizioni di lavoro, ad una migliore comunicazione e interazione sociale ma, se mal gestita, può invece favorire una maggiore intensità del lavoro, difficoltà di conciliazione tra lavoro e vita privata quando i lavoratori vengono privati del diritto di disconnessione, contribuendo così all'aumento di stress e ansia.

I lavoratori che operano unicamente su

piattaforma di monitoraggio digitale, per ora una quota limitata della popolazione, sono esposti ai rischi connessi alla "condizione di isolamento" sia dal punto di vista fisico che relazionale ed all'insorgenza di disturbi del sonno, stress, depressione, burnout. Questi problemi sono



ACCADEMIA DI BELLE ARTI
DI BRESCIA
santaGiulia



AIFOS
Associazione Italiana Formatori
Operatori della Formazione Continua

⁴⁴ <https://osha.europa.eu/it/themes/digitalisation-work>

ulteriormente aggravati dal fatto che la maggior parte della comunicazione tra piattaforma e lavoratori è automatizzata.

È stato pubblicato ad inizio 2025 l'allegato alle linee guida della Commissione Europea sulle pratiche vietate nell'impiego di forme d'intelligenza artificiale (IA), ai sensi del Regolamento (UE) 2024/1689, noto come AI Act.

Alcuni elementi delle linee guida sulle pratiche vietate sembrano particolarmente rilevanti per la prevenzione:

1. DIVIETO DI PRATICHE MANIPOLATIVE DELL'IA.

Sono vietati i sistemi di IA che impiegano tecniche subliminali, ingannevoli o manipolative che compromettano significativamente la capacità decisionale degli individui. Questo divieto può influire direttamente sulle tecnologie HR utilizzate per il reclutamento, la valutazione delle performance e il monitoraggio dei dipendenti.

2. RESTRIZIONI SUL RICONOSCIMENTO DELLE EMOZIONI NEI LUOGHI DI LAVORO.

L'uso di sistemi di IA per il riconoscimento delle emozioni nei luoghi di lavoro è generalmente vietato, salvo eccezioni per motivi medici o di sicurezza. Le restrizioni rappresentano una sfida per la crescente diffusione del cosiddetto *affective computing* in contesti organizzativi e richiede una rivalutazione delle tecnologie utilizzate per monitorare le emozioni e il benessere dei dipendenti.

3. LIMITAZIONI SULL'USO DEI DATI BIOMETRICI.

L'AI Act vieta i sistemi di IA che categorizzano le persone in base a dati biometrici sensibili (es. razza, credenze politiche, orientamento sessuale) per scopi non legittimi. Questo rafforza la necessità di rigorosi standard etici e di protezione dei dati nelle pratiche organizzative.

4. REQUISITI DI CONFORMITÀ ALLA NORMATIVA.

Organizzazioni devono rispettare rigidi protocolli di conformità, inclusa la conduzione di valutazioni d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio. Questo richiede una collaborazione interdisciplinare tra esperti per garantire che l'adozione dell'IA sia conforme agli standard normativi.

5.1.1 Fattori di rischio psicosociale

Un cambiamento profondo come quello derivante dall'introduzione della Intelligenza Artificiale nei processi organizzativi impone una attenzione costante verso gli aspetti di progettazione, organizzazione e gestione del lavoro in fase di costruzione, di cambiamento e di monitoraggio prendendo in considerazione la pianificazione e la successiva messa in atto di misure di prevenzione degli effetti possibili sui singoli e sui gruppi di lavoratori.

I principali effetti della mancata prevenzione dei rischi psicosociali nell'introduzione di sistemi di AI sono di seguito indicati:

1. SOVRACCARICO COGNITIVO DOVUTO ALLA COMPLESSITÀ DELLE TECNOLOGIE INTRODOTTE

L'inserimento della IA nei processi aziendali andrà a modificare vecchi approcci di lavoro consolidati: richiederà ai lavoratori di apprendere nuove modalità di lavoro, accedere a nuovi strumenti tecnologici causando potenzialmente stress, senso di inadeguatezza, sovraccarico cognitivo, soprattutto nei lavoratori "maturi" se tali tecnologie non saranno intuitive/o accompagnate da formazione specifica. Identificazione di nuove "diseguaglianze" legate a

età/cultura/formazione tecnica e legate alla comprensione della corretta interazione con la tecnologia IA, adattamento ai cambiamenti organizzativi, ecc.

2. PERDITA DI SENSO DI CONTROLLO / PERCEZIONE DI RIDOTTA AUTONOMIA NELLO SVOLGIMENTO DELLE PROPRIE MANSIONI

L'introduzione dell'IA quando coincide con una più elevata automatizzazione delle operazioni può causare nelle persone la percezione di perdita di controllo sul proprio operato (acutizzare gli stati di ansia, il senso di perdita di autonomia, senso di alienazione e demotivazione).

3. STRESS DA MONITORAGGIO COSTANTE/PERCEZIONE DI SFIDUCIA

La tecnologia IA può essere utilizzata per il controllo/monitoraggio delle prestazioni (o per es. dell'utilizzo corretto dei DPI) ed essere percepita dai lavoratori come costante sorveglianza da parte dell'organizzazione generando ansia, un senso di mancanza di fiducia da parte dell'organizzazione sull'operato del personale (e del lavoratore nei confronti dell'organizzazione), diminuzione della motivazione.

4. AMBIGUITÀ SUL RUOLO DELL'IA / INCERTEZZA NELLA DEFINIZIONE DELLE RESPONSABILITÀ DEL LAVORATORE SUL SUO OPERATO

I cambiamenti organizzativi / cambiamenti del contenuto del lavoro legati all'introduzione dell'IA possono generare ambiguità sui compiti e sulle responsabilità, lasciando i lavoratori incerti sul loro ruolo questo può avere delle ripercussioni sui livelli di stress e ansia, percezione di insicurezza lavorativa.

5. PRESSIONE NEI TEMPI DI LAVORO/ OBIETTIVI DETTATI DALL'IA

L'introduzione delle IA allo scopo di aumentare la produttività e l'efficienza dei processi di lavoro possono generare pressioni elevate ai lavoratori in essi coinvolti a causa dei tempi di lavoro e l'obbligo di raggiungimento di obiettivi "innaturali/irrealistici" imposti dalla nuova tecnologia mettendo i lavoratori in uno stato di costante tensione. Questo può causare infortuni sul lavoro e/o stress cronico e burnout.

6. TIMORE DI PERDERE IL LAVORO/DI ESSERE SOSTITUITI DALLA NUOVA TECNOLOGIA (IA)

L'introduzione di tecnologie IA avanzate può far insorgere nei lavoratori il timore di essere sostituiti, soprattutto nei settori in cui l'automazione dei processi di lavoro è elevata questo può causare ansia, riduzione dell'attenzione e quindi maggiore esposizione ai rischi di errore/infortunio, riduzione della motivazione. Insicurezza lavorativa e finanziaria.

7. PERDITA DI INTERAZIONE SOCIALE/ISOLAMENTO

L'introduzione della tecnologia IA (robot, processi automatizzati) può portare ad una riduzione dell'interazione umana in alcune fasi di lavorazione, portando ad un maggiore isolamento del lavoratore anche per la ridotta occasione di relazioni sociali; può portare ad una maggiore sensazione di mancanza di supporto da parte di colleghi e superiori/manager.

5.1.2 Prospettiva Europea

L'impatto psicologico dell'IA nel mondo del lavoro, come delineato nel regolamento "AI Act" dell'Unione Europea, comprende vari aspetti legati sia all'utilizzo dei sistemi di IA per compiti specifici che alle implicazioni più ampie sui lavoratori. Di seguito, i principali elementi rilevati:

1. MONITORAGGIO E VALUTAZIONE.

I sistemi di IA ad alto rischio sono utilizzati per monitorare e valutare i dipendenti, con l'intento di gestire compiti in base ai comportamenti e alle caratteristiche personali. Tali applicazioni possono indurre effetti negativi sui lavoratori a causa di una costante percezione di essere monitorati e valutati, il che può avere un impatto negativo sulla loro salute mentale.

2. DECISIONI AUTOMATIZZATE.

Questi sistemi vengono impiegati per prendere decisioni relative all'assunzione, promozione e cessazione del rapporto di lavoro. La percezione di un potenziale bias intrinseco nei modelli di IA, che potrebbe perpetuare discriminazioni storiche, contribuisce al timore di essere trattati in modo iniquo, specialmente per i gruppi più vulnerabili. Ciò può causare preoccupazioni psicologiche relative alla propria sicurezza lavorativa e alle opportunità di carriera.

3. DIRITTI E PRIVACY.

L'uso dell'IA per il monitoraggio può violare la privacy dei lavoratori e generare sensazioni di invadenza e mancanza di controllo sulle proprie informazioni personali. Questa situazione può portare a una riduzione della fiducia nei confronti del datore di lavoro e del sistema aziendale, con conseguente impatto negativo sul benessere psicologico.

4. VULNERABILITÀ E MANIPOLAZIONE.

I sistemi di IA possono sfruttare vulnerabilità specifiche legate all'età, alla condizione economica o a disabilità, mettendo a rischio lavoratori in posizioni di vulnerabilità. Ciò può condurre a stati di tensione e di insicurezza, poiché i lavoratori percepiscono che tali sistemi potrebbero essere utilizzati per scopi manipolativi che vanno contro i loro interessi e benessere.

5. DISCRIMINAZIONE.

L'IA, utilizzata in contesti di valutazione delle prestazioni, potrebbe favorire discriminazioni involontarie, soprattutto quando basata su dati storici che riflettono pregiudizi preesistenti. Questo può far sì che i lavoratori temano un trattamento discriminatorio, che influisce negativamente sul loro senso di equità e di appartenenza sul posto di lavoro.

6. ALFABETIZZAZIONE E FORMAZIONE.

È essenziale promuovere una maggiore alfabetizzazione in IA tra i lavoratori, fornendo loro le conoscenze necessarie per comprendere come le decisioni supportate da IA possano influenzarli. Ciò potrebbe migliorare la trasparenza e, di conseguenza, ridurre l'ansia e il senso di incertezza che l'introduzione dell'IA potrebbe causare.

5.1.3 Misure di prevenzione dei possibili effetti dei fattori di rischio sul lavoratore

La mancanza di una normativa specifica per l'utilizzo dell'IA in ambito lavorativo richiede una particolare attenzione per consentire la corretta applicazione di quanto contenuto nel D.lgs. 81/08 in merito agli obblighi del Datore di Lavoro nella tutela di salute (non solo fisica, ma anche mentale/psicologica) e sicurezza dei lavoratori.

Un supporto nell'individuazione (e successivamente nella gestione) dei potenziali fattori di rischio psicosociali si ricava anche dallo STANDARD ISO 45003:2021 che suggerisce di ricorrere a piani di formazione e sviluppo di competenze per i lavoratori, accompagnando così il cambiamento organizzativo e l'introduzione dei nuovi processi di lavoro o nuove tecnologie (anche IA).

Inoltre, lo stesso STANDARD mira a promuovere un coinvolgimento attivo dei lavoratori e dei loro rappresentanti nei cambiamenti organizzativi, e invita il management a comunicare in maniera chiara i ruoli e le responsabilità per ridurre il rischio di ambiguità.

Adottare buone prassi che possano contenere il senso di disorientamento delle persone e favorire la fiducia reciproca tra azienda e lavoratori, aiuta ad aumentare il livello di “sicurezza psicologica” percepita e il benessere individuale.

In conformità con quanto indicato dal DLgs 81/08 (e in linea con i principi dello STANDARD ISO 45003), il piano di prevenzione dei rischi connessi all’introduzione dell’AI, deve prevedere:

1. PARTECIPAZIONE/COINVOLGIMENTO DEI LAVORATORI, anche attraverso la consultazione dei propri rappresentanti per la sicurezza, in tutte le fasi di progettazione, introduzione e implementazione della tecnologia IA in azienda garantendo così un accompagnamento e introduzione graduale della tecnologia IA (*work design*).
2. FORMAZIONE/ADDESTRAMENTO ALL’USO DELLA SPECIFICA TECNOLOGIA IA rivolti ai lavoratori per aumentare la percezione di familiarità con la tecnologia IA introdotta, garantendo così anche la tutela dei lavoratori da qualsiasi forma di discriminazione dovuta a mancanza di conoscenze/competenze sull’uso delle nuove tecnologie IA.
3. COMUNICAZIONE TRASPARENTE E COMPLETA:
 - a) sui cambiamenti in atto, offrendo un supporto costante a tutti i lavoratori interessati ad esso;
 - b) sulla tipologia di dati raccolti e sul loro utilizzo, comunicando in maniera chiara e comprensibile come vengono utilizzati i dati raccolti.
4. IMPOSTAZIONE DI OBIETTIVI E TEMPI DI LAVORO REALISTICI, che tengano conto dei potenziali fattori di rischio psicosociali legati all’uso di tecnologia IA. Applicare l’IA in un contesto in cui il miglioramento delle prestazioni avvenga senza compromettere il benessere organizzativo/la salute mentale dei lavoratori.
5. PROCESSI CONSOLIDATI di gestione degli aspetti legati alla diversità nell’approcciarsi alle tecnologie IA (es. differenze di età, di cultura, di formazione tecnica, esperienza pregressa nell’uso della tecnologia IA in ambito lavorativo). Preservare momenti di socialità, canali di comunicazione, occasioni di incontro e confronto tra lavoratori anche negli ambienti fortemente automatizzati è vitale.

5.1.4 Benessere individuale e organizzativo nei processi di cambiamento

Il coinvolgimento dei lavoratori e dei loro rappresentanti nel processo decisionale relativo all’introduzione della intelligenza artificiale nei processi di lavoro può portare a una minore resistenza ai cambiamenti e ad un’integrazione più sicura ed efficace dei nuovi sistemi. Lo stress prodotto dalle modificazioni organizzative può essere legato sia al processo di cambiamento sia ai risultati raggiunti.

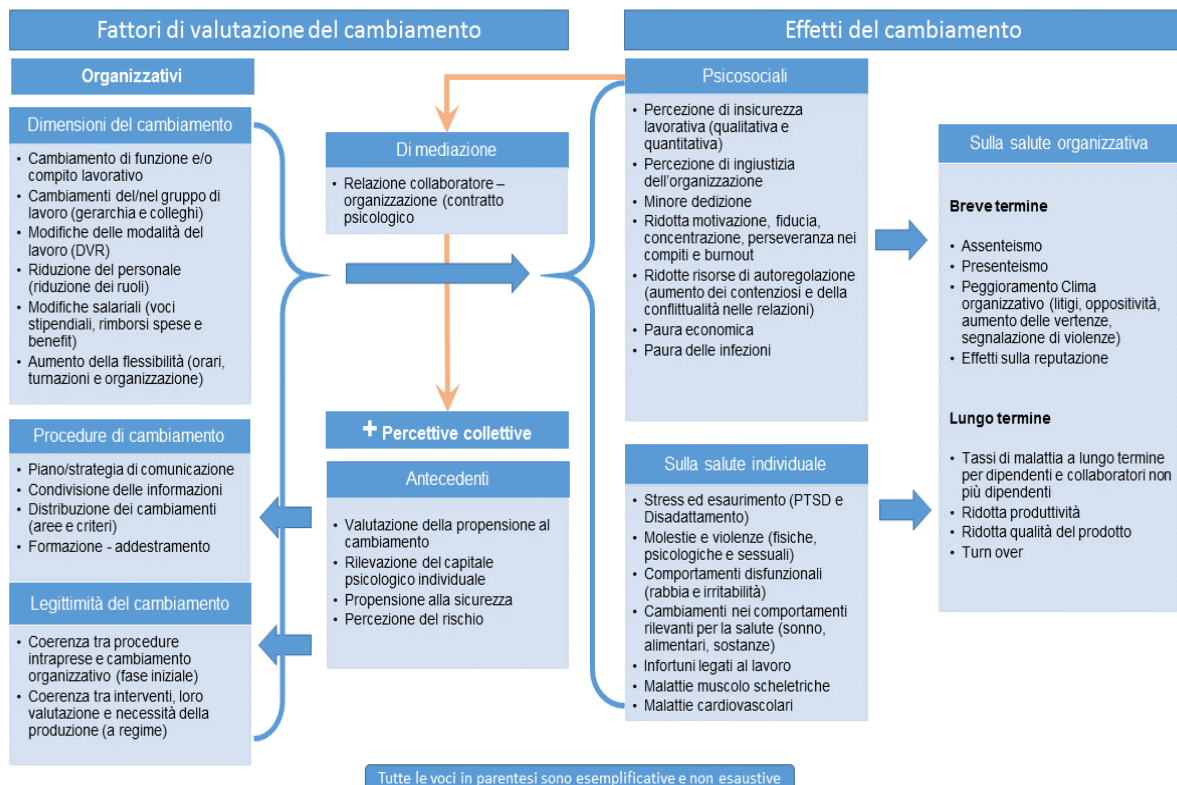
Mitigare le difficoltà nei processi di cambiamento e promuovere il benessere individuale e organizzativo è la sfida della tutela della salute negli ambienti di lavoro.

Il modello sul cambiamento pubblicato nel **rapporto HIREs** (2011), adattato da **SIPLO** nel 2021, è utile a guidare la lettura del processo in atto e prevenire gli effetti sulla salute organizzativa e individuale⁴⁵.

Nel processo di valutazione e sostegno al cambiamento, il modello può fornire un supporto:

⁴⁵ <https://www.siplo.it/wp-content/uploads/2021/12/Benessere-individuale-e-organizzativo-nei-processi-di-cambiamento-.pdf>

- in fase di avvio, perché indica le informazioni che è importante raccogliere per una gestione consapevole del percorso;
- in fase di sviluppo, in quanto suggerisce quali effetti monitorare nel tempo;
- al termine del processo, perché consente di sapere se le trasformazioni avvenute hanno avuto un impatto sulla salute delle persone e/o della organizzazione.



I fattori di valutazione del cambiamento guidano la direzione aziendale e le figure della prevenzione nella analisi delle tre aree da presidiare per promuovere una modifica profonda quale quella introdotta con la digitalizzazione.

- **Le Dimensioni del cambiamento:** descrivono le modifiche organizzative intervenute per introduzione di sistemi di automazione delle attività, digitalizzazione dei processi lavorativi (telelavoro e il lavoro ibrido) e/o utilizzo di piattaforme.
- **Le Procedure del cambiamento:** individuano i piani di comunicazione, informazione, formazione attivati ed i criteri adottati per l'individuazione del personale coinvolto nelle modifiche di compiti/modalità/sedi di lavoro.
- **La Legittimità del cambiamento:** propone una verifica di congruenza tra le Procedure del cambiamento e le Dimensioni del cambiamento attuato; questa analisi deve considerare la sostenibilità dello stesso con le necessità della produzione.

Se un'azienda tiene conto di queste tre aree si può supporre che stia guidando, in una prospettiva di adattamento consapevole, il proprio cambiamento con attenzione alla salute e sicurezza dei collaboratori. Potrà quindi verificare, attraverso il monitoraggio sugli effetti del cambiamento (salute organizzativa e salute individuale), l'andamento del processo di cambiamento.

Gli effetti del cambiamento sono indicatori che descrivono condizioni di mancato adattamento al processo di cambiamento organizzativo nel tempo e comprendono Salute Organizzativa, Effetti psicosociali e Salute individuale.

- **Gli indicatori della salute organizzativa** sono sensori che identificano i possibili effetti a breve e/o lungo termine del cambiamento introdotto e comprendono: diminuita capacità produttiva, aumento infortuni, aumento assenze per malattia, conflittualità, ridotta capacità di adattamento al cambiamento personale e professionale, richiesta di spostamento ad altra mansione/funzione, reclami da clienti o fornitori. Possono trovare riscontro nella lettura degli eventi sentinella propri della valutazione del rischio stress lavoro correlato e in rilevazioni del clima organizzativo, soddisfazione, motivazione tramite questionari e/o focus group.
- **Gli effetti psicosociali** sono indicatori collettivi di malessere, derivanti potenzialmente da carenze nelle funzioni di accompagnamento al cambiamento per possibile sottovalutazione di alcuni fattori organizzativi, o per esigenza di maggior attenzione a condizioni di esposizione al rischio reale o percepito. Si fa quindi riferimento alla valutazione di percezioni collettive tramite questionari, focus group o interviste semi-strutturate, relative a: l'insicurezza lavorativa in relazione al mantenimento del proprio posto di lavoro o allo status raggiunto in precedenza, il vissuto di ingiustizia organizzativa per scelte ritenute inique, la disaffezione al lavoro, la mancanza di fiducia verso la direzione, l'aumento della conflittualità, il timore per la propria salute e sicurezza. Le fonti informative possibili da integrare sono ad esempio: la valutazione della performance lavorativa del gruppo e del singolo; l'aumento dei contenziosi, della conflittualità e delle richieste di trasferimento.
- **Gli effetti sulla salute individuale** possono essere monitorati dal medico competente attraverso l'applicazione di alcuni strumenti di screening che consentono di intercettare sintomi compatibili con condizioni di stress, ansia, depressione, reattività a eventi traumatici per eventuale approfondimento della condizione individuale allo psicologo.⁴⁶

Alcuni strumenti, a titolo esemplificativo e non esaustivo, sono stati resi disponibili dall'Istituto Superiore di Sanità, Rapporto ISS COVID-19, n. 44/2020⁴⁷.

