LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 1 / 2025

Fabio PONTRANDOLFI

Salute e sicurezza sul lavoro, cybersecurity e Intelligenza Artificiale

Salute e sicurezza sul lavoro, cybersecurity e Intelligenza Artificiale

Fabio PONTRANDOLFI
Responsabile Salute e sicurezza nei luoghi di lavoro di Confindustria

Abstract

L'Autore focalizza i profili più rilevanti ed innovativi dell'impatto dell'intelligenza artificiale e della cybersicurezza sulla salute e sicurezza nei luoghi di lavoro, mettendo in luce la necessità di superare alcune previsioni dell'attuale normativa in materia di salute e sicurezza e di altre norme ad essa connesse (es. art. 4 L. n. 300/1970; dlgs 196/2003), essendo necessario dirimere l'insostenibile conflitto tra obbligo di controllo e vigilanza, da un lato, divieto di controllo a distanza, dall'altro, e limitazione dell'accesso ai dati personali, dall'altro ancora.

The Author focuses on the most relevant and innovative aspects of the impact of artificial intelligence and cybersecurity on health and safety in the workplace, highlighting the need to overcome certain provisions of the current legislation on health and safety and other related regulations (e.g., Article 4 of Law No. 300/1970; Legislative Decree 196/2003). It is necessary to resolve the unsustainable conflict between the obligation of control and supervision, on the one hand, the prohibition of remote control, on the other, and the limitation to the access to personal data.

Sommario

Premessa

Le tematiche e le politiche di sicurezza collegate a IA e cibernetica sono ormai passate da una fase di studio (in particolare, sulla maturità culturale e sulla diffusione della coscienza e consapevolezza dei rischi) ad una condizione di obbligo, posto che si tratta di un rischio che le imprese devono prevedere e gestire, con logiche e strumenti innovativi (per quanto sia possibile riscontrare una logica comune nel ciclo di Deming – plan/do/check/act).

In genere, i profili di riferimento per la sicurezza di IA e cybersecurity sono la sicurezza dei dati personali e di quelli informatici, il funzionamento dei sistemi complessi e di rilevanza essenziale pubblica. In realtà, un ulteriore profilo va considerato: l'ingresso dell'IA nei processi produttivi e la necessità di difesa degli stessi da attacchi cibernetici, nella misura in cui possono danneggiare la stessa produzione, l'asset industriale e, più in particolare, la sicurezza delle persone coinvolte nel processo produttivo[1].

L'assolutezza della tutela della vita umana, della salute e della sicurezza dei lavoratori, al di là del corretto principio dell'inesistenza di diritti costituzionali tiranni, impone una profonda riflessione sul rapporto tra le condizioni ed i presupposti per il pieno conseguimento dell'obiettivo, la permanenza e la trasformazione di rischi tradizionali, l'ingresso di rischi nuovi e la logica della mediazione e del contemperamento.

L'avvento di strumenti evoluti e anticipatori della stessa prevenzione, in una logica che, riducendo la discrezionalità dell'agire del lavoratore e l'incremento dell'automazione, sottrae il lavoratore stesso dalla rischiosità della scelta del gesto lavorativo e della stessa relazione con i fattori di pericolo (riducendo così drasticamente il rischio), impongono una riflessione approfondita sulla perdurante opzione del contemperamento, almeno quando gli strumenti a disposizione diano sufficiente certezza (in connessione con la formula BARD del diritto penale, ossia l'oltre ogni ragionevole dubbio) del salvifico risultato prevenzionale.

La valutazione di tutti i rischi

Il punto di partenza dell'analisi di questo ultimo aspetto, sul quale ci si soffermerà, è l'obbligo di valutazione di tutti i rischi: l'indeterminatezza che caratterizza l'obbligo ne determina l'estensione anche ai rischi derivanti da attacchi informatici e dall'uso dell'IA.

Il nostro sistema normativo di salute e sicurezza è fondato, da un lato, sul principio di autonormazione (che risiede nella valutazione dei rischi e nell'adozione di modelli organizzativi e di protocolli) e, dall'altro, su di un conseguente modello di responsabilità penale per omissione

[1] C. Romeo, Tutela e sicurezza del lavoro nell'era della intelligenza artificiale: profili biogiuridici, in Il lavoro nella giurisprudenza, n. 5, 1 maggio 2024, p. 445

(dove il comportamento doveroso spesso non è indicato o specificato nelle norme ma nelle regole fissate nel processo di autonormazione): questo modello comporta l'automatica estensione dell'obbligo e della responsabilità ad ogni fattore di rischio.

