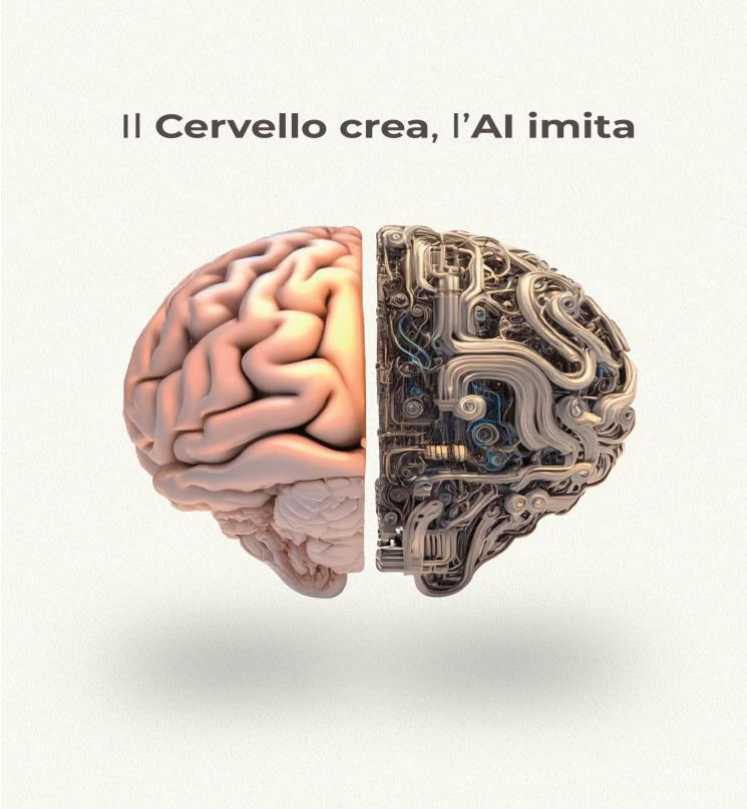
Consulta Interassociativa Italiana per la Prevenzione

Salute e sicurezza sul lavoro nell'era digitale | Ambienti di lavoro sani e sicuri | Partner nazionale campagna 2023-2025



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 Boschiroli
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 ampiamento 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.

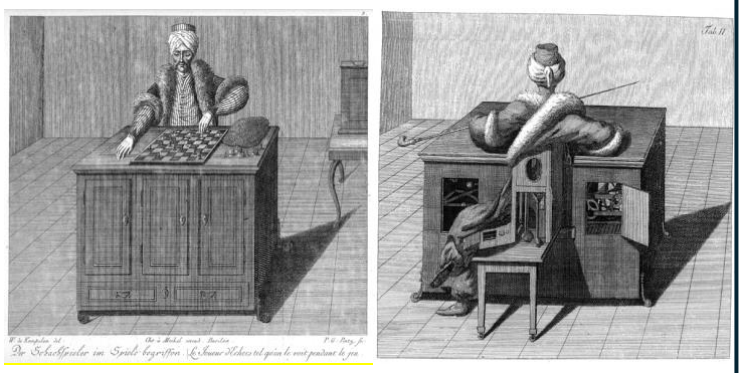
Ci siamo proposti di uscire dal dibattito tra "apocalittici e integrati", come già scriveva Umberto Eco negli anni '60, considerando l'IA una rivoluzione inarrestabile, che offre opportunità ma anche criticità sia per la sicurezza che per il benessere psicofisico dei lavoratori, tema sul quale abbiamo 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 Wolfang von Kempelen *(ndr per Maria Tersa 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**

Gilberto Boschiroli

INTRODUZIONE **4**

Rocco Vitale e Susanna Cantoni

1 IL LAVORO NELL'EPOCA DELL'INTELLIGENZA ARTIFICIALE **10**

1.1 Dall'intelligenza meccanica all'intelligenza artificiale: sintesi dell'evoluzione e rivoluzione tecnologica 10
Antonio Baldassarre e Alberto Baldasseroni

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
Andrea Cirincione

1.4 L'utilizzo di nuove tecnologie per eliminare o ridurre rischi lavorativi: nuove tecnologie, DPC, DPI 32
Cristina Mora e Alice Caporale

1.5 L'utilizzo di piattaforme digitali e la salute e sicurezza dei lavoratori: l'esempio dei riders 46
Francesca Seghezzi

1.6 Presentazione progetto REKON per la prevenzione di incidenti sul lavoro da interferenze macchina/lavoratore 48
Wolfango Pirelli

1.7 Integrazione dell'intelligenza artificiale per la sicurezza nei contesti industriali 49
Andrea Filippini

2 INTELLIGENZA ARTIFICIALE E VALUTAZIONE DEI RISCHI **52**

2.1 Valutazione dei rischi, il fattore umano e le nuove frontiere dell'intelligenza artificiale 52
Rita Somma

2.2 La valutazione del rischio e responsabilità: rischi connessi alle interferenze macchina-uomo-ambiente e relative responsabilità 60
Francesco Costantino

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
Alessandro Palla e Antonio Baldassarre

3 INTELLIGENZA ARTIFICIALE E PARTECIPAZIONE DEI LAVORATORI **75**

3.1 The Filipino workers at the sharp end of AI 75
Théophile Simon

3.2 Documenti EU OSHA: la partecipazione dei lavoratori 76
Rocco Vitale

3.3 La partecipazione degli attori aziendali della prevenzione nella progettazione, valutazione e gestione dei rischi: criticità, opportunità, ruolo della *line* aziendale 79
Sonia Fagotti

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
Cinzia Maiolini e Alessio De luca

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
Matteo Cozzani

4.2 Le ricadute formative previste dall'accordo Stato-Regioni con l'utilizzo dell'intelligenza artificiale 99
Carlo Zamponi e Rocco Vitale

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
Santi Spartà

4.4 L'Accordo Stato Regioni e l'intelligenza artificiale 119
Rocco Vitale

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 124
Barbara Gattoni e Sergio Sangiorgi

6 IL RUOLO DEL MEDICO COMPETENTE NEL LAVORO CON IA 135

6.1 Il ruolo del Medico Competente nel lavoro con AI 135
Terenzio Cassina

7 ASPETTI GIURIDICI ED ETICI 145

7.1 Sistemi di intelligenza artificiale e tutela della salute e della sicurezza sul lavoro 145
Paolo Pascucci
7.2 Intelligenza Artificiale, AI Act e sicurezza del lavoro 149
Giovanni Scudier
7.3 Aspetti normativi dell'intelligenza artificiale in campo lavorativo 163
Mauro Iori
7.4 Linee Guida IA del MLPS 169
7.5 Considerazioni etiche sulla Intelligenza Artificiale in Medicina del Lavoro 170
Antonio Baldassarre e Martina Padovan

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

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 ILO [50] 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 – Rivoluzionare 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 Parlamento[55].

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 esigenza 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 stesso[56].

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 frontiera[58].

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 cibersicurezza 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 ore 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 rinvengono 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 controllo[64].

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 via[65].

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 imprevisto 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.