⁴⁶ https://www.ciip-consulta.it/images/eventlist/Eventi2024/240523-anma/3.6%20Ballottin%20A.%20%20DA_CARICO_MENTALE_A_RISCHI_PSICOSOCIALI.pdf

⁴⁷ https://www.iss.it/documents/20126/0/Rapporto+ISS+COVID-19+44_2020.pdf/f23b53b4-a706-eb54-201c-ea12d2d7ca19?t=1591970625833

GHQ 12. QUESTIONARIO SUL BENESSERE GENERALE Questionario auto-compilato composto da 12 domande che indaga il benessere generale e in particolare i sintomi depressivi ed ansiosi. Il cut-off è stato ridefinito al punteggio 14 (scala Likert).

Scala ZUNG. SCREENING DELLA SALUTE GENERALE (PSICOFISICO E SOCIALE) DELLA PERSONA. Questionario composto da 20 domande che consente di individuare lo stato di sofferenza psicologica e riconoscere la presenza di ansia (Dunstan & Scott et al., 2020).

PHQ 9. SCREENING SINTOMI DEPRESSIVI Questionario composto da 9 domande che guidano l'individuazione dei probabili casi di depressione attraverso il superamento di un punteggio pari o superiore a 10 costituisce la soglia ottimale per massimizzare sensibilità e specificità (Levis et al., 2019).

GAD 7. SCREENING DISTURBI D'ANSIA Questionario auto-compilato composto da 7 domande per la valutazione dell'ansia di stato che si accompagna ad un breve colloquio durante il quale viene indagato lo stato di salute generale (psicofisico e sociale) della persona.

IES-R. SCALA D'IMPATTO DELL'EVENTO. SCREENING PTSD questionario self-report di 22 item progettato per valutare il disagio soggettivo causato da eventi traumatici. È comunemente utilizzato per misurare la gravità dei sintomi correlati al disturbo da stress post-traumatico (PTSD).

5.1.5 Fattori psicologici connessi all'introduzione di forme di intelligenza artificiale nei contesti di lavoro

Spesso si accenna alla percezione dell'IA come minaccia, principalmente sotto forma di ansia da sostituzione lavorativa, di insicurezza derivante dal confronto con sistemi intelligenti e del senso di inadeguatezza rispetto alle nuove competenze digitali richieste, in particolare nei lavoratori senior. Questi elementi sono cruciali per comprendere e mitigare le barriere all'introduzione di nuove tecnologie. Le paure legate alla perdita di centralità e al giudizio automatizzato devono essere affrontate attraverso interventi preventivi mirati, volti a sostenere il benessere psicologico.

Nell'ambito delle attività del **Project Work promosso da SIPLO sull'impatto dell'Intelligenza Artificiale nel mondo del lavoro**⁴⁸, è stata avviata un'indagine esplorativa volta ad approfondire le percezioni, le preoccupazioni e le reazioni psicologiche dei lavoratori nei confronti dell'introduzione di sistemi intelligenti nei contesti organizzativi.

La ricerca ha coinvolto un campione di oltre 500 partecipanti attraverso l'utilizzo integrato di questionari strutturati e interviste qualitative. Tale approccio ha consentito di esplorare in modo articolato aspetti quali il livello di conoscenza dell'IA, le modalità di utilizzo, le percezioni relative all'impatto futuro, nonché le emozioni e i rischi associati.

Dall'analisi è emersa in modo chiaro la centralità della sicurezza psicologica (Clark, 2020), intesa come la percezione di essere inclusi, liberi di apprendere e di contribuire anche in situazioni di forte cambiamento. In linea con le evidenze di Edmondson et al. (2004), è stato osservato che un buon livello di sicurezza psicologica favorisce la condivisione delle conoscenze e l'apertura all'innovazione. Tuttavia, l'ingresso dell'IA nei contesti lavorativi tende a mettere sotto pressione questo equilibrio.

L'indagine ha identificato tre gruppi principali di risposta rispetto all'IA:

- “Entusiasti e competenti”, caratterizzati da un'elevata conoscenza e da un buon livello di serenità emotiva e supporto sociale;
- “Disorientati”, che presentano conoscenze limitate e una bassa percezione di supporto, sia emotivo che sociale;
- “Preparati ma isolati”, dotati di buone competenze cognitive ma con scarso supporto dal contesto relazionale (Kodinariya & Makwana, 2013).

Questi risultati suggeriscono che la sola acquisizione di competenze tecniche non è sufficiente a garantire una transizione fluida verso l'impiego dell'IA. Al contrario, il sostegno emotivo e sociale si configura come fattore critico per affrontare la fase di adattamento e per prevenire forme di esclusione o resistenza.

Inoltre, l'introduzione dell'IA solleva preoccupazioni legate alla possibile sostituzione delle persone nei processi lavorativi. Evidenze scientifiche mostrano come tale ansia sia particolarmente diffusa tra i lavoratori non specializzati in ambito digitale e tra coloro che operano in ruoli tradizionali (Howard, 2019).

L'incertezza rispetto alla propria adeguatezza e al futuro professionale alimenta un senso di minaccia che può ostacolare l'accettazione delle nuove tecnologie e compromettere il benessere psico-fisico.

Infine, sul piano etico e professionale, emerge con forza la convinzione che l'IA debba mantenere una funzione di supporto e non di sostituzione. Le competenze relazionali, empatiche e valoriali, caratteristiche del lavoro umano, non possono essere replicate da sistemi algoritmici. In tal senso, anche il quadro normativo europeo (AI Act – Regolamento (UE) 2024/1689) definisce l'utilizzo di IA in contesti ad alta intensità relazionale come “ad alto rischio”, richiedendo quindi particolare cautela e responsabilità.



⁴⁸ Coordinato da Gianfranco Cicotto, Sandro Furlan Radivo, Fabio Corona, che ringraziamo per aver reso disponibile questa sintesi dei risultati.

Alla luce di tali evidenze, si sottolinea l'importanza di:

- integrare nelle politiche di implementazione dell'IA azioni specifiche di accompagnamento psicologico e sociale;
- promuovere una formazione continua e multidimensionale, che affronti non solo le competenze tecniche ma anche le dimensioni emotive e identitarie della transizione digitale;
- rafforzare i presidi etici e le garanzie di inclusione, in modo da preservare il senso di agency e di valore personale di tutti i lavoratori.

Le evidenze raccolte dal **Project Work di SIPLO** confermano l'esistenza di un'ambivalenza diffusa nell'esperienza quotidiana dei lavoratori. Da un lato, l'IA è percepita come uno strumento utile per ottimizzare tempi e processi; dall'altro, la sua natura opaca e talvolta incomprensibile alimenta un senso di esclusione e perdita di controllo (Newman et al., 2023; Malik et al., 2023). Tale dinamica, già descritta come *black box effect*, può compromettere la percezione di equità e la fiducia organizzativa, elementi fondamentali per il benessere e l'engagement dei lavoratori (Greenberg, 1987).

Alla luce di queste considerazioni, risulta essenziale promuovere tra i lavoratori un'adeguata alfabetizzazione psicologica e digitale, volta a sviluppare una *AI awareness* (Arboh et al., 2025). Questo significa non solo acquisire competenze tecniche, ma anche potenziare la capacità di interpretare criticamente il funzionamento e le implicazioni delle tecnologie intelligenti.

Favorire un uso consapevole e riflessivo dell'IA aiuta infatti a prevenire sia il rischio di delega passiva sia il rifiuto aprioristico, promuovendo un'interazione equilibrata e responsabile tra persone e forme d'intelligenza artificiale.

È auspicabile integrare aspetti legati specificamente alla costruzione e al mantenimento della fiducia organizzativa attraverso:

- Strategie mirate per migliorare la comunicazione interna, basate sulla chiarezza informativa e sul coinvolgimento attivo dei lavoratori nella definizione degli obiettivi e delle modalità operative con l'IA.
- Misurazioni periodiche della percezione di equità e fiducia verso i sistemi decisionali algoritmici utilizzati nelle aziende (Glikson & Woolley, 2020).

In questo scenario, il contributo della psicologia del lavoro assume un ruolo strategico nel progettare e condurre processi di cambiamento organizzativo e culturale, orientati a rafforzare la fiducia informata e la capacità di gestire la complessità etica e relazionale derivante dall'integrazione dell'IA nei contesti organizzativi.

Riferimenti

- Arboh, F., Zhu, X., Atingabili, S., Yeboah, E., & Drokow, E. K. (2025). From fear to empowerment: The impact of employees' AI awareness on workplace well-being – a new insight from the JD–R model. *Journal of Health Organization and Management*, ahead-of-print. <https://doi.org/10.1108/JHOM-06-2024-0229>
- Clark, T. R. (2020). *The 4 stages of psychological safety: Defining the path to inclusion and innovation*. Berrett-Koehler Publishers.
- Commissione Europea. (2025, 4 febbraio). *Linee guida sulle pratiche di intelligenza artificiale vietate stabilite dal Regolamento (UE) 2024/1689 (AI Act)*. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
- Edmondson, A. C., Kramer, R. M., & Cook, K. S. (2004). Psychological safety, trust, and learning in organizations: A group-level lens. In R. M. Kramer & K. S. Cook (Eds.), *Trust and distrust in organizations: Dilemmas and approaches* (pp. 239–272). Russell Sage Foundation.
- Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2), 627–660. <https://doi.org/10.5465/annals.2018.0057>
- Greenberg, J. (1987). A taxonomy of organizational justice theories. *Academy of Management Review*, 12(1), 9–22. <https://doi.org/10.5465/amr.1987.4306437>
- Kodinariya, T. M., & Makwana, P. R. (2013). Review on determining number of clusters in K-means clustering. *International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS)*, 1(6), 90–95.
- Malik, A., Budhwar, P., & Kazmi, B. A. (2023). Artificial intelligence in HRM: Emerging risks and ethical governance. *Journal of Business Ethics*. <https://doi.org/10.1007/s10551-023-05550-4>
- Newman, D. T., Fast, N. J., & Harmon, D. J. (2023). Algorithmic reductionism and procedural justice: How AI alters organizational decision-making processes. *Organizational Behavior and Human Decision Processes*, 170, 104223. <https://doi.org/10.1016/j.obhdp.2023.104223>

6 Il ruolo del Medico Competente nel lavoro con IA

6.1 Il ruolo del Medico Competente nel lavoro con AI

Terenzio Cassina

Comitato scientifico ANMA

L'intelligenza artificiale come pure le tecnologie avanzate di automazione, robotica, sistemi di monitoraggio intelligenti, realtà virtuale e gestione algoritmica, stanno trasformando il mondo del lavoro offrendo tra l'altro opportunità per migliorare la SSL ma introducendo anche nuovi rischi fisici, psicosociali e organizzativi (1).

Questo cambiamento è inarrestabile e coinvolge tutti i settori produttivi. Alcuni degli esempi più riconoscibili e diffusi di intelligenza artificiale in contesti occupazionali includono strumenti software per le risorse umane (HR) (2), robot collaborativi (cobot) utilizzati in contesti industriali, assistenti virtuali nei centri di assistenza clienti, dispositivi indossabili utilizzati sia per migliorare la sicurezza sia per la formazione in tempo reale, piattaforme di gestione del lavoro freelance.

È evidente il mutamento che AI sta comportando nei **lavori amministrativi e gestionali cd "di ufficio"** ma l'IA sta rivoluzionando anche i **processi manifatturieri** (3):

- Ottimizzazione della catena di approvvigionamento: sistemi di AI nell'industria possono analizzare enormi quantità di dati per prevedere la domanda futura e così ottimizzare i livelli di inventario
- L'IA sta alimentando una nuova generazione di robot industriali che possono lavorare insieme agli esseri umani eseguendo compiti complessi e ripetitivi con precisione oppure operando, invece dell'uomo, in ambienti ad alto rischio. Questi sistemi automatizzati possono essere anche opportunità di inclusione nel mondo del lavoro per soggetti portatori di disabilità e più in generale per creare opportunità di "accomodamento ragionevole" per lavoratori con limitazioni dell'idoneità
- Progettazione e sviluppo di nuovi prodotti (Attraverso tecniche di generative design)
- L'IA può essere utilizzata per monitorare la qualità del prodotto in tempo reale
- Miglioramento della logistica attraverso la gestione dei magazzini e l'ottimizzazione delle consegne: l'AI consentendo l'analisi in tempo reale delle condizioni del traffico, delle previsioni meteo, del carico ottimale dei veicoli consente l'ottimizzazione delle rotte
- Miglioramento dell'efficienza produttiva: analizzare grandi quantità di dati in tempo reale consente di identificare inefficienze e colli di bottiglia nel processo produttivo e suggerire modifiche per ridurre i tempi di ciclo. Inoltre, l'analisi dei dati può aiutare a minimizzare gli sprechi di materiali, identificando esattamente dove si verificano le perdite e come evitarle
- Decisioni basate sui dati e ottimizzazione delle risorse: l'IA fornisce alle aziende strumenti avanzati di analisi che permettono di prendere decisioni più informate e strategiche
- Il lavoro su piattaforma digitale offre opportunità di lavoro più flessibile di cui possono trarre beneficio lavoratori con responsabilità familiari o con limitazioni geografiche (oltre che per i portatori di disabilità) migliorando per queste fasce l'accesso al mercato del lavoro.

Nelle attività industriale l'IA può anche contribuire a migliorare la SSL e creare un ambiente di lavoro più ergonomico. Tecnologie come automazione e robotica avanzata permettono di sostituire i lavoratori in ambienti pericolosi, riducendo l'esposizione a sostanze tossiche, temperature estreme e macchinari rischiosi.

Il contributo della IA al miglioramento della SSL riguarda anche la protezione individuale attraverso DPI di nuova generazione (Smart DPI): si tratta di sensori e dispositivi indossabili dotati di

componenti elettroniche che consentono di raccogliere dati in tempo reale e interagire con l'ambiente circostante anche attraverso moduli di trasmissione dei dati che consentono automaticamente di attivare procedure di emergenza prevenendo infortuni e migliorando la sicurezza (6). Questi dispositivi possono monitorare le condizioni dei lavoratori che operano in situazioni di alto rischio rilevando anche parametri relativi allo stato di salute, all'impegno cardiorespiratorio e muscolare.

L'IA può essere utilizzata per progettare postazioni di lavoro più ergonomiche, riducendo il rischio di infortuni e migliorando il benessere dei lavoratori

Formazione e informazione possono trarre un grande beneficio dai sistemi di AI sia per l'uso di specifiche piattaforme che, nelle attività di formazione avanzata, dei sistemi di realtà virtuale e aumentata che offrono simulazioni realistiche utilizzabili per la qualificazione del personale. La realtà virtuale e aumentata viene utilizzata anche per la preparazione dei lavoratori al riconoscimento dei pericoli e alla gestione delle emergenze.

Spesso anche le **attività dirigenziali di impresa** quali organizzazione, decisione e controllo vengono esercitati mediante il ricorso a processi decisionali automatizzati basati sull'utilizzo di strumenti algoritmici; si sta sviluppando l'uso del management algoritmico tramite il quale si assumono decisioni riguardanti le condizioni dei rapporti di lavoro, l'assegnazione di compiti, il monitoraggio e la valutazione delle prestazioni e del comportamento dei dipendenti. Si pone evidente il problema della c.d. "opacità algoritmica", ossia della "scarsa trasparenza intrinseca che contraddistingue i processi decisionali automatizzati, potendo accentuare lo stato di soggezione del lavoratore ovvero creare ulteriori e inediti squilibri nel rapporto di lavoro o, ancora, avallare pratiche discriminatorie"(4). Diviene pertanto cruciale la problematica connessa alla gestione trasparente e intelligibile degli algoritmi, in grado di superare, sul piano individuale, le asimmetrie informative fra lavoratore e impresa, e, su quello collettivo, di porre i rappresentanti dei lavoratori nelle condizioni di esercitare prerogative non solo di supervisione e di controllo, ma anche di partecipazione in relazione alle decisioni circa l'adozione dei sistemi di intelligenza artificiale (5)

"L'AI segna una nuova e significativa fase nel rapporto dell'umanità con la tecnologia", della persona con la macchina. In questo rapporto, soprattutto nell'ambito lavorativo, è necessario mantenere una netta distinzione tra i due fattori: "stabilire un'equivalenza troppo marcata tra intelligenza umana e IA comporta il rischio di cedere a una visione funzionalista, secondo la quale le persone sono valutate (*unicamente*) in base ai lavori che possono (riescono a) svolgere." (7)

I principali rischi nell'uso in ambito lavorativo dell'AI messi fino ad ora in evidenza dalla ancora scarsa letteratura esistente derivano da sovraccarico cognitivo, intensificazione del lavoro, isolamento sociale e sorveglianza/controllo eccessivi.

Secondo il documento **Documento ILO 2025** (1) i principali rischi per la salute e sicurezza del lavoro associati alla digitalizzazione includono:

1. Rischi infortunistici

- **Guasti meccanici:** Malfunzionamenti di robot e macchinari automatizzati possono causare incidenti.

2. Rischi fisici:

- **Esposizione a rumore e vibrazioni:** Tecnologie non ottimizzate possono aumentare il rischio di danni all'udito e disagio fisico.
- **Problemi ergonomici e da sovraccarico biomeccanico:** L'uso di esoscheletri o robot non adeguatamente progettati può provocare tensioni muscoloscheletriche.

- **Rischi chimici:** Batterie e componenti tecnologici possono rilasciare materiali tossici o corrosivi.
- Rischi oculovisivi, **posturali ed ergonomici** da prolungata adibizione a VDT o ad altri dispositivi quali tablet e smartphone

3. Rischi psicosociali:

- **Intensificazione del lavoro:** La gestione algoritmica può aumentare il ritmo e il carico di lavoro, causando stress e affaticamento.
- **Sovraccarico cognitivo:** L'eccesso di dati e informazioni può portare a difficoltà di concentrazione e stress mentale.
- **Burnout e stress:** Lavoro prolungato, mancanza di disconnessione, pressione sul ritmo del lavoro e la costante disponibilità possono portare ad esaurimento psico/fisico
- **Isolamento sociale:** Il lavoro da remoto e su piattaforma può ridurre le interazioni tra colleghi, aumentando la solitudine.
- **Insicurezza lavorativa:** Il timore di essere sostituiti da tecnologie automatizzate può condurre ad ansia e stress
- **Cyberbullismo e molestie:** Lavoratori online possono essere esposti a comportamenti abusivi o denigratori.

4. Rischi organizzativi:

- **Sorveglianza eccessiva:** Monitoraggio costante tramite dispositivi digitali può ridurre l'autonomia e aumentare la pressione psicologica.
- **Disuguaglianze:** Algoritmi non trasparenti possono perpetuare discriminazioni basate su genere, età o altre caratteristiche.

5. Rischi per la privacy:

- **Violazione dei dati:** La raccolta e l'elaborazione di dati personali tramite tecnologie digitali possono compromettere la privacy dei lavoratori.

6. Rischi legati alla sicurezza informatica:

- **Attacchi informatici:** Vulnerabilità nei sistemi digitali possono mettere a rischio la sicurezza dei lavoratori e delle operazioni aziendali.

Si tratta in parte di rischi non facilmente oggettivabili e misurabili a cui anche la più recente normativa europea fa esplicito riferimento. Il Regolamento UE sull'intelligenza artificiale 2024/1689 riconosce che i pregiudizi causati dall'intelligenza artificiale possono essere tanto materiali quanto immateriali (pregiudizio fisico, psicologico, sociale o economico)

Nell'articolo "Regulatory and Ethical Considerations on Artificial Intelligence for Occupational Medicine" di Antonio Baldassarre e coll. vengono analizzati nel dettaglio alcuni impatti dell'utilizzo occupazionale di sistemi di AI come pure le potenzialità che tali strumenti possono offrire per lo sviluppo della medicina del lavoro; nel seguito di questo contributo alcune volte riporteremo sintesi di parti di tale articolo che comunque è utile leggere per intero.

Ad agosto 2023, l'ILO ha pubblicato un documento di lavoro intitolato "Generative AI and Jobs: A Global Analysis of Potential Effects on Job Quantity and Quality", che presenta un'analisi completa della potenziale esposizione di occupazioni e compiti all'intelligenza artificiale generativa, in particolare LLM (Large Language Models) basati su Generative Pre-Trained Transformers (GPT), e le possibili implicazioni di tale esposizione per la quantità e la qualità del lavoro. A differenza delle precedenti ondate di trasformazione tecnologica che hanno interessato principalmente lavori poco

qualificati e ripetitivi con il più alto potenziale di automazione, i sistemi di apprendimento automatico possono migliorare le prestazioni in attività non di routine. La proliferazione di LLM basati su GPT sottolinea ulteriormente questa tendenza in evoluzione, data la loro capacità di eseguire attività cognitive come l'analisi di testo, la stesura di documenti e messaggi o l'estrazione di informazioni da repository privati e dal Web. Di conseguenza, questa nuova ondata di automazione avrà come obiettivo principalmente un gruppo diverso di lavoratori, in genere associato al "lavoro di conoscenza", compresi i lavori impiegatizi (8).

Anche i "lavoratori gig" (che svolgono lavoro a chiamata, occasionale e temporaneo, spesso svolto a distanza tramite piattaforme digitali) pur godendo di una certa autonomia tipica dei lavoratori autonomi, sono soggetti a un elevato grado di controllo sulle loro attività da parte delle piattaforme digitali per cui lavorano attraverso algoritmi di gestione (8).

Prevenzione dei rischi, CONTROLLO E mitigazione degli effetti

I rischi derivanti dalla evoluzione tecnologica e digitalizzazione sul posto di lavoro rientrano nell'ambito della direttiva 89/391/CEE del Consiglio, della direttiva quadro sulla salute e sicurezza sul lavoro e della legislazione nazionale che l'ha recepita.