Secondo la Corte di giustizia[2] "*i rischi professionali che devono essere oggetto di una valutazione da parte dei datori di lavoro non sono stabiliti una volta per tutte, ma si evolvono costantemente in funzione, in particolare, del progressivo sviluppo delle condizioni di lavoro e delle ricerche scientifiche in materia di rischi professionali*"

La valutazione dei rischi "dinamica"

Espressione concreta della genericità dell'obbligo di fondo è – secondo la giurisprudenza[3] - l'introduzione del concetto di "*valutazione dei rischi dinamica*": "*Le misure atte a prevenire il rischio di infortuni, infatti, vanno individuate in ragione delle peculiarità della sede di lavoro e progressivamente adattate in ragione del mutamento delle complessive condizioni di svolgimento delle singole mansioni, secondo un concetto "dinamico" del rischio, che impone l'adeguamento degli strumenti di protezione e l'aggiornamento della formazione ed informazione del lavoratore, ogni qual volta intervenga un rischio nuovo rispetto a quello originariamente previsto*"

La valutazione del rischio specifico di IA e Cybersecurity

Il Regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, approvato da Consiglio il 14 maggio 2024 è il primo strumento per la valutazione dei rischi connessi all'IA.

Con riferimento al rischio da attacco cibernetico, il Dlgs 4 settembre 2024, n. 138, attuativo della direttiva NIS2, indica (art. 24) le modalità di gestione del rischio cibernetico.

Norme tecniche (come, ad es., la ISDO/IEC 2705:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks) supportano il valutatore: la estrema difficoltà della valutazione, il carattere innovativo del rischio e l'altissima attenzione riservata dall'ordinamento a questi temi dovrebbe consigliare la massima libera diffusione e semplificazione di tutti gli strumenti valutativi, posto che si tratta di un rischio dove è evidente la prevalenza della sicurezza di tutti su quella del singolo.

[2] Causa C-49/00
[3] Cass., 12 dicembre 2023, n. 49300

La sicurezza sul lavoro nel Regolamento macchine, tra IA e cybersecurity

Il rischio derivante dall'uso dell'IA (in particolare, se autoevolutiva) è indubbiamente rientrante tra quelli che incidono sulla sicurezza delle attrezzature, per il quale è prevista la valutazione.

Il rischio tecnologico è confermato anche dalla recente previsione del regolamento macchine che fa riferimento alla valutazione dei rischi relativi alla presenza di forme di intelligenza artificiale auto evolutiva nelle attrezzature.

L'interconnessione tra IA e cyber è evidente anche nel medesimo Regolamento, laddove, al fine di affrontare i rischi derivanti da azioni dolose di terzi e che hanno un impatto sulla safety delle macchine, la proposta aggiunge un nuovo requisito essenziale di sicurezza (1.1.9) e chiarisce il requisito sulla safety e l'affidabilità dei sistemi di controllo (1.2.1).

Il rischio cibernetico, che riguarda l'azienda nel suo complesso) indubbiamente può essere ricondotto anche più specificamente alla sicurezza sul lavoro, come ricorda l'Agenzia europea per la salute e sicurezza sul lavoro (OSHA) nel documento Integrare la salute e sicurezza sul lavoro nella valutazione dei rischi connessi alla cibersicurezza[4].

Ecco, allora, che il datore di lavoro si trova di fronte ad una realtà complessa, di difficile valutazione, che richiede nuove professionalità e nuovi strumenti.

IA e sicurezza delle attrezzature di lavoro

La presenza dell'IA nelle attrezzature, se non opportunamente governata, ne può determinare il malfunzionamento (o il funzionamento diverso) rispetto alle previsioni originarie, mettendo a rischio l'asset operativo, la sicurezza delle persone e la qualità e sicurezza dei prodotti oggetto di lavorazione.

Tutte le attrezzature utilizzate in azienda possono essere governate – in tutto o in parte – dall'IA: robot, cobot, macchine predittive, la sensoristica, con rischi da collisione, da comportamenti imprevedibili e per l'ambiente[5].