La modalità di affronto più logica, seppur nella consapevolezza di una ancora iniziale conoscenza delle problematiche, sia per la valutazione del rischio che degli effetti sulla salute deve attuarsi secondo la metodologia della medicina del lavoro e con la finalità preventiva caratteristica della disciplina.

In un luogo di lavoro il ruolo del Medico Competente nella valutazione e gestione di questi rischi ancora poco conosciuti e trattati è di fondamentale importanza.

Tutte le pubblicazioni e gli interventi di esperti in tema di prevenzione dei rischi e del disagio correlato alla implementazione della AI riconoscono come fondamentale **l'attività di informazione, formazione e addestramento degli utilizzatori** svolgendo un processo di alfabetizzazione e di coinvolgimento nel processo di implementazione dei sistemi; il MC per rimanere inserito nel contesto aziendale dove opera deve svolgere il suo compito di tutela e promozione della salute partecipando come protagonista a questa attività.

Per il MC la partecipazione al **processo di valutazione di questi rischi emergenti** (Stress Lavoro Correlato, Tecnostress e più in generale i rischi psicosociali) dovrà avvenire attuando una stretta collaborazione con il datore di lavoro, il Responsabile del servizio di prevenzione e protezione (RSPP), i Rappresentanti dei lavoratori per la sicurezza (RLS), oltre che eventualmente con Psicologi del lavoro e delle organizzazioni, Ergonomi o 'Esperti' di IA.

Per la valutazione del rischio stress lavoro correlato (SLC) l'INAIL ha recentemente aggiornato il suo modello di valutazione inserendo una parte relativa all'innovazione tecnologica e al lavoro da remoto.

Per valutare i rischi psicofisici correlati all'attività lavorativa sono disponibili in letteratura anche altri metodi che alcuni medici competenti hanno già imparato a conoscere

- OiRA – Online Interactive Risk Assessment: www.osha.europa.eu/it
- Evaluacion de riesgos laborales asociados al teletrabajo : www.gobiernodecanarias.org/trabajo
- VIRA - VDT Integrated Risk Assessment: www.cesvor.com/metodo-vira.

Nel dicembre 2022 il gruppo di lavoro CIIP ha pubblicato il “Primo documento di consenso - Dallo stress lavoro correlato alla prevenzione dei rischi psicosociali” che affronta in modo sistematico la problematica offrendo anche numerosi strumenti di valutazione (13).

In una situazione così nuova e in rapida evoluzione anche lo svolgimento della **sorveglianza sanitaria** deve adeguarsi svincolandosi dall'obbligo normativo delle periodicità prefissate e dall'assioma visita del MC/giudizio di idoneità per orientarsi **come “accompagnamento” sanitario del lavoratore.**

La formulazione del giudizio di idoneità può articolarsi, se necessario, in esclusioni o limitazioni mirate alla ricerca dell'equilibrio fra le richieste della mansione e la salute psicofisica del lavoratore, attraverso un approccio empatico ed inclusivo.

Per quanto riguarda i rischi fisici le prescrizioni sono più consolidate e descritte da Linee Guida, Best practice e Documenti dedicati. In merito ai rischi psicosociali le indicazioni sono meno definite, ma possono essere schematizzate in tre gruppi adattando la classificazione proposta dal documento della Regione Marche (9):

-ambito organizzativo: cambio di destinazione lavorativa (modifica dei compiti, attenuazione del carico di lavoro mentale, ecc.), incremento delle pause, rimodulazione dell'orario di lavoro (work life balance).

-ambito tecnico: utilizzo di specifici strumenti, software, dispositivi;

-ambito procedurale: procedure di lavoro specifiche e/o individualizzate, rinforzo della formazione/informazione, miglioramento della comunicazione, tutoraggio.

Il MC deve anche tenere conto della presenza di predisposizioni o co-morbilità nella formulazione del giudizio di idoneità.

In definitiva, l'attività del MC in questo ambito si presenta particolarmente impegnativa, sia per la necessità di affrontare 'nuove' problematiche legate ai rischi psicosociali, sia per la mancanza di indicazioni stringenti e consolidate, sia infine per la rapidissima evoluzione tecnologica della IA, che richiede un aggiornamento continuo.

(Paolo Santucci, II)

La visita del MC potrebbe comprendere:

- Valutazione del livello di conoscenza, della confidenza d'uso e dell'impatto psicologico sul lavoratore nell'utilizzo di strumenti tecnologici e dell'AI sul lavoro. SIPLO (Società Italiana di Psicologia del lavoro e dell'Organizzazione) ha già utilizzato un questionario per la rilevazione dell'impatto psicologico dell'utilizzo dell'AI in ambito lavorativo (13) che potrebbe essere revisionato e finalizzato alla valutazione d'impatto sul singolo lavoratore.
- Valutazione clinica /strumentale correlata ai rischi fisici o comunque classici noti alla medicina del lavoro (rischi oculo/visivi e posturali)
- Valutazione dello stato di benessere generale (visita medica corredata da questionari specifici). Gli effetti sulla salute individuale possono essere monitorati dal medico competente attraverso l'applicazione di alcuni strumenti di screening che consentono di intercettare sintomi compatibili con condizioni di stress, ansia, depressione, reattività a eventi traumatici (14) per poi eventualmente procedere ad inviare dallo psicologo per l'approfondimento della condizione individuale.

GHQ 12. QUESTIONARIO SUL BENESSERE GENERALE Questionario auto-compilato composto da 12 domande che indaga il benessere generale e in particolare i sintomi depressivi ed ansiosi. Il cut-off è stato ridefinito al punteggio 14 (scala Likert).

Scala ZUNG. SCREENING DELLA SALUTE GENERALE (PSICOFISICO E SOCIALE) DELLA PERSONA. Questionario composto da 20 domande che consente di individuare lo stato di sofferenza psicologica e riconoscere la presenza di ansia (Dunstan & Scott et al., 2020).

PHQ 9. SCREENING SINTOMI DEPRESSIVI Questionario composto da 9 domande che guidano l'individuazione dei probabili casi di depressione attraverso il superamento di un punteggio pari o superiore a 10 costituisce la soglia ottimale per massimizzare sensibilità e specificità (Levis et al., 2019).

GAD 7. SCREENING DISTURBI D'ANSIA Questionario auto-compilato composto da 7 domande per la valutazione dell'ansia di stato che si accompagna ad un breve colloquio durante il quale viene indagato lo stato di salute generale (psicofisico e sociale) della persona.

IES-R. SCALA D'IMPATTO DELL'EVENTO. SCREENING PTSD [questionario](#) self-report di 22 item progettato per valutare il disagio soggettivo causato da "[eventi traumatici](#)". È comunemente utilizzato per misurare la gravità dei sintomi correlati al [disturbo da stress post-traumatico \(PTSD\)](#).

- Valutazione degli effetti del rischio Stress Lavoro Correlato e più in generale dei rischi psicosociali con strumenti subentranti secondo flow chart condivise. In medicina del lavoro e anche nelle attività del MC sono già entrati in uso vari questionari validati, autocompilabili o somministrabili al momento della visita, utilizzati soprattutto a scopo di ricerca su gruppi più o meno omogenei di lavoratori per la "misurazione del rischio".

Nello specifico delle problematiche correlate all'utilizzo dell'AI, anche pensando all'utilizzo di piattaforme a supporto dello smart working, la nostra attenzione si dovrà rivolgere in modo particolare al Tecnostress

TECNOSTRESS: stato di stress causato dall'utilizzo eccessivo e disfunzionale delle tecnologie digitali (ICT= Information and Communication Technologies), come computer, internet, email e smartphone, strumenti basati sull'uso di intelligenza artificiale che può avere un impatto negativo sulla salute e il benessere delle persone.

Le cause principali sono:

Eccessivo utilizzo:

L'uso improprio e prolungato delle ICT, ad esempio la continua connessione o la gestione di un flusso continuo di informazioni, può generare sovraccarico mentale e stress.

Tecnocomplessità:

La complessità delle tecnologie e la difficoltà di comprenderle o utilizzarle possono causare ansia e frustrazione.

Invasione della vita privata:

La tecnologia può invadere la sfera personale, rendendo difficile disconnettersi e creare un disequilibrio tra lavoro e vita privata.

Per la valutazione degli effetti del Tecnostress sono stati utilizzati anche altri questionari:

- Questionario di valutazione della percezione soggettiva dello stress lavoro-correlato contestualizzato al lavoro da remoto e innovazione tecnologica (INAIL 2025). Il questionario strumento-indicatore HSE è integrato da fattori che indagano: gli aspetti relativi al lavoro da remoto (10 item), l'innovazione tecnologica (15 item), il bilanciamento vita privata e vita lavorativa (2 item)(15)
- Job Content Questionnaire JCQ (Questionario per l'autovalutazione del compito lavoratore) R. KARASEK, 1985
- ERI (Effort/reward/imbalance) QUESTIONNAIRE di Siegrist et al. del 2008)

Il questionario di Siegrist è molto interessante perché valuta lo squilibrio percepito tra lo sforzo lavorativo richiesto e la ricompensa e tra l'altro valuta anche l'overcommitment ovvero ipercoinvolgimento nel lavoro, spesso causato dalle nuove tecnologie e nel lavoro a distanza ma anche correlato a fattori intrinseci di personalità.

OPPORTUNITA' E SFIDE (Sintesi di spunti di riflessione delle potenzialità offerte dall'AI per la medicina del lavoro e per l'attività di sorveglianza sanitaria dei lavoratori) da Antonio Baldassarre e coll. Med Lav 2024; 115 e seg.(8)

La disciplina della medicina del lavoro non può permettersi di rimanere stagnante di fronte all'adozione dell'intelligenza artificiale generativa da parte del mondo scientifico e del mondo produttivo e commerciale

L'intelligenza artificiale (IA) ha il potenziale per rivoluzionare la medicina del lavoro migliorando l'efficienza, l'accuratezza e l'assistenza sanitaria personalizzata per i lavoratori.

Al momento ci sono pochissime pubblicazioni che si occupano dell'uso dell'intelligenza artificiale nella medicina del lavoro ma si possono fare ipotesi di sviluppo non troppo lontane.

L'uso di chatbot come ChatGPT (Generative Pretrained Transformer) rappresenta un'opportunità in Medicina del lavoro per la capacità di generare frasi coerenti e contestualmente rilevanti. Potrebbero essere utilizzati per redigere documenti informativi, scrivere e aggiornare i DVR per soddisfare gli

obblighi normativi, potrebbero essere impiegati per sviluppare sistemi di gestione più efficienti per la sorveglianza sanitaria facilitando una raccolta dati più completa.

I sistemi di AI potrebbero essere impiegati (e già un po' lo sono) come assistenti virtuali per i professionisti della medicina del lavoro, fornendo risposte immediate in merito alle attuali normative sulla salute e sicurezza sul posto di lavoro. Sistemi analoghi possono permettere una più estensiva consultazione bibliografica di supporto all'attività del medico competente.

L'implementazione di modelli tecnologici sempre più complessi, basati anche sull'IA, sarà in grado di facilitare la transizione verso una medicina del lavoro "di precisione personalizzata, preventiva, predittiva" ... abilitando simulazioni e analisi predittive, ...che potrebbero essere attuate nella medicina del lavoro per lo studio e la previsione dei meccanismi di patogenesi della tecnopatia fornendo una comprensione più profonda del mondo fisico e abilitando prove basate sui dati.

L'uso di sistemi AI in medicina del lavoro, come in altri aspetti settori dell'assistenza sanitaria dove l'utilizzo è già avanzato, presenta problematiche inerenti, la privacy, la conservazione e protezione dei dati, l'etica della gestione e utilizzo delle informazioni.

Recentemente l'Organizzazione Mondiale della Sanità (OMS) ha pubblicato due documenti relativi all'IA generativa con particolare riferimento agli LLM (Large Language Models= modelli di intelligenza artificiale progettati per comprendere, interpretare e generare linguaggio umano) offrendo raccomandazioni per affrontare queste specifiche problematiche.

Il Codice etico internazionale per i professionisti della salute sul lavoro, aggiornato l'ultima volta nel 2014, non contiene né raccomandazioni né linee guida sull'uso dell'IA.

La preoccupazione circa la sicurezza dei dati, la necessità di quadri normativi solidi e la garanzia che queste tecnologie siano accessibili ed eque per tutti i pazienti è stata centrale nella campagna Healthy Workplaces dell'EU-OSHA Safe and Healthy Work in the Digital Age, in corso dal 2023 al 2025. In cima ci sono le allucinazioni LLM, un termine risultato da un'antropomorfizzazione del lessico dell'intelligenza artificiale e attualmente utilizzato quando i sistemi basati su Large Language Models (LLM) si connettono e interpretano male i dati producendo informazioni che sembrano coerenti e plausibili ma sono errate perché mancano di accuratezza fattuale o validità medica.

...quando interagiamo con un LLM stiamo interrogando un sistema progettato per generare testi coerenti, ma non necessariamente veri. Conseguentemente le "allucinazioni" e cioè la produzione di enunciati falsi ma plausibili, è un effetto collaterale probabile e inevitabile conseguente al modo con cui questi sistemi sono costruiti (10)

Questo fenomeno pone un problema significativo per le applicazioni mediche perché i professionisti sanitari potrebbero imbattersi in contenuti generati dall'intelligenza artificiale che potrebbero portare a diagnosi o trattamenti errati se ci si affida senza controllo a quanto prodotto dall'AI generativa.

In medicina l'IA è un supporto nella diagnosi e nella cura dei malati, può migliorare la ricerca e facilitare l'accesso ai servizi sanitari (telemedicina e sistemi di monitoraggio a distanza), ma non può sostituire il medico nella relazione di cura con il paziente, che è più etica che tecnologica.

Il medico resta sempre responsabile delle sue azioni e quindi non può delegare le sue decisioni alla IA senza verificare i suoi "prodotti" alla luce della specifica conoscenza scientifica ma anche della conoscenza fattuale del paziente.

L'IA è uno strumento potenzialmente prezioso anche per i medici del lavoro, ma non può sostituirli. Ciò vale specialmente quando i medici devono prendere decisioni complesse; per il medico competente può esserle l'espressione di un giudizio d'idoneità alla mansione specifica in una

situazione di malattia che richiede attenzione alla tutela della salute ma anche alla dignità della persona nel suo insieme tenendo conto anche delle aspettative professionali, economiche e sociali. trovando soluzioni creative, coinvolgendo altri ruoli aziendali e attori esterni, abilità che l'IA non possiede.

CONCLUSIONI E PROSPETTIVE

Sarebbe auspicabile che attraverso le associazioni scientifiche dei Medici del Lavoro (SIML, ANMA, SNOP, CIIP, ecc) si sviluppi una specifica attività di informazione dei medici competenti e dei medici del lavoro dei Servizi territoriali di prevenzione sulla tematica del tecnostress, si condividano e concordino gli strumenti di valutazione armonizzando la modalità di somministrazione, si definisca un sistema di raccolta dati (ad adesione volontaria dei MC) che consenta la raccolta e verifica dei risultati con la conseguente evoluzione dei set di valutazione e degli interventi di mitigazione degli effetti.

Tenuto conto che l'AI è fonte di opportunità e sfide non procrastinabili per la Medicina del Lavoro è necessario anche che le Università e le scuole di specialità investano nella ricerca in questo settore e sviluppino una didattica ad essa coerente.

Le società scientifiche che riuniscono gli specialisti in medicina del lavoro, ma anche le associazioni datoriali e dei lavoratori dovranno sollecitare modifiche normative finalizzate a che la sorveglianza sanitaria dei lavoratori possa uscire da vincoli burocratici per aprirsi ad uno sviluppo di qualità delle prestazioni in linea con l'evoluzione tecnologica della medicina: un percorso che, a mio parere, potrà avvenire solo in una interazione delle attività di prevenzione e tutela della salute affidate al datore di lavoro con il Servizio Sanitario Nazionale.

Fonti bibliografiche

1. Documento ILO 2025: "Rivoluzionare la salute e la sicurezza sul lavoro: L'intelligenza artificiale e la digitalizzazione nel mondo del lavoro"
2. Verso sistemi di gestione del personale basati su intelligenza artificiale e algoritmi per luoghi di lavoro più produttivi, più sicuri e più sani – EU-OSHA, 2025 <https://healthy-workplaces.osha.europa.eu/it/publications/towards-ai-based-and-algorithmic-worker-management-systems-more-productive-safer-and-healthier-workplaces>
3. Alessandra Talarico : Intelligenza artificiale e industria: come le macchine stanno cambiando la produzione (Pubblicato il 22 lug 2024) <https://www.agendadigitale.eu/industry-4-0/intelligenza-artificiale-e-industria-come-le-macchine-stanno-cambiando-la-produzione/>
4. Stefano Cairolì, Università degli Studi di Perugia: "Intelligenza artificiale e sicurezza sul lavoro: uno sguardo oltre la siepe" in "Diritto della sicurezza sul lavoro" dell'Osservatorio Olympus, 2/2024
5. Paolo Pascucci, Università di Urbino Carlo Bo: "Sistemi di intelligenza artificiale e tutela della salute e della sicurezza sul lavoro (in questo e book pag. 137-140)
6. Castrignanò e coll : "Sicurezza in edilizia e innovazione tecnologica: esempi di utilizzo" (congresso ANMA 2025)

7. ANTIQUE ET NOVA rapporto della Santa Sede sul rapporto AI e intelligenza umana
https://www.vatican.va/roman_curia/congregations/cfaith/documents/rc_dof_doc_20250128_antiqua-et-nova_it.html
8. Antonio Baldassarre, Martina Padovan : “Regulatory and Ethical Considerations on Artificial Intelligence for Occupational Medicine” (*Med Lav* 2024; 115 (2): e2024013 DOI: 10.23749/mdl.v115i2.15881)
9. Piano regionale prevenzione Marche 2020/2025. Buone pratiche nella sorveglianza sanitaria sui rischi psicosociali
10. Walter Quattrociochi, Università Sapienza di Roma: “L’AI non è davvero intelligente, è una questione di statistica. Le allucinazioni? Inevitabili, è una caratteristica intrinseca”
https://www.corriere.it/tecnologia/25_giugno_03/l-ai-non-e-intelligente-e-una-questione-di-statistica-le-allucinazioni-inevitabili-e-una-caratteristica-intrinseca-9699a0b6-4952-4d69-bd8d-d4772bdb2xlk.shtml
11. P.Santucci; seminario di formazione AIFES (28 febbraio 2025)
12. Questionario SIPL0:
https://docs.google.com/forms/d/e/1FAIpQLSc1JiWY09sQRE_57_V8TTdQDkSXVKQYiAuw_JOBtTAgc63e_A/viewform)
13. CIIP - Primo documento di consenso - Dallo stress lavoro correlato alla prevenzione dei rischi psicosociali, dicembre 2022 https://www.ciip-consulta.it/index.php?option=com_phocadownload&view=file&id=53:11-primo-documento-di-consenso-dallo-stress-lavoro-correlato-alla-prevenzione-dei-rischi-psicosociali&Itemid=609
14. Dr.ssa Antonia Ballottin: “Dalla valutazione del carico mentale alla valutazione dei rischi psicosociali” congresso ANMA Bologna 24 maggio 2024 chrome-extension://efaidnbmnnnibpcaipcgklcfeindmkaj/https://www.ciip-consulta.it/images/eventlist/Eventi2024/240523-anma/3.6%20Ballottin%20A.%20-%20DA_CARICO_MENTALE_A_RISCHI_PSICOSOCIALI.pdf
15. Modulo contestualizzato al lavoro da remoto e all’innovazione tecnologica INAIL 2025
<https://www.inail.it/portale/it/inail-comunica/pubblicazioni/catalogo-generale/catalogo-generale-dettaglio.2025.04.metodologia-valutazione-gestione-rischio-stress-lavoro-correlato.html>

7 Aspetti giuridici ed etici

7.1 Sistemi di intelligenza artificiale e tutela della salute e della sicurezza sul lavoro

Paolo Pascucci

Università di Urbino Carlo Bo

1. Nell'ampia discussione sul rapporto tra lavoro e intelligenza artificiale, l'interesse per la tutela della salute e della sicurezza è centrale.

Ciò non sorprende se si pensa che l'introduzione dei sistemi di intelligenza artificiale incide sull'organizzazione dell'impresa e del lavoro, cioè sull'elemento che è in grado di generare i rischi per la salute e la sicurezza delle persone che lavorano nell'ambito di tale organizzazione.

Peraltro, l'interesse per il tema va probabilmente anche ascritto al fatto che l'intelligenza artificiale costituisce una sfida a talune certezze, reali o apparenti.

2. Una certezza reale riguarda l'impatto di quella che possiamo chiamare la macchina, che è sempre stato messo in relazione al ruolo del lavoratore, sia che valga ad alleviarne la fatica, o per modificarne le modalità della prestazione, quando non per sostituirsi ad esso.

Senonché, pur non facendo venir meno questi scenari, alcune moderne macchine intelligenti – specie nel contesto del *management* algoritmico – incidono anche sul ruolo del datore di lavoro, sulla sua posizione di *dominus* dell'organizzazione, sull'esercizio dei suoi poteri fin quasi a personalizzarlo e ridimensionarne il ruolo, talora a far sì che la figura datoriale si impersoni nella macchina e talaltra a far emergere tra datore di lavoro e lavoratore quello che è stato definito terzo elemento.

Se ciò non può far velo alle eventuali responsabilità datoriali in tema di salute e sicurezza sul lavoro, peraltro da rileggere in una cornice più ampia che chiama in causa anche le responsabilità dei soggetti contemplati dal Regolamento europeo sull'intelligenza artificiale 2024/1689, tuttavia non dovrebbe trascurarsi il rischio che, appannando il ruolo del datore di lavoro, certe forme di intelligenza artificiale ne offuschino anche la sua dignità di soggetto socialmente responsabile, giacché ad essere messa a repentaglio dall'intelligenza artificiale non è solo la salute e la dignità del lavoratore, bensì anche quella particolare dignità del datore di lavoro insita nella rilevanza costituzionale dell'impresa.

3. Una certezza più apparente che reale messa in crisi dall'intelligenza artificiale riguarda la distinzione tra i rischi e le misure di prevenzione e protezione. Infatti, se la tecnologia è sempre stata fonte di certi rischi, è stata però spesso anche misura di prevenzione per altri rischi, il che può valere anche per l'intelligenza artificiale.

D'altro canto, come emerge nello stesso d.lgs. n. 81/2008, è la stessa organizzazione, nella quale la tecnologia è introiettata, a costituire la fonte dei rischi, ma anche lo strumento per evitarli e contrastarli.

D'altronde, a proposito delle potenzialità preventive di certi sistemi di intelligenza artificiale, l'esplicito riferimento dell'art. 2087 cod. civ. alla tecnica e la dimensione aperta dell'obbligo di sicurezza non solo non escludono, ma anzi potrebbero imporre di considerare tra le misure da adottare anche certi sistemi intelligenti capaci di migliorare le condizioni di lavoro, eliminando o mitigando certi rischi.

Senza potersi soffermare sull'intreccio fra i rischi e i benefici dell'intelligenza artificiale, occorre però osservare che, se la deroga posta per motivi di sicurezza dall'art. 5, par. 1, lett. *f*, del citato Regolamento europeo sull'intelligenza artificiale al generale divieto di pratiche volte a inferire le emozioni di una persona fisica nell'ambiente di lavoro da un lato potrebbe consentire di monitorare fatica o distrazioni del lavoratore prevenendo eventuali infortuni, da un altro lato evoca tuttavia delicate questioni connesse alla raccolta di dati anche sensibili in relazione alle regole sulla protezione dei dati personali.

4. Tra i vari rischi per la salute e la sicurezza sul lavoro connessi alla diffusione di strumenti basati sull'intelligenza artificiale non rientrano solo rischi fisici, ma anche e soprattutto rischi psicosociali specialmente con riferimento ai sistemi di intelligenza artificiale riconducibili al *management* algoritmico tramite i quali si assumono decisioni riguardanti le condizioni dei rapporti di lavoro, l'assegnazione di compiti, il monitoraggio e la valutazione delle prestazioni e del comportamento dei dipendenti.

Si tratta di rischi non facilmente oggettivabili e misurabili a cui anche la più recente normativa eurounitaria fa esplicito riferimento.

Così la Direttiva sul miglioramento delle condizioni del lavoro mediante piattaforme digitali 2024/2831 cerca di riumanizzare la gestione del lavoro prevedendo l'obbligo di valutare i rischi dei sistemi decisionali o di monitoraggio automatizzati, in particolare con riguardo ai rischi di infortuni e a quelli psicosociali ed ergonomici, oltre a disporre il divieto di utilizzare sistemi che mettano indebitamente sotto pressione i lavoratori o comunque a rischio la loro sicurezza e salute fisica e mentale.

Anche il nuovo Regolamento macchine 2023/1230 impone l'eliminazione o la riduzione al minimo del disagio, della fatica e delle tensioni psichiche e fisiche dell'operatore, e di evitare un ritmo di lavoro condizionato dalla macchina e un controllo che richieda una concentrazione prolungata.

E anche il Regolamento sull'intelligenza artificiale 2024/1689 riconosce che i pregiudizi causati dall'intelligenza artificiale possono essere tanto materiali quanto immateriali compreso il pregiudizio fisico, psicologico, sociale o economico, il che vale anche per i contesti lavorativi, tanto più che i sistemi di intelligenza artificiale impiegati nell'ambito dei rapporti di lavoro dovrebbero essere tendenzialmente classificabili come ad alto rischio.

5. L'aspetto più delicato riguarda la sfida dei sistemi di intelligenza artificiale all'obbligo di valutazione dei rischi presenti nell'organizzazione del lavoro a causa talora della difficile percezione di tutti i possibili effetti dell'utilizzo di quei sistemi soprattutto con riferimento a quelli che possono emergere nel caso dei sistemi generativi.

Ciò pone seri interrogativi sulla tenuta della nostra disciplina in materia di salute e sicurezza sul lavoro, la quale, in base al principio di prevenzione, obbliga a valutare i rischi conosciuti e prevedibili, laddove il cosiddetto ignoto tecnologico parrebbe piuttosto evocare il ricorso al più ampio principio di precauzione, applicato in ambito ambientale e relativo ai rischi su cui non vi siano certezze

scientifiche, che tuttavia rischierebbe di ampliare eccessivamente il perimetro dell'obbligo di sicurezza datoriale con evidenti problemi anche dal punto di vista sanzionatorio in omaggio al principio di tassatività.

In ogni caso, è evidente che la valutazione dei rischi di tali sistemi esige il possesso di particolari conoscenze da acquisire mediante specifici percorsi formativi.

Ove mai si ipotizzasse di assimilare i sistemi di intelligenza artificiale alle attrezzature di lavoro, già oggi per il datore di lavoro la formazione sarebbe obbligatoria dato che, in base all'art. 73, comma 4-bis, del d.lgs. n. 81/2008, ove egli faccia uso di attrezzature che richiedano per il loro impiego conoscenze o responsabilità particolari in relazione ai loro rischi specifici, deve provvedere alla propria formazione e al proprio addestramento specifico al fine di garantire l'utilizzo delle attrezzature in modo idoneo e sicuro.

Ma l'esigenza di una specifica formazione varrebbe anche per tutti coloro che a vario titolo partecipano alla valutazione dei rischi, non dovendosi escludere la necessità anche di un supporto di esperti da coinvolgere prima dell'adozione dei sistemi automatizzati, come la Direttiva sulle piattaforme prevede a supporto dei rappresentanti dei lavoratori delle piattaforme digitali.

Per altro verso, considerando che, in base al citato Regolamento europeo, i sistemi di intelligenza artificiale che riguardano il lavoro dovrebbero essere considerati ad alto rischio e come tali assoggettati a pregnanti obblighi sia per i *provider* (i progettisti, gli sviluppatori e i produttori) – tra cui quelli di valutazione dei rischi, di trasparenza, di monitoraggio e di segnalazione – sia per i *deployer* (chi utilizza o rende disponibili sotto la propria autorità sistemi di intelligenza artificiale, compresi i datori di lavoro), la valutazione dei rischi effettuata dal datore di lavoro presupporrebbe uno stretto raccordo con gli adempimenti che il Regolamento europeo pone in capo al *provider*.

D'altro canto, non si deve trascurare che, in caso di infortunio causato da una macchina (e perché non anche da un sistema di intelligenza artificiale?) per l'inosservanza degli obblighi gravanti sui progettisti, fabbricanti e fornitori, l'art. 18, comma 3-bis, del d.lgs. n. 81/2008 riconduce la responsabilità non solo ad essi, ma anche allo stesso datore di lavoro ove non abbia vigilato sull'adempimento dei loro obblighi previsti dagli artt 22, 23 e 24 dello stesso d.lgs. n. 81/2008, i quali ora potrebbero forse integrarsi con quelli del Regolamento europeo sull'intelligenza artificiale.

6. Se per un verso l'irruzione sulla scena dell'intelligenza artificiale potrebbe rendere necessari alcuni adattamenti della nostra disciplina prevenzionistica, per altro verso non può però scardinarne i caposaldi, a partire da quello della prevenzione primaria secondo cui i rischi debbono innanzitutto essere evitati o eliminati alla fonte.

Un dubbio in tal senso potrebbe emergere dal testo definitivo della menzionata Direttiva sul lavoro su piattaforma dal quale è scomparso l'esplicito obbligo delle piattaforme digitali di evitare innanzitutto i rischi dei sistemi decisionali e di monitoraggio automatizzati che era stato proposto da alcuni emendamenti del Parlamento europeo.

Senonché, considerare sempre inevitabili i rischi connessi all'intelligenza artificiale non solo striderebbe con l'esplicita salvezza della Direttiva quadro 89/391/CEE da parte della Direttiva sulle piattaforme, ma significherebbe riconoscere una sorta di totale sudditanza alla tecnologia e una impotenza a concepire un'organizzazione di lavoro che possa se non altro fare a meno di alcuni rischi.

D'altronde, la valutazione dei rischi è innanzitutto valutazione delle possibilità di insorgenza del rischio per evitarlo e solo in secondo luogo è valutazione del rischio in atto.

7. Un altro aspetto che emerge nei recenti interventi eurounitari riguarda il profilo partecipativo.

Sia nella Direttiva sulle piattaforme digitali, sia nel Regolamento europeo sull'intelligenza artificiale emerge l'immagine di una gestione trasparente e intelligibile degli algoritmi, in grado di superare, sul piano individuale, le asimmetrie informative fra lavoratore e impresa, e, su quello collettivo, di porre i rappresentanti dei lavoratori nelle condizioni di esercitare prerogative non solo di supervisione e di controllo, ma anche di partecipazione in relazione alle decisioni circa l'adozione dei sistemi di intelligenza artificiale.

Il che rappresenta una sfida importante per il sindacato e per la contrattazione collettiva per quanto attiene all'esigenza di una specifica formazione dei rappresentanti dei lavoratori.

8. A ben guardare, la via maestra per incanalare nei giusti binari l'inclusione dei sistemi di intelligenza artificiale nell'organizzazione aziendale pare essere l'adozione e l'efficace attuazione dei modelli di organizzazione e di gestione della sicurezza sul lavoro evocati dall'art. 30 del d.lgs. n. 81/2008.

Infatti, in quanto basati, in virtù dei sistemi di gestione volontari di cui si avvalgono (come la ISO 45001), su procedure trasparenti e tracciabili di programmazione, attuazione, monitoraggio, riesame ed eventuale modifica dei processi organizzativi, tali modelli paiono infatti gli strumenti più idonei per far sì che i sistemi di intelligenza artificiale che si inseriscono nell'organizzazione del lavoro siano utilizzati in modo da essere costantemente controllati anche nella loro evoluzione.

D'altronde, se è evidente che i rischi generati dall'intelligenza artificiale sono rischi di organizzazione, sarebbe illogico non valorizzare proprio quei modelli che il legislatore indica come strumenti indispensabili per prevenire i reati presupposto di quella responsabilità amministrativa delle persone giuridiche collegata alla colpa di organizzazione.

Così come sarebbe illogico non valorizzare correlativamente quell'asseverazione dell'adozione e dell'efficace attuazione dei predetti modelli organizzativi che l'art. 51 del d.lgs. n. 81/2008 ha affidato al sistema della pariteticità a ulteriore conferma della dimensione necessariamente partecipata del sistema della salute e della sicurezza sul lavoro.

7.2 Intelligenza Artificiale, AI Act e sicurezza del lavoro

Giovanni Scudier

C&S Studio Legale Casella e Scudier – Padova

7.2.1 La questione definitoria

Una riflessione di natura giuridica sulla Intelligenza Artificiale (IA) rispetto alla sicurezza e salute nei luoghi di lavoro non può prescindere dall'affrontare la questione definitoria: cosa intendiamo, quando parliamo di Intelligenza Artificiale?

È una domanda necessaria, perché non esiste una definizione di IA riconosciuta universalmente per tutti i settori e tutti i contesti, e tantomeno nello specifico ambito normativo della sicurezza e salute del lavoro.

Sotto il nome di IA troviamo pratiche ed esperienze diverse sia dal punto di vista della tecnologia, sia degli effetti sul mondo esterno, sia dei problemi legali/etici/economici/sociali che ne derivano; sulla nozione stessa di "intelligenza" riferita alla macchina le opinioni sono le più disparate, siano esse tecniche, filosofiche, sociologiche, giuridiche.

Quanto alle forme in cui si manifesta quella che viene chiamata IA, esistono sistemi/applicazioni/software privi di corporeità; robot contraddistinti dalla dimensione fisica della macchina (a loro volta enormemente diversi tra loro andando dal robot industriale al robot indossabile alle applicazioni di biorobotica); algoritmi che ottimizzano ed automatizzano processi valutativi; veicoli autonomi terrestri o volanti. L'elenco potrebbe continuare, contraddistinto dalla estrema eterogeneità delle voci che lo compongono.

Quanto al significato della intelligenza, accanto alla ricerca di una intelligenza generale, in grado di emulare ed anzi superare il cervello umano, le esperienze attuali sembrano caratterizzarsi per la loro riconducibilità ad ambiti specifici, rispetto ai quali l'intelligenza viene individuata nella loro capacità di raggiungere obiettivi predeterminati. Anche in questo caso, ciò accade in modi diversi e con diversi livelli di risultato.

Anche le esperienze che impattano il mondo della sicurezza e salute del lavoro sono molte e variegate; numerose di esse sono menzionate nei contributi di questo E-book.

Ricercando un riferimento per così dire istituzionale, il recente Rapporto ILO⁵⁰ suddivide le "tecnologie e processi lavorativi" che contraddistinguono queste esperienze in cinque categorie: l'automazione e la robotica avanzata; gli strumenti e sistemi di monitoraggio intelligenti; la realtà estesa e virtuale; la gestione algoritmica del lavoro; la modifica delle modalità del lavoro attraverso la digitalizzazione.

Rispetto al tema definitorio, è significativo osservare che il Rapporto, che pure presenta la "Intelligenza Artificiale" nel titolo, la considera poi una parte del contesto assai più ampio della Digitalizzazione, che è la vera protagonista del Report e della domanda a cui esso vuole dare risposta.⁵¹

Così, il Rapporto ricorda che "Secondo l'OIL, la digitalizzazione è intesa, in senso lato, come l'applicazione delle tecnologie digitali, e quindi di informazioni o dati digitalizzati, nell'economia e nella società (GB.350, Gruppo di lavoro sulla dimensione sociale della globalizzazione. Sfide e

⁵⁰ ILO-Organizzazione Internazionale del Lavoro, Rapporto Mondiale – Rivoluzionario la salute e la sicurezza sul lavoro: L'intelligenza artificiale e la digitalizzazione nel mondo del lavoro, 2025

⁵¹ ILO, cit., p. 5: "In che modo la digitalizzazione sta trasformando la sicurezza e la salute sul lavoro?"

opportunità della digitalizzazione)⁵²; poi precisa che “L'intelligenza artificiale è una componente fondamentale della digitalizzazione”⁵³.

Porre la questione definitoria significa allora ricercare, all'interno dell'infinito mondo della digitalizzazione, quali sono gli elementi che contraddistinguono la IA. Una volta che avremo fatto questo, potremo domandarci come questi elementi distintivi si pongono rispetto alla sicurezza del lavoro: potremo verificare se e come alle “pratiche innovative”⁵⁴ che chiamiamo IA si possono applicare per via interpretativa principi e regole tradizionali del sistema normativo della sicurezza e salute nei luoghi di lavoro, o se invece l'IA pone un problema di *disruption* rispetto a paradigmi consolidati da decenni. Potremo insomma provare a porre delle domande, consapevoli che le risposte sono tutte da scrivere, come tutta da scrivere è l'esperienza umana sulla IA.

7.2.2 La definizione di Intelligenza Artificiale nell'AI ACT.

Dovendo compiere una riflessione che riguarda il mondo del diritto, ci sembra inevitabile provare a rispondere alla domanda definitoria guardando alle norme.

Il riferimento fondamentale non può che essere il Regolamento Ue 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, al quale ci riferiremo d'ora in poi come AI ACT.

Esso definisce così (art. 1 n. 1) un «*sistema di intelligenza artificiale*»:

“un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.”

È una definizione analoga a quella della Convenzione Quadro del Consiglio d'Europa sull'intelligenza artificiale del 5 settembre 2024 (art. 2); è la stessa definizione che ritroviamo nell'articolo 2 del Disegno di legge italiano all'esame del Parlamento⁵⁵.

Come la migliore dottrina giuridica ha avuto modo di approfondire, si tratta di una definizione che non descrive una tecnologia, ma semmai i suoi utilizzi; che non individua e definisce dei settori, ma detta dei principi; essa vuole avere “*la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici*” (Considerando 12), facendo così salvo il principio di neutralità tecnologica, ma al tempo stesso agevolare “*un'ampia accettazione*”.

Gli elementi che secondo questa definizione distinguono un sistema di IA “*dai tradizionali sistemi software o dagli approcci di programmazione più semplice*” (ancora Considerando 12) sono: l'automazione; la progettazione finalizzata a specifiche modalità di funzionamento; l'autonomia; l'adattabilità dopo la diffusione; la produzione di output in grado di influenzare l'ambiente esterno al sistema, sia esso un ambiente fisico o virtuale; la deduzione di tali output da input che il sistema di IA riceve; l'esistenza di obiettivi espliciti o impliciti.

Sono due gli elementi, all'interno di questa definizione, per i quali una riflessione incentrata sulla sicurezza e salute nei luoghi di lavoro propone a nostro avviso le domande più rilevanti: l'autonomia e l'adattabilità.

⁵² ILO, cit., p. 7, nota 1.

⁵³ ILO, cit., p. 7, nota 2. La sottolineatura è nostra.

⁵⁴ ILO, cit., ibidem.

⁵⁵ Per esigenze di sintesi, in queste note non viene preso in considerazione il “modello di IA per finalità generali”, la cui definizione è contenuta nell'art. 1 n. 63 dell'AI ACT, e che comprende anche i sistemi di intelligenza generativa aventi crescente diffusione.

L'autonomia è l'elemento per così dire necessario per aversi intelligenza artificiale, quello che la rende tale: come si legge nel Considerando (12), la definizione stessa di IA *“non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico”*.

L'adattabilità invece, sempre secondo il Considerando (12), è una caratteristica *“che un sistema di IA potrebbe presentare dopo la diffusione”*, cioè dopo la immissione sul mercato, la messa in servizio e l'inizio del suo utilizzo; e *“si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso”*.

Questi due elementi ci dicono che le caratteristiche tecniche, le modalità di funzionamento, le interazioni con l'ambiente esterno di un sistema di IA che vanno considerate non sono soltanto quelle conosciute/conoscibili, previste/prevedibili al momento di immetterlo sul mercato o di utilizzarlo: occorre invece ricordare che il sistema di IA (i) opera secondo regole che può definire da sé nonché (ii) opera secondo regole che possono cambiare nel tempo, e cambiare per iniziativa del sistema stesso⁵⁶.

Il tema dell'autonomia e dell'autoapprendimento di una intelligenza “artificiale” non riguarda certo soltanto la sicurezza del lavoro: il dibattito sulla IA sta ponendo in maniera assolutamente generale la questione, se e quanto gli strumenti giuridici di cui disponiamo siano sufficienti e adeguati per trovare le risposte, o se non sia invece indispensabile produrre nuovi strumenti che tengano conto del cambio di paradigma introdotto dalla esistenza di “sistemi” autonomi e adattabili in grado di generare output senza l'intervento dell'essere umano.⁵⁷

Ragionando di sicurezza del lavoro, è con i paradigmi giuridici della materia che dobbiamo affrontare questa autonomia e questa adattabilità che si evolve nel tempo, segnalando fin d'ora la necessità di una riflessione più profonda quando autonomia e adattabilità acquisiscono rilevanza dominante ed il sistema di IA assume un ruolo prevalente rispetto alla presenza dell'umano, quando si va cioè verso la frontiera⁵⁸.

Per sviluppare questa riflessione, riteniamo sia prima necessario almeno tratteggiare i contenuti dell'AI ACT e le risposte che il legislatore europeo ha ritenuto di dare alle sfide poste dai sistemi di IA.

7.2.3 L'approccio dell'AI ACT

7.2.3.1 La persona al centro

La prima e fondamentale risposta dell'AI ACT è che, al centro di tutto, è la persona.

Scopo del regolamento è sì migliorare il funzionamento del mercato, promuovere l'innovazione, istituire un quadro giuridico uniforme per promuovere lo sviluppo dell'IA, ma non una IA qualsiasi, bensì *“un'intelligenza artificiale antropocentrica e affidabile”*, in grado di garantire *“un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali”*. Così recitano il

⁵⁶ Ovviamente, i “livelli di autonomia” possono essere diversi, come recita lo stesso AI ACT; anzi è probabile che sotto il nome di IA vengano compresi esempi in cui l'autonomia è modesta, quando non addirittura inesistente (sono sistemi puramente automatici, per esempio, i robot chirurgici che dipendono esclusivamente dall'azione dell'operatore).

⁵⁷ La dottrina giuridica, così come gli studiosi dei temi etici, sociali, economici (oltre che ovviamente per quelli più spiccatamente tecnologici) stanno affrontando da tempo le sfide che ne derivano: basti pensare alle questioni della soggettività dell'IA (l'IA Agente), della (mancanza di) trasparenza e conoscibilità delle regole di produzione dell'output, della necessità di risolvere il rebus della responsabilità.

⁵⁸ Secondo la felicissima espressione utilizzata nella rubrica di P. BENANTI, *Etica di frontiera*, ne *Il Sole 24 Ore*.

Considerando (1) con cui si apre il Regolamento e il Considerando (176) che quasi lo chiude; nello stesso modo comincia l'articolato (cfr. art. 1).

Da questo punto di vista, si può certo dire che i valori fondativi su cui si regge e per cui esiste la normativa di sicurezza e salute del lavoro sono la stella polare anche rispetto all'AI ACT.