L'IA, che deve restare strumento non sostitutivo della decisione dell'uomo[6], specie laddove sia auto evolutiva o generativa, può alterare (anche insensibilmente e non in modo immediatamente visibile ma in modo dannoso nel tempo) il funzionamento di macchine e attrezzature di lavoro:

[4] V. anche M. Grandi, EU-OSHA "Salute e sicurezza sul lavoro nell'era digitale", in Igiene & Sicurezza del Lavoro, n. 11, 1 novembre 2022, p. I

[5] Robot Labor Law. Linee di ricerca per una nuova branca del diritto del lavoro e in vista della sessione sull'intelligenza artificiale del G7 del 2024* di Michele Faioli in Federalismi.it, 8/2024 https://federalismi.it/nv14/articolo-documento.cfm?Artid=50376

[6] T. Treu, Intelligenza Artificiale (IA): integrazione o sostituzione del lavoro umano?, in WP CSDLE "Massimo D'Antona".IT – 487/2024 - https://csdle.lex.unict.it/sites/default/files/Documenti/WorkingPapers/Treu_487_2024it.pdf

le attrezzature dotate di IA possono imparare a svolgere azioni nuove e diventare più autonome, possono elaborare informazioni in tempo reale, risolvere problemi, essendone perfezionati la mobilità, i sistemi di sensori, l'apprendimento, l'adattabilità e la capacità di funzionare in ambienti non strutturati.

Secondo il regolamento macchine, i rischi individuati durante la valutazione del rischio dovrebbero comprendere i rischi che potrebbero manifestarsi durante il ciclo di vita del prodotto in ragione di un'evoluzione prevista del suo comportamento affinché operi con livelli diversi di autonomia. La sicurezza dell'intera macchina o dell'intero prodotto correlato si basa sulle dipendenze e sulle interazioni tra i suoi componenti, comprese le quasi-macchine e, ove pertinente, con altre macchine o altri prodotti correlati che partecipano alla costituzione di un insieme coordinato di un sistema di macchine, che può anche avere come risultato un insieme di macchine. Di conseguenza i fabbricanti dovrebbero essere tenuti a considerare tutte tali interazioni nella valutazione del rischio.

IA e salute

Anche il tema della salute è interessato, soprattutto sul versante prestazionale: le macchine possono supportare l'azione umana e diminuire o annullare i rischi. Allo stesso tempo, possono "aumentare" positivamente i processi produttivi, introducendo, però, richieste maggiori e diverse nell'interazione uomo-macchina, sia sul versante dei tempi che della capacità e velocità cognitiva, che possono incidere – se non adeguatamente governati – sulla capacità di adeguamento consapevole e reazione (stress).

Sotto altro versante, sempre in tema di salute, l'avvento dell'IA introduce numerosi profili innovativi, come la medicina sul lavoro predittiva (e non più solo preventiva), caratterizzata dall'identificazione precoce del rischio di sviluppare una determinata malattia (il che introduce rilevanti elementi d'interesse, ad esempio con riferimento alla idoneità attuale e futura alle mansioni). Il Ministero della salute definisce la medicina predittiva come un approccio che, prima e/o dopo la nascita, tende a scoprire e valutare in termini probabilistici i fattori che, per una specifica persona e in un dato contesto, possono favorire l'insorgenza di una malattia. Per definizione, la medicina predittiva si rivolge alle persone sane o senza malattie evidenti, in queste ricerca i segni della fragilità o del difetto che conferiscono loro una certa predisposizione a sviluppare una malattia. Conseguentemente, la medicina predittiva è probabilistica e individuale e come tale consente la massima personalizzazione degli interventi. Permette inoltre di determinare il profilo di rischio di ciascuna persona, di monitorarne l'evoluzione e di realizzare appropriati interventi preventivi oltre che di selezionare la terapia, la dose e il tempo di trattamento migliori.

La medicina predittiva si pone, quindi, come medicina dell'individualità, ma per essere tale richiede un processo di crescita delle conoscenze e di profonda innovazione nei modelli culturali medici.

Il tema è assai delicato in quanto pone delicati problemi anche sul piano delle responsabilità: essendo disponibile l'analisi predittiva del rischio sanitario, il datore poteva (e, quindi, doveva) conoscere l'evoluzione, per cui doveva adottare le misure preventive per evitare l'insorgenza della malattia o il verificarsi dell'infortunio.