L'IA antropocentrica non rappresenta, peraltro, soltanto una dichiarazione di principio: essa viene perseguita tramite l'affermazione di principi etici che poi diventano obbligo giuridico. Per effetto di questi principi e questi obblighi, la persona umana non rimane soltanto sullo sfondo rispetto alla regolazione dei sistemi di IA, come titolare di diritti e beneficiaria di tutela: la persona umana è essa stessa artefice della tutela e protagonista nel funzionamento dei sistemi.

Ed infatti, il primo dei principi vincolanti per una IA "eticamente valida" è il principio di "**intervento e sorveglianza umana**", in forza del quale "...i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani" (Considerando 27).

Il principio etico diventa poi obbligo quando ci troviamo in presenza di sistemi di IA ad alto rischio (su cui v. *infra*): per questi la sorveglianza umana costituisce vero e proprio requisito ai sensi dell'art. 14, secondo cui essi devono essere progettati e sviluppati "*in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso*".

La sorveglianza include: la comprensione del sistema; la corretta interpretazione degli output; il monitoraggio anche al fine di individuare anomalie, disfunzioni e prestazioni inattese; la possibilità di interrompere il funzionamento; ma l'aspetto a nostro avviso più interessante, perché riguarda il funzionamento in sé e non le sue anomalie, è che l'intervento e la sorveglianza umana presuppone/richiede di "*decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema*" (art. 14, comma 4, lettera d).

All'umano spetta l'ultima parola; l'umano con la sua azione costituisce il limite ultimo alla autonomia della macchina, che non è e non deve mai essere totale: anche in questo senso la persona è al centro.

Non è un tema di poco conto per la sicurezza del lavoro, perché impone di determinare a chi compete il potere (e il dovere!) di assicurare il requisito della sorveglianza umana; ci torneremo tra poco.

Prima però occorre citare l'ulteriore obbligo che l'AI ACT sancisce per assicurare la centralità della persona: tanto il fornitore del sistema di IA quanto il deployer (l'utilizzatore) devono garantire "**l'alfabetizzazione in materia di IA del loro personale nonché di qualsiasi persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto**". L'obbligo è sancito nell'art. 4 e non a caso è uno degli articoli dell'AI ACT che già si applica dal 2 febbraio 2025.

L'alfabetizzazione coinvolge la persona in una doppia prospettiva, illustrata nel Considerando (20): dal lato "passivo", cioè nei confronti di coloro sui quali si producono i risultati del sistema di IA (le "persone interessate", secondo l'AI ACT), l'alfabetizzazione deve fornire "*le conoscenze necessarie per comprendere in che modo le decisioni adottate con l'assistenza dell'IA incideranno su di esse*"; dal lato "attivo", nei confronti di coloro che dovranno intervenire nello sviluppo e poi nel funzionamento del sistema, l'alfabetizzazione deve fornire le "*nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA*".

Letto con la lente della sicurezza sul lavoro, il tema dell'alfabetizzazione si intreccia con il tema della formazione: formazione dei datori di lavoro e dei lavoratori, ma anche di qualsiasi altra persona coinvolta nel funzionamento o nell'utilizzo del sistema: già nell'AI ACT, dunque, prima ancora di

ricavarlo dal Decreto 81, troviamo indirettamente il richiamo a tutte le figure del sistema di sicurezza delle singole organizzazioni.

7.2.3.2 L'approccio basato sul rischio

La seconda risposta dell'AI ACT per garantire la tutela della persona umana rispetto all'intelligenza artificiale, all'autonomia ed all'adattabilità, è la scelta dell'approccio basato sul rischio.

L'IA, infatti, "contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività umane e sociali" e "può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale"; lo può fare perché l'uso dell'IA garantisce "un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili" (Considerando 4); ma può nel contempo, "a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali" (Considerando 5).

Per questo motivo, la scelta dell'AI ACT è quella di dettare regole che promuovano lo sviluppo, l'uso e l'adozione dell'IA, ma garantiscano nel contempo un elevato livello di protezione degli interessi pubblici quali la salute e la sicurezza e dei diritti fondamentali: il che avviene regolando immissione ed uso dei sistemi di IA in base al rischio che ne deriva per tali interessi e diritti.

Il rischio di cui parla l'AI ACT è quello intrinseco alla natura dei sistemi di IA, quello cioè legato alle caratteristiche che li definiscono come tali:⁵⁹ la conferma *a contrario* la si rinviene, ad esempio, nell'art. 6 comma 3, ai sensi del quale un sistema di IA, che pure rientri nella classificazione dei sistemi ad alto rischio, può non essere considerato tale quando non presenta un rischio significativo "anche nel senso di non influenzare materialmente il risultato del processo decisionale".⁶⁰ L'influenza del sistema di IA sul processo decisionale e sull'output, ovvero la mancanza di intervento umano nella produzione dell'output, è l'elemento che determina il rischio.

L'ulteriore osservazione da fare è che si tratta di un rischio nuovo e diverso, e questo vale anche rispetto ai rischi tradizionalmente considerati dalle norme che regolano la sicurezza del lavoro, come precisato dallo stesso AI ACT in riferimento alle normative armonizzate dell'Unione che regolano la materia;⁶¹ ne deriva la necessità di combinare l'approccio basato sul rischio dell'AI ACT con l'approccio basato sul rischio del Decreto 81 e, in generale, della normativa che regola la sicurezza sul lavoro.

Tanto precisato, rispetto ai rischi propri dei sistemi di IA il Regolamento europeo individua quattro diversi livelli di rischio: rischio inaccettabile e quindi pratiche vietate (Capo II); sistemi di IA ad alto rischio (Capo III); sistemi di IA soggetti a obblighi di trasparenza (Capo IV); sistemi di IA non soggetti a obbligazioni specifiche ma per i quali è incoraggiata l'elaborazione di codici di condotta per l'applicazione volontaria di regole (Capo X). I primi due livelli sono quelli più significativi ai nostri fini.

È un approccio cosiddetto top-down, diverso da quello bottom-up adottato ad esempio nel GDPR (Regolamento Generale sulla Protezione dei Dati) in cui il principio di *accountability* rimette al

⁵⁹ Si veda ad esempio il Considerando 47: "...è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati" (la sottolineatura è nostra).

⁶⁰ Perché esegue un compito procedurale limitato, o serve solo per migliorare un'attività umana già completata, o per analizzare schemi decisionali precedenti e non per sostituire o influenzare valutazioni umane già completate, o ancora per compiere compiti soltanto preparatori.

⁶¹ "I pericoli dei sistemi di IA disciplinati dai requisiti del presente regolamento riguardano aspetti diversi rispetto alla vigente normativa di armonizzazione dell'Unione": Considerando 64.

destinatario della normativa la identificazione del rischio, la sua valutazione e l'adozione delle misure conseguenti a fini di compliance.

Nell'AI ACT invece è il legislatore stesso che detta le regole di classificazione per i sistemi di IA.

Nel Capo II sono elencate le **pratiche di IA vietate** (manipolazione subliminale, sfruttamento delle vulnerabilità, social scoring, profilazione per la prevenzione di reati, scraping di immagini facciali, inferimento di emozioni di una persona fisica, categorizzazione biometrica indiscriminata, identificazione biometrica in tempo reale per attività di contrasto). Per quanto riguarda le pratiche configurabili anche nel mondo del lavoro e rispetto alla sicurezza del lavoro, un breve cenno può riservarsi qui ai sistemi di riconoscimento delle emozioni, finalizzati *“a identificare o inferire emozioni o intenzioni di persone fisiche, sulla base dei loro dati biometrici”*: il Considerando 18 precisa che *“la nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento”* mentre *“non comprende stati fisici, quali dolore o affaticamento, compresi, ad esempio, ai sistemi utilizzati per rilevare lo stato di affaticamento dei piloti o dei conducenti professionisti al fine di prevenire gli incidenti”*. Ai sensi dell'art. 5 comma 1 lettera f), l'uso di tali sistemi costituisce pratica vietata *“nell'ambito del luogo di lavoro...tranne laddove l'uso del sistema di IA sia destinato ad essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza”*. Considerato che l'art. 5 sulle pratiche vietate (e sanzionate dall'art. 99) è già applicato dal 2 febbraio 2025, in anticipo rispetto alla decorrenza generale del Regolamento prevista dal 2 agosto 2026, e ciò *“per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile”*, la definizione dei confini del divieto di questa pratica – della quale sono già note applicazioni concrete nel mondo del lavoro anche e proprio a fini di prevenzione degli infortuni, ad esempio per rilevare stati di stanchezza dell'operatore – è un tema sul quale si renderà senz'altro necessario un dibattito approfondito. Rientrare o non rientrare nella fattispecie significa, infatti, liceità o illiceità dell'utilizzo del sistema di IA.

L'art. 6 classifica come **sistemi di IA ad alto rischio** quelli (comma 1 lettera a) che sono destinati ad essere utilizzati come componenti di sicurezza di un prodotto, o sono essi stessi un prodotto, disciplinato da una delle norme di armonizzazione elencate nell'allegato I, nonché quelli (comma 1 lettera b) che sono soggetti a valutazione di conformità da parte di terzi per l'immissione sul mercato ai sensi delle norme di armonizzazione dello stesso elenco.

Le normative di armonizzazione elencate nell'Allegato I sono ben note al mondo della sicurezza del lavoro: esse riguardano, tra l'altro, macchine, ascensori, apparecchi in atmosfere esplosive, attrezzature a pressione, DPI, dispositivi medici.

Per il Regolamento, dunque, le normative di armonizzazione sono un criterio per classificare i sistemi di IA come ad alto rischio: in sostanza, quando l'IA viene utilizzata in un contesto regolato dalle normative di armonizzazione, essa viene considerata ad alto rischio perché quel contesto è già considerato dalle norme UE come potenzialmente pericoloso per la salute e la tutela dei lavoratori.

Va però sottolineato che le normative di settore definiscono il confine, ma non dettano le regole per i sistemi di IA: questi comportano rischi diversi, e come tali vanno gestiti in maniera specifica e dedicata;⁶² al fornitore tuttavia è concesso di integrare le informazioni e documentazioni richieste dall'AI ACT nella documentazione e nelle procedure già esistenti richieste dalla vigente normativa di

⁶² “Ad esempio, le macchine o i dispositivi medici in cui è integrato un sistema di IA potrebbero presentare rischi non affrontati dai requisiti essenziali di sicurezza e di tutela della salute stabiliti nella pertinente normativa armonizzata dell'Unione, in quanto tale normativa settoriale non affronta i rischi specifici dei sistemi di IA”: Considerando 64 (la sottolineatura è nostra).

armonizzazione dell'Unione, allo scopo di garantire la coerenza ed evitare oneri amministrativi e costi inutili (Considerando 64).

Una seconda categoria di sistemi ad alto rischio include (art. 6 comma 2) quelli dell'Allegato III, il quale individua alcuni settori e poi classifica ad alto rischio taluni sistemi in questi settori. Per quanto qui interessa, sono ad alto rischio, nel settore della *"Occupazione, gestione dei lavoratori e accesso al lavoratore autonomo"*, i sistemi di IA impiegati per l'assunzione o la selezione, per adottare decisioni sulle condizioni dei rapporti di lavoro, per assegnare compiti, per monitorare e valutare prestazioni e comportamenti.

In sostanza, se guardiamo agli ambiti dell'Allegato I, qualsiasi ragionamento che riguardi la sicurezza del lavoro in tema di macchine, attrezzature, DPI (e tutti gli altri ambiti dell'Allegato I) deve muovere dal presupposto che, se intervengono sistemi di IA, essi sono da considerare sicuramente sistemi ad alto rischio; sicchè le regole consolidate della sicurezza del lavoro dovranno necessariamente intrecciarsi con le regole dell'AI ACT su tali sistemi.

Ma non è meno rilevante, per la sicurezza del lavoro, la seconda tipologia di sistemi di IA, quelli dell'Allegato III: invero, le attività elencate nell'Allegato III (assunzione, adozione di decisioni sulle condizioni di lavoro, assegnazione di compiti, monitoraggio), che spesso vengono menzionate per i danni significativi alla persona in una prospettiva strettamente giuslavoristica (discriminazioni in fase di selezione, violazione del diritto alla protezione dei dati, pratiche lesive della dignità del lavoro), presuppongono anche adempimenti tipici della sicurezza ed igiene del lavoro, che vanno dalla valutazione dei rischi alla formazione, alla sorveglianza sanitaria, alla vigilanza. Si pensi, per fare un esempio, all'utilizzo di un sistema di IA per esprimere un giudizio di idoneità in fase di visita preassuntiva, o per la organizzazione delle squadre e l'assegnazione dei compiti ai lavoratori.

In conclusione, quando consideriamo le implicazioni che l'introduzione di un sistema di IA all'interno di una organizzazione comporta rispetto alla sicurezza del lavoro, dobbiamo partire dal presupposto che la prima base normativa è rappresentata dalle regole dell'AI ACT sui sistemi ad alto rischio; da questa base normativa deve partire il datore di lavoro di quella organizzazione, in quanto utilizzatore (deployer) del sistema di IA, se non addirittura come fornitore.

7.2.3.3 Sistemi di IA ad alto rischio: gli obblighi del fornitore

Il primo e principale destinatario degli obblighi sanciti nell'AI ACT è il fornitore, cioè il soggetto che sviluppa o fa sviluppare un sistema di IA e immette tale sistema sul mercato o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito (art. 1 n. 3).

Questi deve innanzitutto garantire che il sistema risponda a stringenti **requisiti di sicurezza**, che includono (Capo II, Sezione 2): la istituzione di un sistema di gestione dei rischi, che assicuri la identificazione e analisi dei rischi connessi all'uso del sistema conforme alle sue finalità e istruzioni nonchè la stima e valutazione dei rischi per l'uso improprio ragionevolmente prevedibile, l'adozione di misure per la eliminazione o la riduzione dei rischi, le misure di controllo, la fornitura delle informazioni, ove opportuno la formazione dei deployer (art. 9); adeguate governance e gestione dei dati di addestramento, convalida e prova dei sistemi (art. 10); redazione della documentazione tecnica (art. 11); registrazione automatica degli eventi (log) e conservazione delle registrazioni (art. 12); trasparenza e istruzioni per l'uso (art. 13); sorveglianza umana (art. 14); accuratezza, robustezza e cbersicurezza dei sistemi (art. 15).

Gli obblighi fanno capo al fornitore del sistema (artt. 16-21) ma coinvolgono poi con gradi diversi tutta la catena del valore: rappresentanti autorizzati (art. 22), importatori (art. 23), distributori (art. 24).

Nella prospettiva della sicurezza del lavoro, è interessante osservare che gli obblighi di gestione dei rischi da parte del fornitore sono modulati sul fatto che il sistema è destinato ad essere utilizzato dai deployer: sono emblematici, in questo senso, gli obblighi di garantire una trasparenza del sistema di IA *“tale da consentire ai deployer di interpretare l’output del sistema e utilizzarlo adeguatamente”* (art. 13) e di individuare misure di sorveglianza umana sul sistema *“adatte ad essere attuate dal deployer”* (art. 14).

Tali obblighi assumono altresì una connotazione peculiare perché riguardano i rischi di un sistema che, per definizione, è autonomo nonché adattabile e quindi capace di auto-apprendere e modificarsi.

In questo senso è particolarmente interessante richiamare l’ulteriore obbligo del fornitore di istituire un sistema di gestione della qualità (art. 17) per *“certificare”* la conformità del sistema ai requisiti normativi, che include anche *“la conformità...alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio”* (comma 1 lettera a); altrettanto rilevante, anche nella prospettiva della sicurezza del lavoro, sono gli obblighi del fornitore di conservare per dieci anni la documentazione tecnica (art. 18), di conservare i log generati automaticamente dai sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo (art. 19), di adottare immediatamente misure correttive, fino al ritiro, disabilitazione o richiamo, quando ritengono o hanno motivo di ritenere che un sistema non sia conforme al presente regolamento (art. 20).

Strettamente connessa con tali obblighi è la previsione nel Capo IX dell’AI ACT (artt. 72 e ss.) di un sistema di monitoraggio *“successivo all’immissione sul mercato che sia proporzionato alla natura delle tecnologie di IA e ai rischi del sistema di IA ad alto rischio”*, che deve consentire al fornitore *“di valutare la costante conformità dei sistemi di IA ai requisiti”* di sicurezza.

Accanto all’uso proprio (della macchina, dell’attrezzatura, del DPI) e all’uso improprio ragionevolmente prevedibile, si aggiunge ora l’uso nuovo e diverso *“deciso”* autonomamente dal sistema.

Per fare fronte alle conseguenze di questo *“divenire”* dei sistemi di IA ad alto rischio *“che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio”*, l’AI ACT impone ai fornitori di predeterminare fin dal momento iniziale della valutazione della conformità le modifiche apportate al sistema (art. 43 comma 4), indicandole nella documentazione tecnica di cui all’art. 11 (Allegato IV, punto 2, lettera f). In quanto predeterminate, tali modifiche non sono da considerare modifiche sostanziali, e quindi non impongono una nuova valutazione di conformità del sistema (art. 43 comma 3).

Questo significa che eventuali modifiche non predeterminate, ma che sono possibili, impongono di rinnovare la valutazione di conformità, implicitamente riconoscendosi la possibilità che un sistema di IA presente sul mercato possa *“diventare”* non conforme ai requisiti di sicurezza.

Sullo sfondo di questa analisi degli obblighi del fornitore, va sempre ricordato che il Regolamento europeo, avendo l’esigenza di non bloccare l’innovazione e la diffusione dei sistemi di IA, prescrive che le misure di gestione dei rischi siano *“tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili”* (art. 9 comma 5) e che, posto che un sistema di IA ad alto rischio è conforme a normativa anche in presenza di un rischio purché accettabile, le informazioni obbligatoriamente contenute nella documentazione tecnica che accompagna il sistema di IA devono riguardare anche *“i prevedibili risultati indesiderati e fonti di rischio per la salute, la sicurezza e i diritti fondamentali”* (Allegato IV, punto 3).

Ricordato anche che la sorveglianza umana è vera e propria misura di prevenzione/riduzione al minimo dei rischi, *“in particolare qualora tali rischi persistano nonostante l’applicazione di altri requisiti di cui alla presente sezione”* (art. 14 comma 2), ne consegue che il fornitore può immettere sul mercato un sistema di IA che non esclude la presenza di un rischio per la salute, per la sicurezza e per i diritti fondamentali della persona.

È una constatazione rilevante, in un contesto nazionale in cui non raramente si rinvencono affermazioni che sembrano sottintendere il “rischio zero” come paradigma ordinario.

L’adozione di un sistema di IA da parte di una organizzazione (una macchina “intelligente”, uno SMART DPI, un sistema di manutenzione predittiva, di gestione degli accessi a spazi confinati, ecc.), dunque, pone all’organizzazione il problema di gestire il rischio residuo che il fornitore ha stimato come accettabile (e per il quale il fornitore deve mettere a disposizione le informazioni e tutti gli strumenti necessari alla gestione).

Questo conduce ad esaminare quali sono gli obblighi dell’utilizzatore di un sistema di IA.

7.2.3.4 Sistemi di IA ad alto rischio: gli obblighi dei deployer. Il datore di lavoro tra AI ACT e Decreto 81

Il ruolo del fornitore è destinato a incrociarsi necessariamente con quello del deployer (art. 26).

Deployer è il soggetto *“che utilizza un sistema di IA sotto la propria autorità.”*⁶³

È una figura fondamentale, perché governa il contesto in cui il sistema di IA viene utilizzato, il personale che ne farà uso, ed ancora le persone interessate che subiranno gli effetti degli output del sistema.

Il riferimento all’autorità che il deployer esercita nel contesto di funzionamento del sistema di IA spiega le ragioni per le quali l’AI ACT affida appunto al deployer l’obbligo, partendo da quanto fatto dal fornitore, di “completare” la gestione del rischio dell’IA modellandola in funzione del contesto: vale a dire, appunto, dell’organizzazione del deployer.

Così, al deployer incombono gli obblighi (art. 26) di adottare idonee misure tecniche e organizzative che garantiscano un uso *“conformemente alle istruzioni per l’uso”* del fornitore (comma 1) e di assicurare la sorveglianza umana richiesta e resa possibile dal fornitore, affidandola *“a persone fisiche che dispongono della competenza, della formazione e dell’autorità necessarie nonché del sostegno necessario”* (comma 2).

Se poi “esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi” (comma 4), cosa che deve avvenire naturalmente in coerenza con la finalità prevista del sistema di IA.

Ed ancora, ad integrazione ed in funzione dell’obbligo del fornitore di assicurare nel tempo la conformità del sistema di IA, il deployer deve monitorare il funzionamento del sistema, se del caso informando il fornitore ed eventualmente sospendendo l’uso del sistema (comma 5); così come i deployer devono conservare i log generati automaticamente dal sistema *“nella misura in cui tali log sono sotto il loro controllo”* (comma 6).

Anche il deployer, in sostanza, si deve occupare dei rischi intrinseci al sistema di IA, nella misura in cui tali rischi sono correlati al contesto governato dal deployer.

⁶³ È escluso il caso in cui il sistema di IA sia utilizzato nel corso di un’attività personale non professionale.

A tale proposito, nella prospettiva della sicurezza del lavoro appare particolarmente significativo il richiamo della definizione di deployer come soggetto che utilizza il sistema di IA *“sotto la propria autorità”*.

È una formula che a nostro avviso presenta un doppio significato.

Questa *“autorità”* è innanzitutto l'autorità che il deployer esercita sul contesto di utilizzo del sistema: il deployer ha obblighi rispetto al sistema di IA perché governa il contesto in cui il sistema è introdotto. Se il contesto è l'ambiente di lavoro, dove a governare il contesto è il datore di lavoro, allora la nozione di autorità si ricollega a quella di *“potere decisionale e di spesa”*; ne deriva che, applicando i principi della sicurezza del lavoro, il datore di lavoro appare il naturale destinatario degli obblighi; dopodiché l'attuazione materiale degli adempimenti previsti dall'AI ACT si dipana secondo le regole proprie dell'organizzazione che utilizza il sistema, coinvolgendo, a partire dal datore di lavoro, tutte le figure del sistema di sicurezza aziendale. La definizione dei ruoli di ciascuno sarà certamente uno dei temi che dovranno essere affrontati nell'immediato futuro.

Ma l'autorità del deployer va intesa anche come autorità rispetto al sistema di IA ed al suo funzionamento, e in questo senso la nozione funziona come un limite. Il sistema di IA è sviluppato da altri (il fornitore) e il deployer è in grado soltanto in parte di intervenire sul suo funzionamento: ciò dipende sia da quanto il fornitore lo abbia davvero messo in condizione di gestire il sistema di IA ed il rischio accettabile che residua, sia da elementi tecnici del sistema: non a caso, ad esempio, l'AI ACT prevede per il deployer l'obbligo di gestire i dati di input solo se su di essi esercita il controllo, o ancora l'obbligo di conservare i log generati automaticamente solo nella misura in cui sono sotto il suo controllo⁶⁴.

Certo è che un sistema di IA ad alto rischio è esso stesso, per l'organizzazione in cui viene introdotto, un fattore di rischio; questo rischio deve essere gestito applicando le regole che gli sono proprie, cioè gli obblighi del deployer contenuti nell'AI ACT; ma una volta fatto questo, l'AI ACT specifica che restano *“impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale”* (art. 26 comma 3).

Per il deployer datore di lavoro, soggetto agli obblighi previsti dal diritto dell'Unione e nazionale per garantire la sicurezza e salute nei luoghi di lavoro, esiste dunque un ulteriore livello di gestione del rischio, oltre a quello dell'AI ACT: quello dettato dalle norme del sistema di sicurezza e salute nei luoghi di lavoro.

Volendo semplificare, potremmo dire che il fornitore deve effettuare la valutazione dei rischi *del sistema di IA*; il deployer deve effettuare la valutazione dei rischi *dell'ambiente di lavoro in cui l'IA sarà inserito*.

Questa valutazione dei rischi presuppone quella del fornitore, la assorbe e la fa propria, la completa per quanto di propria competenza; ma non si esaurisce in essa; ai rischi intrinseci del sistema di IA si aggiungono i rischi per la salute e la sicurezza riconnessi al suo utilizzo in un dato contesto.

Questi rischi sono gestiti secondo le altre norme del diritto nazionale applicabili alle singole fattispecie, e nella sicurezza del lavoro comportano che il deployer deve ad esempio assolvere tutti gli adempimenti, nessuno escluso, che il Decreto 81 prevede quando ci sia una modifica

⁶⁴ Va osservato, al riguardo, che il deployer è considerato fornitore di un sistema di IA ad alto rischio ed è soggetto ai relativi obblighi se appone il proprio nome o marchio su un sistema già immesso sul mercato o messo in servizio, se lo modifica, se modifica la finalità di un sistema non ad alto rischio rendendolo tale (art. 25).

dell'ambiente di lavoro: valutazione dei rischi, innanzitutto, ma anche formazione ed informazione, sorveglianza sanitaria, informazione e formazione dei lavoratori, e così via⁶⁵.

L'operazione necessaria, ma non banale, è dunque di disegnare una gestione di un sistema di IA che soddisfi tanto le previsioni dell'AI ACT quanto quelle del Decreto 81.

Ciò richiede consapevolezza profonda della diversità dei due contesti (ad esempio, la sorveglianza umana su un sistema di IA non va confusa con la vigilanza del Decreto 81), ma anche risposte alle criticità (ad esempio: chi sorveglia il sistema di IA deve essere necessariamente un preposto, quando il sistema abbia specifica finalità di sicurezza o sia in grado anche solo indirettamente di influire su di essa? E ancora: l'IA è un rischio "in sé"? Se lo è va assoggettato a sorveglianza sanitaria come rischio non normato ma valutato, o potrebbe darsi un sistema di IA che non determina sorveglianza sanitaria perché, per quanto ad alto rischio quanto al suo funzionamento interno, non genera nessun rischio suscettibile di sorveglianza sanitaria?). E ancora: l'IA è un rischio "in sé"? Se lo è va assoggettato a sorveglianza sanitaria come rischio non normato ma valutato, o potrebbe darsi un sistema di IA che non determina sorveglianza sanitaria perché ecc. ecc.

In ogni caso, questa operazione di integrazione dei due corpi normativi a nostro avviso richiede soprattutto il preliminare soddisfacimento dell'esigenza di alfabetizzazione in materia di IA, senza la quale qualsiasi gestione dei rischi di un sistema di IA rimarrebbe una vana ambizione o una amara finzione.

7.2.4 Autonomia e adattabilità: quale governo dell'area di rischio?

Il tema di fondo, quando si parla di sistemi di IA, è quello della loro autonomia e della loro adattabilità. La capacità di produrre output senza che le regole siano scritte esclusivamente dall'essere umano, di auto-apprendere sulla base di un'esperienza che è solo del sistema, di sviluppare nuovi input che non provengono dall'essere umano e di modificare i propri criteri di elaborazione degli output, sono tutti elementi che pongono l'essere umano al di fuori del percorso che conduce al risultato.

L'essere umano non ha il governo totale del processo di produzione del risultato; quanto maggiore è l'autonomia, tanto minore è il governo.

L'essere umano non ha la conoscenza totale del processo di produzione del risultato; quanto maggiore è l'adattabilità, tanto minore è la conoscenza.

Nel sistema normativo e giurisprudenziale della sicurezza del lavoro, imputabilità e prevedibilità sono principi fondanti. In forza di tali principi, vige la regola del governo dell'area di rischio; il sistema si basa sull'esercizio dei poteri che sono propri di chi governa quell'area di rischio; chi governa l'area di rischio è chiamato a prevenire l'evento tramite l'esercizio dei propri poteri rispetto a ciò che è prevedibile.

Quello che distingue i sistemi IA, invece, è proprio il fatto che, operando il sistema in autonomia, nonché essendo il sistema adattabile in forza di una capacità di autoapprendimento, si affievolisce il *potere* di governo dell'area di rischio, così come si affievolisce la capacità di *prevedere* i risultati.

La valutazione dei rischi, connessi all'uso di un sistema di IA, potrebbe (dovrebbe?) invero concludersi necessariamente con il riconoscimento, da parte (prima del fornitore e poi) del

⁶⁵ Un aspetto particolare riguarda RLS e lavoratori, anche perché espressamente nominati nell'AI ACT (art. 26 comma 7): "i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio."

deployer/datore di lavoro, che esiste un ambito nel quale gli output non sono prevedibili né governabili perché esclusivamente frutto del sistema e in nessun modo dell'intervento umano.

Non è una ipotesi che l'AI ACT esclude, anzi: la valutazione di accettabilità del rischio residuo di un sistema di IA dotato di autonomia e adattabilità implica che la soluzione tecnologica adottata è considerata adeguata a tutelare la persona e i diritti rispetto ad un danno significativo; e se il sistema di IA è immesso sul mercato, significa che per definizione il rischio è accettabile.

Una prima implicazione di questo assetto è la posizione certamente critica del *deployer*, il quale, pur essendo totalmente estraneo al processo di sviluppo e di immissione in commercio del sistema di IA (nonché, ragionevolmente, ampiamente estraneo anche alle implicazioni tecnologiche connesse al suo funzionamento ivi compreso l'auto-apprendimento), rimarrebbe il primo e principale destinatario delle conseguenze dell'utilizzo di quel sistema di IA (tanto più, quanto più il fornitore avrà "spinto" sugli obblighi di intervento e sorveglianza umana del *deployer* per valutare accettabile il rischio del proprio sistema di IA).

Certo, il datore di lavoro potrà ben decidere di non introdurre il sistema di IA nella sua organizzazione: ma potrebbe invece decidere che gli effetti benefici che derivano dal sistema di intelligenza artificiale sono tali da rendere accettabile il rischio, ad esempio perché la valutazione dei rischi mostra che ci sarebbe un aumento del livello di prevenzione e protezione (impossibilità di accesso a spazi confinati in mancanza dei DPI o da parte di un lavoratore solitario) superiore al rischio ineliminabile di eventi negativi non prevedibili, (una autonoma rielaborazione algoritmica del sistema che ammette un accesso allo spazio confinato ritenendolo un output coerente con un obiettivo implicito). In questa fattispecie, che allo stato sembrerebbe dover essere la regola in ogni caso di introduzione di un sistema di IA autonoma e adattabile, dovrebbe evidentemente porsi un problema di ridefinizione della disciplina della responsabilità.

Si pone, in ultima analisi, l'esigenza di domandarci se e quanto una responsabilità (del datore di lavoro e/o di altre figure del sistema di sicurezza aziendale) per gli output di un sistema di IA siffatto sia compatibile con i presupposti essenziali del sistema normativo di sicurezza e salute del lavoro: cioè, con il concetto di area di rischio e con il concetto di governo dell'area di rischio.

La responsabilità di un evento potrà imputarsi al datore di lavoro che adotta un sistema di IA, al produttore che glielo ha venduto, al progettista che lo ha progettato; o ancora ad una delle molteplici figure di garanzia dell'organizzazione, ciascuna in funzione dei propri poteri. Il criterio sarà quello consueto: la individuazione, in capo al soggetto, del potere di governare l'area di rischio che gli è propria, e quindi di porre in essere le azioni necessarie al perseguimento dell'obiettivo di tutela del bene giuridico costituito dalla vita e dalla salute dei lavoratori.

Come è stato detto, però, ciò che caratterizza l'IA è il fatto di essere passati da un procedimento deduttivo che fornisce la certezza del risultato, ad un procedimento induttivo in cui siamo sorpresi del risultato; e questo impone la esigenza di approfondire la riflessione sui paradigmi che regolano la materia della sicurezza del lavoro.

Lo scopo, si badi, non è e non può essere quello di perseguire una finalità di esonero di responsabilità giustificata dall'autonomia della tecnologia; anzi ed al contrario, si tratta di verificare se si renda necessario costruire un diverso paradigma che tenga conto che la "macchina" può arrivare dove l'essere umano *non può* arrivare; dove l'essere umano *non sa* arrivare, e soprattutto dove l'essere umano non sa *come* arrivare; anzi, ed è anche questo il punto, non sa ricostruire neppure a posteriori *come ci si è arrivati*.

Intimamente connesso è il tema della valutazione del rischio.

Se guardiamo al tema dei rischi occulti della macchina, fino ad oggi la giurisprudenza ha affermato più spesso la responsabilità del datore di lavoro, financo nel caso in cui si fosse avvalso di consulenti della più elevata specializzazione, piuttosto che il suo esonero per aver posto in essere tutta la diligenza ed esercitato tutto il potere di cui disponeva. La nuova domanda che occorre porsi è se e come imputare al datore di lavoro un evento riconducibile non alla omessa o incompleta valutazione di un rischio, quanto piuttosto alla non valutabilità di un rischio: non perché non adeguatamente ricercato, ma perché non conosciuto e non conoscibile dall'essere umano; o addirittura perché non ancora esistente.

In realtà, alla fine, occorre domandarsi se siamo disposti a riconoscere che l'utilizzo di un sistema di IA non solo configura esso stesso un fattore di rischio, ma addirittura implica un rischio non valutabile, perché si tratta del rischio che il sistema produca un output impreveduto e imprevedibile per l'umano, e perché questa è la natura e la stessa essenza dell'intelligenza artificiale.

Se siamo disposti a riconoscerlo, si renderà inevitabile la ricerca di nuove chiavi di lettura.

7.2.5 AI ACT, intelligenza artificiale e art. 2087 c.c.

Una ulteriore questione che si pone riguarda il rapporto tra IA e art. 2087 c.c.

Sarebbe davvero illusorio, oltre che profondamente sbagliato, affermare in assoluto che un sistema di IA rappresenta la massima sicurezza tecnologicamente fattibile; dobbiamo ammettere che potrebbe non esserlo, e che quindi non adottarlo non implica necessariamente una violazione dell'art. 2087 c.c.

Ci sembra una prima conclusione importante sull'argomento, non fosse altro perché pone il datore di lavoro di fronte all'evidente necessità di decidere se adottare o non adottare un sistema di IA.

C'è però un tema più di fondo, che vogliamo evidenziare: è legato al fatto, che se il *deployer* decide di adottare il sistema, ne accetta il quoziente di rischio intrinsecamente connesso all'autonomia e all'adattabilità del sistema.

Ma come dobbiamo leggere un sistema di IA che contiene una quota di imprevedibilità "assoluta", rispetto all'art. 2087 c.c. ed al ruolo che ha assunto nel sistema di sicurezza e salute nei luoghi di lavoro? Come sancito dalla giurisprudenza, la norma ha un ruolo di chiusura del sistema di prevenzione perché consente di tenere conto della concreta realtà aziendale e della maggiore o minore possibilità di venire a conoscenza e di indagare sull'esistenza di fattori di rischio in un determinato momento storico; non contiene l'affermazione di un obbligo assoluto del datore di lavoro di rispettare ogni cautela possibile al fine di un "rischio zero"; occorre la violazione di un obbligo di comportamento, che se non è imposto dalla legge può però essere ricavabile "dalle conoscenze sperimentali o tecniche in relazione al lavoro svolto". Entrano qui in gioco la particolarità del lavoro (complesso di rischi e pericoli che caratterizzano la specifica attività lavorativa); l'esperienza (conoscenza di rischi e pericoli acquisita nello svolgimento della specifica attività lavorativa); la tecnica (progresso scientifico e tecnologico attinente a misure di tutela su cui il datore di lavoro deve essere aggiornato).

La questione è, se e quanto l'utilizzo di un sistema di IA consenta l'applicazione di questi parametri, che sono ad un tempo il presupposto ed il limite della responsabilità del datore di lavoro: se sia possibile affermare che il datore di lavoro, che utilizza un sistema di IA, ha consapevolezza piena dell'esatto perimetro dei rischi della propria specifica attività lavorativa (particolarità del lavoro), dei rischi e dei pericoli frutto dell'esperienza (esperienza), delle misure tecniche da attuare (tecnica); se non ci sia invece una quota di non conosciuto e non conoscibile in un sistema di IA che rende più

indefinita la concreta realtà aziendale e meno afferrabile la esistenza dei fattori di rischio nonché degli accorgimenti per fronteggiarli.

Durante l'esperienza pandemica, la natura sconosciuta del rischio da affrontare ha reso inevitabile una mitigazione della portata dell'art. 2087 c.c. come chiusura del sistema di sicurezza, tramite la definizione di linee guida la cui osservanza scriminava il soggetto obbligato. Ci dobbiamo domandare se quell'esperienza possa essere replicata, e se nel farlo sia necessario concentrare l'attenzione su una attività determinante quale è il monitoraggio del funzionamento del sistema di IA.

Per altro verso, approfondire questi temi costringe ad interrogarsi sul significato del ruolo della persona umana, quando un'organizzazione utilizza il sistema di IA.

Come si è visto, la supervisione umana è ritenuta l'elemento imprescindibile perché l'IA diventi parte del mondo in cui viviamo.

Se però supervisione umana significa che spetta all'essere umano l'ultima parola, e che il risultato fornito dal sistema di IA non può e non deve essere messo in condizione di modificare l'ambiente esterno se prima non è stato verificato e validato dall'essere umano, si pongono due questioni.

La prima questione è di carattere assolutamente pratico, potremmo dire procedimentale, e riguarda la disciplina dell'attribuzione del ruolo nonché dei tempi e dei modi di questa supervisione: altro è chiedere al medico di valutare un referto e di decidere se l'output fornito dal sistema di IA è condivisibile o se va invece modificato, altro è immaginare una verifica dell'output di un sistema di IA la cui funzione è quella di autorizzare o non autorizzare un lavoratore ad accedere ad una determinata area di lavoro o di condizionare quell'accesso alla disponibilità o meno di un determinato DPI; o ancora di consentire ad un lavoratore di eseguire o non eseguire una certa specifica attività nell'ambito di una lavorazione.

La seconda questione è legata ancora una volta ai temi della responsabilità per la decisione presa e per l'azione adottata. La persona cui compete la sorveglianza verrebbe chiamata a decidere non di confermare l'output del sistema di IA (così validando, con il suo personalissimo giudizio, il dato probabilistico), bensì di contraddire l'output del sistema di IA. In un sistema normativo che valuta la responsabilità della persona agente attraverso il paradigma della più alta probabilità logica e del giudizio controfattuale, il soggetto agente si troverebbe costretto a dimostrare, in caso di evento infortunistico conseguito alla sua valutazione personale diversa da quella della macchina, che l'evento si sarebbe verificato comunque anche aderendo alla indicazione, proveniente dall'IA, di una condotta di segno diverso o addirittura contrario.

7.2.6 Conclusioni

La portata dirompente del fenomeno che va sotto il nome di Intelligenza Artificiale, unita alla tempestosa rapidità con cui si manifesta, stanno mettendo in crisi gli approcci, anche normativi, fino ad oggi utilizzati per gestire l'innovazione.

Per quanto riguarda il diritto, e nello specifico la sicurezza e salute nei luoghi di lavoro, molte sono le domande ancora senza risposta; anzi, molte sono le domande che ancora ci dobbiamo porre.

La questione è se l'ingresso dell'IA nei luoghi di lavoro avverrà (sta già avvenendo?) in assenza di un contesto normativo appropriato, o se invece la costruzione di nuovi paradigmi diventerà fin da subito tema di discussione, così da trovare in tempi rapidi le soluzioni più adatte a garantire, ancora una volta, la tutela della persona come centro di un sistema dove sono ben definiti ruoli e funzioni di ciascuno.

7.3 Aspetti normativi dell'intelligenza artificiale in campo lavorativo

Mauro Iori

Fisica Medica, AUSL di Reggio Emilia – IRCCS, Associazione Italiana di Fisica Medica (AIFM)

L'Intelligenza Artificiale (IA) sta radicalmente trasformando il mondo del lavoro, aprendo nuovi scenari e lasciando intravedere grandi opportunità, ma è fondamentale affrontarne le sfide adottando politiche adeguate a garantire una transizione equa e inclusiva dei lavoratori nell'impiego di tali dispositivi e sistemi. La relazione che si sta creando tra lavoro ed intelligenza artificiale è ogni giorno più forte, trovando sempre nuove applicazioni in un maggior numero di settori, trasformando processi e modificando mansioni anche in forza della crescita esponenziale della digitalizzazione (era digitale).

Si consideri, ad esempio, l'automazione di compiti ripetitivi ed usuranti (robotica che automatizza le attività di routine nella produzione e nella logistica), il supporto fornito nel servizio clienti (chat bot e assistenti virtuali che gestiscono h24 le interazioni), l'ottimizzazione dei processi aziendali (catene di montaggio automatizzate, smistamento pacchi, inserimento dati), la gestione delle risorse umane (supporto al reclutamento, selezione e formazione del personale), il potenziamento del marketing e delle vendite (campagne pubblicitarie personalizzate ed ottimizzazione delle strategie), il supporto di processi decisionali (analisi di grandi moli di dati per l'identificazione di tendenze e nuove opportunità del mercato) o il mondo della sanità (supporto allo screening, alla diagnostica, personalizzazione delle terapie, ecc.).

L'interrelazione tra lavoro ed intelligenza artificiale è ampia e diversificata, caratterizzata da forti aspetti positivi. Si pensi all'automazione di compiti ripetitivi, che ha liberato i lavoratori da mansioni



monotone consentendo loro di concentrarsi su attività più creative e a valore aggiunto, alla creazione di nuove opportunità di lavoro in settori come lo sviluppo di software, all'analisi dei dati e della gestione dei sistemi, migliorando le condizioni di sicurezza, riducendo i rischi e creando ambienti di lavoro più confortevoli e meno gravosi. Parimenti sta generando nuove sfide e/o criticità quali un'importante perdita di posti di lavoro, soprattutto nei settori con compiti altamente ripetitivi, sta esacerbando le disuguaglianze esistenti, con i lavoratori meno qualificati che rischiano di essere esclusi dal mercato del lavoro, rende sempre più urgente la necessità di riqualificare i lavoratori che dovranno acquisire nuove competenze per adattarsi ai cambiamenti del mercato del lavoro, cosa che richiederà investimenti significativi in formazione e riqualificazione, sollevando importanti questioni etiche, come la privacy dei lavoratori e la discriminazione algoritmica.

A conferma di quanto riportato si possono considerare le stime del *World Economic Forum*, vedi il testo integrale in appendice 8.1 (*The Future of Job Reports 2025 [survey based]*) nel quale viene indicata la creazione di 170 milioni di nuove attività lavorative (pari al 14% dell'attuale impiego globale), ma anche la scomparsa di 92 milioni di attività oggi presenti (pari all'8% dell'attuale impiego globale).

Considerando le problematiche IA nella loro interezza, facilmente si comprende l'importanza di investire nella formazione continua e nella riqualificazione dei lavoratori per prepararli al futuro del lavoro, che le aziende adottino un approccio responsabile all'IA, tenendo conto delle implicazioni

etiche e sociali, e che si instauri un dialogo aperto e costruttivo tra i governi, le aziende, i lavoratori e le istituzioni per affrontare le sfide e massimizzare i benefici legati all'IA.