La formazione

L'innovazione tecnologica di IA e cybersecurity incide anche sul fondamentale tema della formazione, posto che i nuovi modelli organizzativi ed operativi possono richiedere, oltre ad una probabile modifica radicale delle mansioni, un supporto formativo notevolmente differente rispetto al passato, sia in termini di contenuti che di professionalizzazione[7].

Intelligenza artificiale e interconnessione informatica sono al centro dell'evoluzione tecnologica, del progresso nella conoscenza, nella scoperta di nuove opportunità, nella apertura a nuovi business: vederli unicamente come rischi non è corretto. Occorre, quindi, gestirli, affinché – in una visione antropocentrica – costituiscano un supporto conoscitivo e valutativo alla decisione, che deve rimanere in capo all'uomo, ed i cui rischi siano valutati e siano oggetto di adeguata prevenzione.

La complessità è incrementata dal fatto che IA e cybersecurity si intrecciano laddove la sicurezza cibernetica può essere gestita attraverso l'IA o, viceversa, quando l'IA è lo strumento per violare la sicurezza cibernetica o, ancora, quando la cybersecurity deve considerare, tra i rischi, anche le forme di IA.

La proprietà intellettuale

Notevoli anche i problemi di segreto e proprietà industriale, posto che la documentazione tecnica allegata alla macchina deve indicare anche il codice sorgente o la logica di programmazione del software relativo alla sicurezza al fine di dimostrare la conformità della macchina o del prodotto correlato rispetto al presente regolamento a seguito di una richiesta motivata da parte di un'autorità nazionale competente, a condizione che sia necessario/a affinché tali autorità siano in grado di verificare il rispetto dei requisiti essenziali di sicurezza e di tutela della salute.

La privacy

Evidenti le interconnessioni con la tutela dei dati personali: il garante europeo sta valutando i pro e i contro di IA e sicurezza cibernetica ai fini della garanzia della privacy.

Il limiti attualmente imposti dalle regole della privacy alla gestione dei lavoratori sono sempre meno coerenti con le esigenze di conoscenza a fini di tutela di alcuni aspetti che vengono ritenuti

[7] V. F. Pedroni, L'interfaccia uomo-software, nuova frontiera dell'ergonomia, in Igiene & Sicurezza del Lavoro, n. 6, 1 giugno 2024, p. 315

rientrare nella sfera di protezione dei dati personali: dalla posizione fisica ai dati relativi allo stato di salute, dai dati personali al comportamento lavorativo.

È ancora possibile ritenere che la tutela della salute e della sicurezza possa cedere o dover essere contemperata e condizionata dall'istanza di riservatezza, soprattutto alla luce delle nuove tecnologie che anticipano la potenziale conoscenza del pericolo e del rischio? o forse la normativa dovrebbe ridurre la responsabilità del datore di lavoro a ciò che è stato possibile conoscere, a seguite delle limitazioni? E ha ancora senso applicare il principio dell'equivalenza causale (ad esempio, in tema di malattie professionali), laddove molte di queste cause e dei fattori individuali di rischio siano ignoti al datore di lavoro, in natura o per effetto dei limiti della privacy?

Il modello 231

Il profilo della responsabilità dell'ente per i reati informatici ha assunto un rilievo progressivamente sempre maggiore[8].

Con le modifiche all'art. 24-bis del Dlgs 231/2001 si sono aggravate le sanzioni relative ai delitti informatici e al trattamento illecito di dati. Una attenzione particolare va rivolta alle interazioni con la privacy, anche alla luce della sentenza 14/12/2023, n. 340/21 e con l'intervento del Garante della Protezione dei Dati personali su "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", plastico.

Un nuovo approccio: dal controllo al supporto

La tecnologia, nel pervadere il sistema produttivo, incide non solo sulle relazioni uomo-macchina ma anche tra persone e tra ruoli in azienda. uno dei nodi essenziali è quello della relazione le figure di supporto alla prevenzione ed i lavoratori. In particolare, uno dei temi principali è la ridefinizione (culturale e normativa) del concetto di controllo, che deve evolversi verso quello di supporto ed assistenza. Realtà virtuale ed aumentata e strumenti di supporto a distanza devono prendere il posto al concetto del controllo a distanza e dei limiti imposti dall'art. 4 della legge n. 300/1970[9].