Il Regolamento Europeo sull'intelligenza artificiale (EU IA ACT, 2024/1689A), il primo quadro giuridico globale in assoluto sull'IA a livello mondiale, entrato in vigore a febbraio 2025, cerca di rispondere a queste nuove esigenze e criticità, stabilendo norme armonizzate sull'intelligenza artificiale e ponendosi l'obiettivo di garantire che il suo utilizzo sia sicuro, etico e rispettoso dei diritti fondamentali delle persone, evitando discriminazioni e danni ai lavoratori, e promuovendo un'adozione responsabile dell'IA nel contesto lavorativo. Nello specifico, introduce vari concetti relativi alla:

- i. *protezione dei diritti dei lavoratori*: l'uso dell'IA nei luoghi di lavoro deve rispettare i diritti fondamentali dei lavoratori, come la privacy, la non discriminazione e la dignità. Ciò include il monitoraggio, la valutazione delle performance, e l'uso di algoritmi di assunzione e promozione.
- ii. *Prevenzione della discriminazione*: il regolamento cerca di evitare che gli algoritmi usati per selezionare o valutare i dipendenti siano discriminatori. L'IA deve essere progettata in modo da ridurre il rischio di bias (pregiudizi) che potrebbero portare a trattamenti ingiusti o disuguali nei confronti dei lavoratori, ad esempio, in base a genere, etnia, età o altre caratteristiche personali.
- iii. *Trasparenza e spiegabilità*: le decisioni prese attraverso sistemi di IA devono essere trasparenti e comprensibili. I lavoratori devono poter comprendere come e perché un algoritmo ha preso determinate decisioni, soprattutto quando queste decisioni influenzano la loro carriera, come nel caso di assunzioni, promozioni o licenziamenti.
- iv. *Sicurezza e affidabilità dell'IA*: il regolamento stabilisce norme rigorose per la sicurezza
- v. degli algoritmi e dei sistemi di IA. L'intelligenza artificiale utilizzata in ambito lavorativo deve essere sicura e affidabile, evitando che errori nel sistema possano danneggiare i lavoratori o compromettere la qualità del lavoro.
- vi. *Responsabilità in caso di danni*: in caso di danni causati da un sistema di IA, il regolamento stabilisce la responsabilità degli utilizzatori o dei fornitori del sistema. Ciò significa che le aziende devono assumersi la responsabilità per gli effetti negativi che l'uso dell'IA potrebbe avere sui lavoratori.
- vii. *Promozione di un impiego etico dell'IA*: le aziende devono utilizzare l'IA in modo etico, evitando l'automazione di compiti che potrebbero mettere a rischio il benessere dei lavoratori o ridurre eccessivamente le opportunità di lavoro. In alcuni settori, potrebbe essere necessaria una regolamentazione aggiuntiva per evitare che l'IA riduca la qualità del lavoro o crei disparità nel mercato del lavoro.
- viii. *Monitoraggio e regolamentazione delle applicazioni ad alto rischio*: avendo suddiviso i sistemi di IA in quattro categorie legate al rischio che presentano per la sicurezza, i diritti e le libertà fondamentali delle persone: *rischio minimo* [sistemi che non presentano rischi significativi, come applicazioni di IA nei videogiochi o negli assistenti virtuali], *rischio limitato* [sistemi che presentano un rischio moderato, come i chatbot e gli assistenti vocali], *rischio elevato*: sistemi che potrebbero comportare rischi significativi, come la IA usata in sanità, nei trasporti, nelle forze dell'ordine, nella giustizia e nelle decisioni di credito], *rischio inaccettabile* [sistemi di IA che sono vietati, come quelli che manipolano il comportamento umano, ad esempio le applicazioni di sorveglianza di massa e la social scoring], il regolamento pone particolare attenzione alle applicazioni di IA ad alto rischio.

Queste applicazioni devono essere monitorate e conformarsi a standard elevati di sicurezza, trasparenza e protezione dei diritti dei lavoratori.

In Italia le normative sull'intelligenza artificiale sono in evoluzione ma, in quanto Stato membro dell'Unione Europea, l'Italia ha adottato l'EU IA ACT come anche il Regolamento Generale sulla

Protezione dei Dati (GDPR), che regola la raccolta, l'elaborazione e l'uso dei dati personali, anche nell'ambito degli strumenti di IA. Sono state, inoltre, emanate alcune leggi sulla sicurezza informatica nell'uso dell'IA nelle tecnologie che coinvolgono dati sensibili e infrastrutture critiche, ed è stata lanciata una strategia nazionale per l'IA con l'obiettivo di favorirne l'adozione in ambito pubblico e privato.

Tali norme hanno inteso promuovere l'innovazione attraverso la ricerca e lo sviluppo di tecnologie avanzate, garantendo l'etica, la trasparenza e la protezione dei diritti umani nelle applicazioni IA, rivolgendo un'attenzione particolare alla formazione di competenze sull'IA nella forza lavoro. Il raggiungimento di questi obiettivi vede il forte coinvolgimento dell'Agenzia Italiana per l'Intelligenza Artificiale (AgID), la quale dovrà garantire la realizzazione degli obiettivi dell'Agenda digitale italiana, IA compresa. Vedi in appendice il documento integrale. 8.2.

L'AgID è l'agenzia tecnica della Presidenza del Consiglio che garantisce la realizzazione degli obiettivi dell'Agenda digitale italiana coordinando tutte le Amministrazioni del Paese, contribuendo anche alla diffusione delle tecnologie dell'informazione e della comunicazione, e promuovendo le competenze digitali e la loro diffusione, in collaborazione con le istituzioni, gli organismi internazionali, nazionali e locali.

Il Ministero del Lavoro e delle Politiche Sociali ha avviato la stesura delle **“Linee Guida per l'Implementazione dell'Intelligenza Artificiale (IA) nel Mondo del Lavoro”**: un documento innovativo pensato per aiutare imprese, lavoratori, enti di formazione e intermediari a sfruttare appieno le potenzialità dell'IA, in modo etico, responsabile e centrato sulla persona, che sarà oggetto di dialogo anche con le parti sociali. L'obiettivo è favorire produttività, efficienza, benessere e sicurezza in ogni ambiente di lavoro, nel rispetto della dignità individuale e collettiva.

In appendice viene proposta la versione integrale delle “Linee guida sull'IA nel mondo del lavoro” nella versione iniziale 8.3. Su tali Linee guida il Ministero del lavoro ha promosso una consultazione pubblica ed in appendice viene proposto il report finale.⁶⁶ 8.4.

Ritornando alle linee guida AgID, cui fanno riferimento sia l'Osservatorio che il Ministero del lavoro, esse richiamano le norme ISO/IEC, un insieme di standard internazionali sviluppati congiuntamente dalle organizzazioni ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*).

L'organizzazione ISO si occupa di sviluppare standard per migliorare la qualità, l'affidabilità e l'efficienza dei prodotti, dei servizi e dei sistemi in diversi settori industriali e commerciali. La IEC è un'organizzazione internazionale che sviluppa e pubblica normative tecniche per l'elettronica e l'elettrotecnica. L'IEC si concentra su standard relativi a dispositivi elettronici, apparecchiature elettriche, sistemi di comunicazione e molte altre tecnologie. Tali norme (tecniche) sono applicate

⁶⁶ Il Senato ha approvato nel marzo 2025 un disegno di legge, all'esame della Camera, si pone l'obiettivo di operare un bilanciamento tra opportunità e rischi, prevedendo norme di principio e disposizioni di settore che, da un lato, promuovano l'utilizzo delle tecnologie IA per le condizioni di vita dei cittadini e della coesione sociale e, dall'altro, forniscano soluzioni per la gestione del rischio fondate su una visione antropocentrica. In quest'ottica il DDL non intende sovrapporsi all'EU IA ACT, ma accompagnarne il quadro regolatorio a livello nazionale, tenendo in conto l'architettura dei rischi connessi all'uso dell'IA (inaccettabili, alti, limitati e minimi), per cui maggiore è il rischio, maggiori saranno le responsabilità e i divieti per chi sviluppa o adopera sistemi di intelligenza artificiale.

In coerenza con il Ddl il Ministero del lavoro ha già istituito l'Osservatorio sull'adozione dei sistemi di Intelligenza Artificiale (IA) nel mondo del lavoro nasce per monitorare e analizzare concretamente l'impatto delle tecnologie di IA su aziende e lavoratori, fornendo strumenti pratici per un'integrazione efficace e sostenibile.

in vari settori industriali e vengono adottate da governi, organizzazioni e aziende per assicurare la conformità a standard internazionali che promuovono la qualità, l'affidabilità e la sicurezza.

Nel campo dell'intelligenza artificiale, è stata pubblicata la *norma CEI UNI ISO/IEC 42001 - ISO/IEC 42001 "Information Technology – Artificial Intelligence – Management System"*, la quale fornisce un quadro essenziale per la gestione responsabile dell'IA. La sua finalità è aiutare le organizzazioni a gestire i rischi legati all'IA mentre se ne sfruttano le opportunità. Tale norma si occupa di aspetti come la sicurezza, la privacy, la trasparenza e l'equità, garantendo che i sistemi di IA siano utilizzati in modo responsabile ed etico.

Adottare la *ISO/IEC 42001* significa impegnare l'azienda in un processo continuo di valutazione e mitigazione dei rischi, assicurando che ogni applicazione dell'IA non solo rispetti le normative vigenti ma sia anche allineata con i valori etici e sociali. Questo non solo protegge l'organizzazione da potenziali rischi (legali, reputazionali, di gestione sicura delle informazioni, ecc.), ma apre anche la strada a un'innovazione sostenibile che può portare a un vantaggio competitivo significativo.

In Italia, le norme ISO/IEC non hanno forza di legge, ma vengono adottate per allinearsi alle normative nazionali e internazionali. Il rispetto di queste norme è spesso considerato un criterio di conformità a leggi e regolamenti italiani in vari settori, tra cui le leggi sulla sicurezza sul lavoro (es. *D.lgs. 81/2008*) e la protezione dei dati personali (*GDPR - Regolamento 2016/679*). Infatti, le norme ISO, come quelle sulla gestione della salute e sicurezza sul lavoro, possono essere integrate nelle politiche aziendali per garantire che l'ambiente di lavoro sia sicuro e conforme alle leggi italiane.

Inoltre, le aziende che ottimizzano la sicurezza delle informazioni seguendo gli standard ISO possono dimostrare di essere conformi alla normativa GDPR e rispettare pertanto la privacy dei lavoratori.

Le norme tecniche pubblicate dall'ISO/IEC nel campo dell'IA sono molte e riguardano le indicazioni sulla terminologia (standard) per descrivere i concetti e la terminologia nel campo dell'IA [*CEI UNI EN ISO/IEC 22989*], le istruzioni su come le organizzazioni che sviluppano, producono, distribuiscono o utilizzano prodotti, sistemi e servizi che utilizzano l'IA possono gestire i rischi specificamente legati all'IA [*CEI UNI EN ISO 23894*], le informazioni su come affrontare le distorsioni indesiderate nei sistemi di Intelligenza Artificiale (IA) che utilizzano l'apprendimento automatico per svolgere compiti di classificazione e regressione [*EI UNI CEN/CLC ISO/IEC/TS 12791*]. Quartultime, offrono un quadro di riferimento per i sistemi generici di IA che utilizza tecniche di apprendimento Automatico (Machine Learning) [*CEI UNI EN ISO/IEC 23053*], fornendo una terminologia coerente per specificare, misurare e valutare la qualità di un sistema di IA [*CEI EN ISO/IEC 25059*], definendo le fasi e identificando le azioni associate all'elaborazione dei dati durante il ciclo di vita dei sistemi di IA, tra cui l'acquisizione, la creazione, lo sviluppo, la distribuzione, la manutenzione e la dismissione di tali sistemi [*CEI UNI EM ISO/IEC 8183*].

Nel contesto normativo nazionale sull'IA, seppur non ancora consolidato ed in divenire, un posto particolare è riservato all'utilizzo dei sistemi di IA nel campo della salute. I software che hanno una destinazione d'uso medica sono infatti considerati SaMD (*Software as a Medical Device*), dispositivi ad alto rischio, e devono pertanto rispettare i requisiti del Regolamento *MDR (UE) 2017/745*. Tale regolamento si applica sia ai software che hanno l'obiettivo di diagnosticare, prevenire, monitorare, trattare o attenuare una malattia, sia a quelli che forniscono informazioni destinate a informare un operatore sanitario nel prendere la decisione diagnostica o terapeutica finale. Se al momento non esistono regolamenti o norme armonizzate che disciplinano specificatamente l'uso dell'IA nei Dispositivi Medici (DM), la definizione di intelligenza artificiale presente nell'EU IA ACT tenderebbe a ricondurre questi sistemi tra i DM sottoponendoli al rispetto di entrambe le normative.

Poiché nel documento sulle *“Proposte per una strategia italiana per l’intelligenza artificiale”* (https://www.mimit.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf), elaborata dal Gruppo di Esperti MISE sull’IA, non si era entrati in dettaglio nell’area della Medicina, il Consiglio Superiore di Sanità del Ministero della salute aveva ritenuto opportuno approfondire il tema dei sistemi di AI in diagnostica medica, partendo dall’analisi delle evidenze scientifiche, regolatorie ed etiche esistenti, con lo scopo di formulare delle proposte operative per introdurre in modo sicuro nella pratica clinica i sistemi di IA. Nel loro rapporto *“I Sistemi di intelligenza artificiale come strumento di supporto alla diagnostica”* (<https://sirm.org/wpcontent/uploads/2022/04/Intelligenza-artificiale.pdf>), dopo una prima analisi sulle definizioni di AI, gli aspetti tecnologici e lo stato dell’arte dei sistemi operanti in diagnostica, sono elencate le proposte operative per introdurre nella pratica clinica i software di IA in modo sicuro e per implementare infrastrutture e modalità di governance corrette. Considerando l’attività dei lavoratori, in questo caso del personale sanitario, il loro rapporto evidenzia la necessità di garantire la formazione degli operatori sanitari, oltre che degli utenti, mettendo in atto misure dirette a migliorarne le conoscenze (e le competenze) sui sistemi di AI e sul significato dei dati utilizzati per la loro modellizzazione, sulla necessità di realizzare studi sul gradimento dell’interazione fra l’uomo e la macchina.

Una proposta per le Associazioni della CIIP

All’interno del percorso che vede l’impiego dell’IA per migliorare le condizioni di lavoro, tutelare l’integrità psicofisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell’Unione europea un ruolo fondamentale potrebbe essere svolto dalla *“Consulta Interassociativa Italiana per la Prevenzione (CIIP)”*, formata dalle associazioni professionali e scientifiche più rappresentative che operano nei settori della medicina del lavoro, della psicologia del lavoro, dell’igiene industriale, della prevenzione ambientale, della formazione, della sicurezza del prodotto e dell’ergonomia, della protezione radiologica e degli agenti fisici, la quale diverrebbe uno strumento competente e super-partes per l’integrazione delle conoscenze e l’armonizzazione delle risposte alle problematiche della prevenzione e della sicurezza dei lavori.

Le azioni che la CIIP potrebbe intraprendere sono:

- a) *offrire formazione ed aggiornamento continuo*, organizzando seminari di formazione, workshop e programmi di aggiornamento per i lavoratori, in particolare per quelli che potrebbero trovarsi in prima linea nell’interazione con l’IA;
- b) *sostenere la ricerca ed il dialogo interdisciplinare*, promuovendo il dialogo e la collaborazione tra gli sviluppatori di IA, gli esperti di settore, i lavoratori e le istituzioni per garantire che le tecnologie siano progettate e implementate in modo che rispondano alle reali esigenze dei lavoratori e per affrontare in modo completo le sfide normative: si potrebbero sviluppare sistemi di certificazione o audit per garantire che i sistemi di IA siano conformi alle normative sanitarie, etiche e legali;
- c) *favorire l’inclusione digitale e l’accessibilità*, promuovendo politiche per ridurre il *digital divide*, garantendo che tutti i lavoratori abbiano pari opportunità nell’apprendimento e nell’accesso alle tecnologie IA (alfabetizzazione digitale, programmi di supporto e riqualificazione per i lavoratori in transizione, l’inclusione digitale e l’accessibilità) e contribuendo allo sviluppo di linee guida etiche per l’uso dell’IA, enfatizzando il rispetto per i diritti umani, la privacy, la non discriminazione e la trasparenza;
- d) *garantire la protezione dei diritti dei lavoratori*, promuovendo politiche che salvaguardino l’occupazione dei lavoratori (automazione e l’IA cambiano il mercato del lavoro, e garantendo che i sistemi basati su IA non violino la privacy dei lavoratori (ad esempio, attraverso la raccolta e l’elaborazione dei dati personali senza il loro consenso);

- e) *facilitare la transizione professionale*, aiutando i lavoratori a navigare nelle transizioni professionali causate dall'automazione e dall'adozione dell'IA, in particolare nei settori che potrebbero subire grandi cambiamenti (riqualificazione, orientamento professionale e upskilling);
- f) *assistere il benessere psicologico dei lavoratori*, supportando i professionisti nel gestire le preoccupazioni legate all'automazione e alla digitalizzazione (*dissonanza cognitiva, ansia da tecnologia, stress da incertezza, burnout professionale, preoccupazione etica, senso di impotenza*), lavorando sulla resilienza psicologica, organizzando eventi o sessioni di consulenza per preparare i lavoratori ai cambiamenti legati all'IA;
- g) *promuovere politiche di IA per il bene comune*, sostenendo politiche che assicurano l'adozione dell'IA in modo equo, riducendo le disparità di accesso e di opportunità per i lavoratori, lavorando con i rappresentanti dei lavoratori e/o le organizzazioni sindacali e indirizzando le imprese ad integrare soluzioni basate su IA che migliorino la qualità del lavoro piuttosto che ridurre i posti di lavoro;
- h) *monitorare l'impatto dell'IA e garantire la valutazione dei rischi*, conducendo studi e ricerche per monitorare come l'IA influenzi l'occupazione, le disuguaglianze, la qualità del lavoro (paura dell'errore), suggerendo programmi di revisione e monitoraggio (misure di sorveglianza umana, verifiche di garanzia della qualità ed affidabilità, validazione continua) dei sistemi di IA al fine di minimizzarne i rischi associati all'adozione, e sviluppando raccomandazioni per ridurre al minimo gli effetti negativi dell'IA sui lavoratori. L'applicazione delle normative e linee guida nel campo della radioprotezione e dell'assicurazione di qualità, considerando le criticità delle radiazioni ionizzanti al pari degli algoritmi di IA, potrebbe costituire un utile riferimento.

A titolo di esempio si riporta l'esperienza dell'alfabetizzazione in IA svolta attraverso i corsi d'aula, due all'anno, presso l'Azienda USL di Reggio Emilia - IRCCS che dal 2023 ha visto la partecipazione volontaria di quasi duecento sanitari (personale della dirigenza sanitaria e del comparto). La formazione è stata tenuta dal personale fisico del servizio di Fisica Medica dell'AUSL. Tale personale è fortemente coinvolto nella ricerca in IA (anche nel campo della protezione dei lavoratori con radiazioni ionizzanti), grazie all'esistenza di un laboratorio dedicato, oltre che nell'accettazione e nella valutazione di sistemi IA che sono presenti nell'ambiente ospedaliero. Le attività di accettazione e monitoraggio dei sistemi di IA di tipo medico (radiologia, radioterapia, medicina nucleare, interventistica, anatomia patologica, ecc..) in molte realtà sanitarie italiane sono svolte dai servizi di Fisica Sanitaria. I corsi effettuati (<https://www.ausl.re.it/laboratorio-di-Ricerca-MAIA>) nell'AUSL di RE hanno ricevuto un significativo gradimento e dal 2025 sono condivisi con un'altra azienda sanitaria regionale e saranno realizzati anche in FAD (formazione a distanza), per essere poi messi a disposizione dell'intero personale dell'AUSL secondo quanto richiesto dall'EU IA ACT in termini di formazione.

7.4 Linee Guida IA del MLPS

Il 17 giugno 2025 il Ministero del Lavoro e delle Politiche Sociali ha pubblicato il report della consultazione pubblica per le "Linee guida sull'IA nel mondo del lavoro"

Il documento [a questo link](#)

7.5 Considerazioni etiche sulla Intelligenza Artificiale in Medicina del Lavoro

Antonio Baldassarre*, Martina Padovan**

*Professore di Medicina del Lavoro - Università degli studi Firenze

** Medico competente-Dirigente UOC Medicina preventiva aziendale-Azienda USL Toscana Nord Ovest

7.5.1 Introduzione

L'implementazione della Intelligenza Artificiale (IA) nell'ambito della Medicina del Lavoro promette di rivoluzionare la gestione della salute e sicurezza occupazionale, ma solleva simultaneamente questioni fondamentali di carattere etico. Le implicazioni etiche della IA nella Medicina del Lavoro sono già al vaglio di organismi internazionali, comunitari e nazionali, così da poter fornire direttrici che permettano di navigare in sicurezza questa rivoluzione tecnologica.

7.5.2 I Principi Etici Fondamentali

7.5.2.1 Il Framework di Floridi: Cinque Principi per una IA Etica

La Medicina del Lavoro, essendo una disciplina medica, si avvale anche dei quattro principi classici della bioetica che vengono integrati nel framework di Floridi: beneficenza, non-maleficenza, autonomia e giustizia. Questi principi acquisiscono nuove dimensioni quando applicati all'IA, richiedendo un'interpretazione che consideri sia gli aspetti tecnologici che quelli relazionali tra i diversi attori della prevenzione.