È obbligo (e quindi diritto) del datore di lavoro accertarsi del comportamento lavorativo corretto, esente da rischi e da deviazioni rispetto alle istruzioni di lavoro (tendenzialmente, attraverso la figura del preposto) ma è anche obbligo di vigilare costantemente sulla sicurezza dei lavoratori (art. 18 Dlgs 81/2008).

[8] A. Sica, Il cybercrime e le responsabilità ex D.Lgs. n. 231/2001, in Amministrazione & Finanza, n. 12, 1 dicembre 2022, p. 48

[9] V. A. Stanchi, Apparecchiature di controllo, strumenti di comunicazione elettronica e controlli difensivi del datore di lavoro, in Il lavoro nella giurisprudenza, n. 4, 1 aprile 2008, p. 351

Il diritto alla privacy può limitare il dovere di controllo e l'obbligo di prevenzione attraverso le misure tecnologiche ed organizzative più innovative in vista della eliminazione del rischio? alla novità dei rischi deve far fronte un innovativo sistema di gestione degli stessi, che comporta anche strumenti innovativi? La possibilità concreta di supporto e vigilanza immediati, efficaci e diretti (es. attraverso telecamere, sensori o occhiali dotati di smart tecnology) deve cedere il passo al divieto di controllo a distanza? In definitiva: ha ancora spazio una mediazione/contemperamento tra le diverse istanze (che non sia riferita alla necessaria informativa) laddove ci siano in ballo l'obbligo di tutela della vita e della integrità psicofisica, da un lato, e la responsabilità penale, dall'altro? A fronte di una responsabilità penale tendenzialmente oggettiva ed assoluta hanno ancora cittadinanza le delimitazioni alla conoscenza e all'intervento in tempo reale e, quindi, efficace fondate su divieto di controllo e privacy? A fronte della concreta possibilità di prevenire l'evento, che spazio c'è per condizionare e delimitare l'adozione di moderni ed incisivi strumenti di vigilanza?

La responsabilità penale in materia di salute e sicurezza

Da ultimo, non certo per importanza, si pone il tema delle responsabilità, in particolare penale, per le conseguenze della errata valutazione del rischio e per eventuali eventi che dovessero mettere a rischio la sicurezza o la salute delle persone o della collettività[10].

Il tema va esteso alla necessità di introdurre sistemi di controllo e vigilanza innovativi, in primo luogo superando impostazioni tradizionali (es. art. 4 l. 300/1970) che vedevano nel controllo un fattore negativo e violativo della privacy e che, ora devono diventare il vero strumento di tutela e supporto operativo e cognitivo.

Proposte

Sul piano normativo, occorre garantire al datore di lavoro – nella sua difficile attività di prevenzione dal rischio – un compendio regolatorio che garantisca certezza del diritto, semplicità ed efficacia. Sul versante regolatorio-procedurale, occorre mettere a disposizione del datore di lavoro una strumentazione definita e semplice, soprattutto in considerazione del fatto che il 97% delle imprese occupa meno di 10 lavoratori. La pubblica amministrazione, poi, dovrebbe adottare una impostazione di supporto collaborativo nella difficile opera di valutazione, offrendo strumenti che guidino in modo semplice alla valutazione ed alla adozione ed implementazione delle corrette misure di protezione, posta l'intersezione tra interessi pubblici (la sicurezza di tutti, intesi come Paese) e privati (cittadini e imprese).

[10] Sul tema generale dei riflessi del diritto della cibernetica sulla disciplina penalistica, v. A. Mattarella, Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite, in Diritto penale e processo 6/2022, p. 809 segg.

Conclusioni

Il tema appassionante, delicato e innovativo della incidenza delle nuove forme di intelligenza artificiale e della sicurezza cibernetica sulla sicurezza sul lavoro impone di aprire lo sguardo su realtà innovative ed anche in modo innovativo: la novità del rischio introduce la necessità di introdurre nuovi strumenti tecnologici, organizzativi e normativi.

Su questi ultimi, che costituiscono il punto di partenza di ogni riflessione, deve assicurarsi priorità, tempestività e adeguatezza all'innovazione.