Luciano Floridi, la cui ricerca sugli aspetti etici sulla IA è raccolta nel libro "The Ethics of AI" (2023, Oxford Press), propone un framework unificato basato su cinque principi etici fondamentali ed imprescindibili per la corretta implementazione della IA in campo di salute e sicurezza del lavoro:

- Beneficenza, quale principio per promuovere il benessere dei lavoratori, preservare la loro dignità e sostenere la sostenibilità ambientale in ottica globale One Health. Nel contesto occupazionale, questo principio richiede che l'IA sia progettata con l'obiettivo di migliorare le condizioni di lavoro, promuovendo il benessere dei lavoratori così come sancito dall'art. 2087 del Codice civile;
- Non-maleficenza, quale principio a tutela della privacy, della sicurezza e della "prudenza delle capacità". Questo principio assume particolare rilevanza nel settore sanitario, dove i dati particolari e sensibili ai sensi del Regolamento generale sulla protezione dei dati (GDPR), ivi inclusi quelli dei lavoratori, devono essere protetti da uso improprio o discriminatori;
- Autonomia, quale principio di lasciare all'uomo la possibilità di decidere di delegare (decide-to-delegate), mantenendo il controllo umano sui processi decisionali ed organizzativi. L'autonomia dei lavoratori deve essere preservata anche quando l'IA supporta o automatizza determinate funzioni;
- Giustizia, quale principio atto a promuovere e preservare la solidarietà sociale ed evitare l'ingiustizia. Negli ambienti di lavoro, questo richiede che l'IA non amplifichi le disuguaglianze esistenti o crei nuove forme di discriminazione, in piena compliance con quanto sancito dalle convenzioni ILO n. 111 del 1958 e n. 190 del 2019;
- Esplicabilità, fulcro attorno al quale ruotano intelligibilità e responsabilità, per garantire che i sistemi IA siano comprensibili e che vi sia chiara attribuzione di responsabilità per le loro azioni.

Le Sette Questioni Etiche di Santoni de Sio

La prima questione etica identificata da Santoni de Sio riguarda la governance dell'impatto dell'IA sulle perdite di posti di lavoro e sui problemi sociali derivanti dal conseguente rimodellamento del mercato del lavoro. Lo studio ILO-NASK (ILO Working Paper 140, maggio 2025) stima che un posto di lavoro su quattro a livello mondiale sia potenzialmente esposto (fino al 34% nei Paesi ad alto reddito), con una maggiore esposizione di alcune professioni cognitive altamente digitalizzate nei settori dei media, del software e della finanza, con un divario di genere sfavorevole per le donne, sebbene sostenendo come il risultato più probabile sia la trasformazione del lavoro piuttosto che la sostituzione, anche per limiti tecnologici, lacune infrastrutturali e carenza di competenze.

La seconda questione etica riguarda il possibile contributo della IA nel creare nuove forme di oppressione attraverso sistemi di controllo algoritmico caratterizzati da quattro elementi distintivi: comprensività (raccolta estensiva di dati attraverso sensori, telecamere e dispositivi biometrici), istantaneità (feedback e valutazione continui), interattività (sistemi che modificano dinamicamente il comportamento lavorativo) e opacità (mancanza di trasparenza nei processi decisionali), come già studiato da Leso nel 2018. Un esempio paradigmatico è rappresentato dai c.d. riders della gig-economy ovvero economia delle piattaforme digitali, i quali, nonostante siano stati inseriti tra i lavoratori essenziali, da intendersi come preposti allo svolgimento di mansioni critiche ai fini della sicurezza pubblica e salute dalla Commissione Europea (Comunicazione 2020/C1021/103) durante la pandemia COVID-19, operano sotto costante sorveglianza, sperimentando quello che Santoni de Sio descrive come una combinazione dei peggiori aspetti della catena di montaggio del XX secolo con il controllo algoritmico del XXI secolo.

La terza questione etica riguarda il possibile impatto della IA sull'agentività morale (moral agency), sull'autonomia e sulla responsabilità dei lavoratori attraverso meccanismi di dominazione algoritmica. Le piattaforme digitali, come riportato anche da un approfondimento della European Trade Union Institute (ETUI) nel 2020, esercitano un controllo estensivo sui lavoratori senza fornire trasparenza sui processi decisionali, creando quello che Vredenburg nel 2022 definisce come una violazione dell'autonomia morale hegeliana.

I lavoratori devono mantenere la capacità di comprendere, valutare e governare (meaningful human control, Santoni de Sio e Van den Hoven, 2018) i sistemi IA che governano il loro lavoro, non viceversa. La perdita di tale controllo, paradossalmente, potrebbe creare un vulnus, laddove nessun essere umano potrebbe essere legittimamente ritenuto responsabile per gli esiti potenzialmente negativi dell'interazione uomo-macchina.

La quarta questione etica riguarda il lavoro sommerso, ovvero attività economicamente preziose svolte da lavoratori senza adeguato riconoscimento, compenso o protezione. Questo fenomeno è evidente, ancora una volta, nella gig-economy, che vede un indebito vantaggio ed incremento del potere socioeconomico delle aziende tecnologiche senza appropriato riconoscimento per i lavoratori.

Inoltre, come denunciato da Crawford (*Atlas of AI*, 2021), la produzione di IA dipende massicciamente dall'estrazione di materie prime, energia e lavoro dai paesi del Sud del mondo, creando strutture neo-coloniali che perpetuano le disuguaglianze globali. A tal proposito, citiamo Floridi, il quale ha recentemente diffuso un estratto del suo ultimo libro, prossimo all'uscita:

Sometimes intelligence is the ability to achieve effortlessly what an AI requires warehouses of servers, oceans of data,

gigawatts of electricity, truckloads of cash, and algorithms so complex nobody is quite sure what they are doing to deliver.

La quinta questione etica riguarda il possibile ruolo della IA come fattore e generatore di opportunità per le persone di svolgere un lavoro significativo, nella accezione di lavoro che produce ricchezza da un punto di vista psicologico, sociologico e politico (Yeoman, 2014). Gheaus e Herzog, già nel 2016, avevano identificato quali ricchezze morali e materiali, diverse dal denaro, lo sviluppo di abilità e la costruzione di una identità lavorativa propria che portassero al raggiungimento della eccellenza. Tali ricchezze, secondo gli autori, si basano sulla contemperazione dell'idea aristotelica secondo la quale lo sviluppo di capacità e competenze produce conoscenza, avanzamento tecnologico o bellezza, e dell'ideale kantiano di raggiungimento della autonomia morale, attraverso la creazione di relazioni positive e costruendo una comunità sul lavoro basata sull'equità, che contribuiscono al benessere della società che, chiudendo un circolo virtuoso, riconosce identità e status professionale dei lavoratori, in linea con la dottrina hegeliana. La sfida etica consiste nel garantire che l'automatizzazione non privi i lavoratori di queste dimensioni di significato, mantenendo spazi per l'espressione del fattore umano.

La sesta questione etica riguarda il possibile impatto della IA sui valori e le norme sociali, influenzando le "sfere di giustizia" (Walzer, 1983) e potenzialmente causando la "colonizzazione del mondo vitale" (Habermas, 1987), anche grazie alla spinta tecnologica che potrebbe portare ad un progressivo ricorso alla IA per ottenere beni e servizi a discapito dei professionisti, come testimoniato dal c.d. fenomeno di "Googlizzazione" (utilizzo di Google, ndr) della ricerca in sanità (*Googlization of healthcare research*, Sharon, 2016). I sistemi IA possono, pertanto, alterare le norme professionali consolidate, ridefinire i rapporti di potere all'interno delle organizzazioni e spostare gli equilibri sociali.

La settima, ed ultima, questione etica identificata da Santoni de Sio riguarda la definizione ed identificazione dei responsabili (e garanti) che l'IA abbia un impatto positivo piuttosto che negativo sui valori etici e sociali. Questa responsabilità è distribuita tra sviluppatori, datori di lavoro, legislatori e lavoratori stessi, richiedendo approcci collaborativi e multi-stakeholder, come anche sancito dal AI Act approvato dal Parlamento Europeo il 13 marzo 2024 sulla base del Trattato sull'Unione Europea (TUE) e del Trattato sul Funzionamento dell'Unione Europea (TFUE).

7.5.3 Il quadro regolatorio e normativo

7.5.3.1 Organizzazione Mondiale della Sanità (OMS)

Nel 2024 l'OMS ha pubblicato linee guida complete sull'etica e la governance dell'IA per la salute, identificando sei principi chiave. La protezione dell'autonomia umana richiede che l'espansione dell'autonomia delle macchine non comprometta quella umana. La promozione del benessere umano enfatizza la sicurezza e l'interesse pubblico come priorità principali. La trasparenza, chiarezza e intelligibilità sono essenziali per la fiducia. La responsabilità e l'accountability devono essere chiaramente definite in tutti gli usi dell'IA. La inclusività ed equità richiedono che l'IA non amplifichi le disparità esistenti. Una IA responsiva e sostenibile deve rispondere efficacemente ai bisogni umani senza compromettere l'ambiente. L'OMS raccomanda oltre 40 misure specifiche per governi, aziende tecnologiche e fornitori di servizi sanitari, inclusi investimenti in infrastrutture pubbliche per l'IA, valutazioni obbligatorie post-implementazione e coinvolgimento degli stakeholders nello sviluppo di ecosistemi digitali basati sulla IA e centrati sull'uomo.

7.5.3.2 International Labour Organization (ILO)

Nel 2025 l'ILO, nel rapporto *"Revolutionizing Health and Safety: The Role of AI and Digitalization at Work"*, evidenzia come l'IA possa migliorare la sicurezza sul lavoro riducendo l'esposizione ai fattori

di rischio, ammonendo circa l'emersione di nuovi pericoli. Le raccomandazioni dell'ILO includono il rafforzamento dell'accesso alla formazione digitale, il dialogo sociale inclusivo e partecipativo dei lavoratori nei processi tecnologici e l'espansione dell'infrastruttura per garantire accesso equo alle innovazioni tecnologiche.

7.5.3.3 Unione Europea: AI Act e Platform Workers Directive

Come richiamato sopra, il Parlamento Europeo ha approvato il Regolamento 2024/1689, c.d. "AI Act", stabilendo un sistema di classificazione basato sul rischio, con implicazioni specifiche anche per il settore lavorativo. I sistemi IA utilizzati nella gestione dell'occupazione sono considerati "ad alto rischio" e, pertanto, soggetti a requisiti rigorosi. La Direttiva EU 2024/2831 per i lavoratori delle piattaforme, approvata il 23 ottobre 2024, regola l'utilizzo di algoritmi intelligenti nelle piattaforme digitali, vietando il trattamento automatizzato di certi tipi di dati personali e richiedendo trasparenza nei sistemi decisionali automatizzati. Tali principi sono stati richiamati dall'ETUI, che ha sottolineato la necessità di un'IA centrata sull'essere umano, avanzando la richiesta di una direttiva specifica sul lavoro, complementare all'AI Act che è principalmente una regolamentazione di prodotto (*Future of Work*, ETUI, 2025).

La Medicina del Lavoro si occupa dello studio, della prevenzione e della terapia di malattie derivanti dalle attività lavorative e, perché strettamente collegata per gli aspetti normativi e prescrittivi al Diritto del Lavoro, è chiamata a contemperare due diritti fondamentali del lavoratore, sanciti costituzionalmente: il diritto alla salute ed il diritto al lavoro. È, pertanto, necessario definire una strategia sull'utilizzo dell'IA in ambito lavorativo, monitorare l'impatto sulle realtà lavorative e promuovere la formazione dei lavoratori e dei datori di lavoro in materia di IA. La sua implementazione in Medicina del Lavoro può trovare applicazione in diverse aree, quali il supporto alla definizione ed inquadramento diagnostico delle malattie professionali, ad esempio attraverso l'analisi di immagini radiologiche delle pneumoconiosi, il supporto alla valutazione del rischio mediante sistemi predittivi capaci di raccogliere, campionare ed analizzare dati ambientali attraverso sensori intelligenti (*Internet of Things*, IoT), il supporto alla sorveglianza sanitaria attraverso sensori o dispositivi indossabili per il monitoraggio continuo (*real-time*) durante il turno di lavoro ovvero il supporto per la definizione di piani di ritorno al lavoro secondo un approccio preciso, ovvero non più basato sul paradigma *one-size-fits-all*. D'altro canto, la crescente adozione di queste soluzioni innovative solleva questioni complesse sulla privacy e sull'autonomia dei lavoratori, potendo rappresentare una forma invasiva di controllo. Ogni applicazione richiede considerazioni etiche



specifiche, dalla protezione della privacy dei dati biometrici alla prevenzione di discriminazioni basate su predizioni algoritmiche. Il principio della “capability caution” di Floridi, infatti, suggerisce prudenza nell'implementazione di capacità di sorveglianza estese, bilanciando i benefici per la salute con il rispetto della dignità umana.

L'integrazione ed aggiornamento del codice etico dell'International Commission on Occupational Health (ICOH) alla luce delle linee guida dell'OMS contribuirebbe ad aumentare la consapevolezza sulle opportunità e sulle potenziali ricadute di questa tecnologia e regolarne l'utilizzo, rappresentando un punto di partenza e non un punto di arrivo in un processo dinamico, come quello che caratterizza la Medicina del Lavoro. Lo sviluppo e l'applicazione di standard professionali secondo un approccio multidisciplinare e al passo con i tempi dovrebbe esprimersi, sulla falsariga dell'OMS, sulle nuove sfide etiche e di governance dell'IA generativa date le possibili applicazioni della IA in Medicina del Lavoro. Le aree chiave per l'integrazione includono, come già richiamato, la trasparenza e esplicabilità nei processi decisionali supportati dall'IA, con gli operatori della medicina occupazionale come primi responsabili dell'uso trasparente delle tecnologie a garanzia della privacy e della confidenzialità dei dati, con enfasi particolare sui dati di sorveglianza sanitaria.

L'IA ha il potenziale per rivoluzionare la Medicina del Lavoro migliorando l'efficienza, l'accuratezza, garantendo un approccio personalizzato per i lavoratori. In questa rapida evoluzione tecnologica, è fondamentale stabilire chiari limiti etici e di governance, promuovendoli tra tutti i professionisti della tutela della salute e della sicurezza sul lavoro. Il futuro non vedrà l'IA sostituire il medico del lavoro ma, possibilmente, il medico del lavoro che potrà utilizzare, secondo scienza e coscienza, l'IA.

Bibliografia

- Floridi, Luciano, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford, 2023; online edn, Oxford Academic, 24 Aug. 2023), <https://doi.org/10.1093/oso/9780198883098.001.0001>
- Floridi, Luciano and Cows, Josh, *A Unified Framework of Five Principles for AI in Society* (September 20, 2019). Available at SSRN: <https://ssrn.com/abstract=3831321> or <http://dx.doi.org/10.2139/ssrn.3831321>
- Santoni de Sio, F. (2024). *Artificial Intelligence and the Future of Work: Mapping the Ethical Issues*. *Journal of Ethics*, 28 (3), 407-427. <https://doi.org/10.1007/s10892-024-09493-6>
- Leso, V., Fontana, L., & Iavicoli, I. (2018). *The occupational health and safety dimension of Industry 4.0: Industry 4.0 and occupational health*. *La Medicina Del Lavoro | Work, Environment and Health*, 109(5), 327–338. <https://doi.org/10.23749/mdl.v109i5.7282>
- Six Dijkstra MWMC, Siebrand E, Dorrestijn S, Salomons EL, Reneman MF, Oosterveld FGJ, Soer R, Gross DP, Bieleman HJ. *Ethical Considerations of Using Machine Learning for Decision Support in Occupational Health: An Example Involving Periodic Workers' Health Assessments*. *J Occup Rehabil*. 2020 Sep;30(3):343-353. doi: 10.1007/s10926-020-09895-x
- Baldassarre A, Padovan M. *Regulatory and Ethical Considerations on Artificial Intelligence for Occupational Medicine*. *Med Lav*. 2024 Apr 24;115(2):e2024013. doi: 10.23749/mdl.v115i2.15881
- *Ethics and governance of artificial intelligence for health: WHO guidance*. Geneva: World Health Organization; 2025
- *Revolutionizing health and safety: The role of AI and digitalization at work*. Geneva: International Labour Organization; 2025

- Addressing AI risks in the workplace: Workers and algorithms. European Parliamentary Research Service (EPRS). European Union; 2024
- Artificial Intelligence and the future of work. Eurobarometer Report. European Union; 2024
- Immad A Shah, SukhDev Mishra, Artificial intelligence in advancing occupational health and safety: an encapsulation of developments, *Journal of Occupational Health*, Volume 66, Issue 1, January-December 2024, uiad017, <https://doi.org/10.1093/joccuh/uiad017>
- Harishbhai Tilala M, Kumar Chenchala P, Choppadandi A, Kaur J, Naguri S, Saoji R, Devaguptapu B. Ethical Considerations in the Use of Artificial Intelligence and Machine Learning in Health Care: A Comprehensive Review. *Cureus*. 2024 Jun 15;16(6):e62443. doi: 10.7759/cureus.62443
- Maciej Jarota. Artificial intelligence in the work process. A reflection on the proposed European Union regulations on artificial intelligence from an occupational health and safety perspective. *Computer Law & Security Review*. Volume 49, 2023, 105825, doi: 10.1016/j.clsr.2023.105825.
- Hanna MG, Pantanowitz L, Jackson B, Palmer O, Visweswaran S, Pantanowitz J, Deebajah M, Rashidi HH. Ethical and Bias Considerations in Artificial Intelligence/Machine Learning. *Mod Pathol*. 2025 Mar;38(3):100686. doi: 10.1016/j.modpat.2024.100686
- Shehu Mohammed, Neha Malhotra. Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers and future directions. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*. Volume 5, Issue 1, 2025, 100215. doi: 10.1016/j.tbench.2025.100215.
- El-Helaly M. Artificial Intelligence and Occupational Health and Safety, Benefits and Drawbacks. *Med Lav*. 2024 Apr 24;115(2):e2024014. doi: 10.23749/mdl.v115i2.15835
- European approach to artificial intelligence. European Commission (<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>)
- Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. *Journal of Risk Research*, 1–14. <https://doi.org/10.1080/13669877.2024.2350720>
- Lekadir K, Frangi A F, Porras A R, Glocker B, Cintas C, Langlotz C P et al. FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare *BMJ* 2025; 388 :e081554 doi:10.1136/bmj-2024-081554
- Ning Y, Teixayavong S, Shang Y, Savulescu J, Nagaraj V, Miao D, Mertens M, Ting DSW, Ong JCL, Liu M, Cao J, Dunn M, Vaughan R, Ong MEH, Sung JJ, Topol EJ, Liu N. Generative artificial intelligence and ethical considerations in health care: a scoping review and ethics checklist. *Lancet Digit Health*. 2024 Nov;6(11):e848-e856. doi: 10.1016/S2589-7500(24)00143-2. Epub 2024 Sep 17. Erratum in: *Lancet Digit Health*. 2024 Nov;6(11):e777. doi: 10.1016/S2589-7500(24)00220-6
- Alena Valtonen, Minna Saunila, Juhani Ukko, Luke Treves, Paavo Ritala. AI and employee wellbeing in the workplace: An empirical study. *Journal of Business Research*, Volume 199, 2025, 115584. doi: 10.1016/j.jbusres.2025.115584
- Chaudhry, Zaira S. MD, MPH; Choudhury, Avishek PhD. Clinical Applications of Artificial Intelligence in Occupational Health: A Systematic Literature Review. *Journal of Occupational and Environmental Medicine* 66(12):p 943-955, December 2024. | DOI: 10.1097/JOM.0000000000003212
- Franco G. Virtù e valori etici della Diatriba. Un tributo a Bernardino Ramazzini in occasione del trecentesimo anniversario della morte (1714). *Med Lav*. 2014 Jan-Feb;105(1):3-14

Appendice – Documenti da scaricare

7.6 [Regolamento EU AI 13 giugno 2024](#)

Gazzetta Ufficiale dell'Unione Europea

7.7 [Il futuro del lavoro, Davos, 2025](#)

Etica Sgr

7.8 [Agenda digitale italiana](#)

Presidenza del Consiglio dei ministri

7.9 [Disposizioni e deleghe al Governo in materia di intelligenza artificiale](#)

(LEGGE 23 settembre 2025, n. 132)

7.10 [Presentazione volume INAPP](#)

Istituto Nazionale per l'analisi delle Politiche Pubbliche

7.10.1 [Volume INAPP](#)

Rapporto INAPP 2024



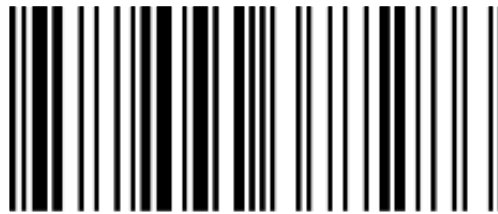
Consulta Interassociativa
Italiana per la Prevenzione

L'Intelligenza Artificiale per la Salute e Sicurezza sul Lavoro

Alcuni contributi sulle opportunità e sulle criticità della applicazione dell'IA nel mondo del lavoro

Ottobre 2025

ISBN 978-88-943772-8-6



9788894377286

Consulta Interassociativa Italiana per la Prevenzione

Sede presso: Clinica del Lavoro "Luigi Devoto"

Via San Barnaba, 8 - 20122 Milano info@ciip-consulta.it - www.ciip-consulta.it

