Dalla paura dell'algoritmo alla cultura dell'automazione

Avv. Roberto Sammarchi
consigliere AIAS, rappresentante AIAS in ENSHPO

Milano, 3 aprile 2025

Ringrazio FAST e tutti gli organizzatori per l'invito a questo importante workshop.

Viviamo in un'era in cui l'intelligenza artificiale e gli algoritmi sono sempre più presenti nel mondo del lavoro, sollevando interrogativi cruciali sul futuro dell'occupazione e sui diritti dei lavoratori. Il mio intervento oggi vuole tracciare un percorso: quello che ci porta dalla diffidenza, a volte vera e propria paura, nei confronti dei sistemi algoritmici e dell'automazione negli ambienti di lavoro, verso una possibile e auspicabile "cultura dell'automazione", intesa come una gestione consapevole, trasparente e sicura delle nuove tecnologie digitali.

1. Il contesto dei nuovi rischi da algoritmo

Viviamo in un'epoca di trasformazione digitale senza precedenti. L'intelligenza artificiale e gli algoritmi pervadono sempre più i nostri luoghi di lavoro, promettendo efficienza, ottimizzazione dei processi, supporto decisionale e, in alcuni casi, persino un miglioramento della sicurezza fisica. Pensiamo agli algoritmi che gestiscono la pianificazione dei turni, l'assegnazione dei compiti, il monitoraggio delle performance individuali e collettive, o che coadiuvano nella valutazione stessa dei rischi lavorativi. Tuttavia, come è stato giustamente evidenziato nell'introduzione di questo evento, a fronte di queste indubbie opportunità, emergono sfide significative e profonde preoccupazioni. La sensazione di essere costantemente monitorati e valutati da una macchina, la potenziale perdita di autonomia nello svolgimento del proprio lavoro, il rischio concreto che decisioni importanti vengano prese sulla base di logiche opache o addirittura discriminatorie, e l'emergere di nuovi rischi per la salute, in particolare quella psicosociale, sono elementi che non possiamo ignorare.

2. Tutela della privacy e protezione dei dati

Questa ambiguità si traduce concretamente in una serie di rischi specifici che alimentano la diffidenza. La "paura" nasce spesso dall'ignoto, dalla percezione dell'algoritmo come una "scatola nera", imperscrutabile nelle sue dinamiche interne. Innanzitutto, vi è il tema cruciale della **privacy**. I sistemi algoritmici, per funzionare, necessitano di enormi quantità di dati, spesso dati personali dei lavoratori. Il loro trattamento deve avvenire nel rispetto del Regolamento Generale sulla Protezione dei Dati (GDPR, Reg. UE 679/2016) e del nostro Codice Privacy (D.Lgs. 196/2003).

Ciò implica non solo l'individuazione di solide basi giuridiche per ogni trattamento, ma anche l'aderenza ai principi fondamentali di finalità, minimizzazione dei dati raccolti, trasparenza verso l'interessato e responsabilizzazione (accountability) del titolare del trattamento.
Spesso, l'implementazione di sistemi decisionali o di monitoraggio automatizzato richiede una preventiva Valutazione d'Impatto sulla Protezione dei Dati (DPIA) per analizzare e mitigare i rischi per i diritti e le libertà degli individui.

3. Limiti al controllo a distanza e art. 4 dello Statuto dei Lavoratori

Strettamente connesso è il tema del **controllo a distanza**, la cui disciplina affonda le radici nell'articolo 4 dello Statuto dei Lavoratori (Legge 300/1970). La *ratio* della norma è proteggere la dignità del lavoratore e impedire controlli eccessivi e invasivi. Pur aggiornato per tener conto delle evoluzioni tecnologiche, questo articolo continua a porre limiti precisi all'uso di strumenti dai quali derivi la possibilità di un controllo sull'attività lavorativa. Tale controllo è ammesso solo per specifiche esigenze (organizzative, produttive, sicurezza del lavoro, tutela del patrimonio aziendale), previo accordo sindacale o autorizzazione amministrativa, e sempre garantendo adeguata informazione ai lavoratori sulle modalità d'uso e di controllo. Gli algoritmi che monitorano le prestazioni, tracciano le attività o valutano l'efficienza ricadono pienamente in questo ambito normativo, e la loro adozione deve superare il vaglio di legittimità imposto dallo Statuto.

4. La sfida della cybersicurezza

Infine, ma non meno importante, non possiamo trascurare la dimensione della **cybersicurezza**. La crescente dipendenza da sistemi digitali complessi e interconnessi introduce nuove e significative vulnerabilità. Un attacco informatico che comprometta l'integrità di un algoritmo gestionale, i dati su cui si basa, o il sistema automatizzato che controlla, può avere conseguenze devastanti, sia sulla sicurezza fisica dei lavoratori (si pensi agli impianti industriali automatizzati) sia sulla correttezza delle decisioni che impattano i rapporti di lavoro (valutazioni errate, assegnazioni inappropriate). La normativa europea, come la Direttiva NIS e la sua recente evoluzione NIS2, e quella nazionale, penso ad esempio al Perimetro di Sicurezza Nazionale Cibernetica per le infrastrutture critiche, impongono standard di sicurezza sempre più elevati, essenziali per garantire l'affidabilità e la resilienza di questi sistemi tecnologici.

5. Le nuove tutele nel Decreto Trasparenza

Proprio per affrontare direttamente il nodo cruciale dell'opacità dei sistemi automatizzati, il legislatore italiano, recependo una specifica direttiva europea focalizzata sulla trasparenza delle condizioni di lavoro, ha introdotto con il Decreto Legislativo n. 104 del 2022, noto come "**Decreto Trasparenza**", un articolo di fondamentale importanza: l'articolo 1-bis. Questa disposizione impone al datore di

lavoro **obblighi informativi specifici e dettagliati** sull'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati, qualora questi siano impiegati per prendere decisioni rilevanti ai fini dell'instaurazione, gestione, esecuzione o cessazione del rapporto di lavoro, nonché per l'assegnazione di incarichi, la sorveglianza e la valutazione delle prestazioni. Il datore di lavoro è ora tenuto a comunicare chiaramente al lavoratore (o ai suoi rappresentanti) informazioni essenziali come: l'esistenza del sistema e le sue finalità; i parametri principali utilizzati per la sua programmazione o addestramento, inclusi i meccanismi di valutazione delle prestazioni; l'importanza relativa attribuita a tali parametri nel processo decisionale algoritmico; le categorie di dati personali trattate; le misure di controllo adottate per garantire l'accuratezza delle decisioni, compresi i meccanismi di supervisione e riesame umano ("human oversight"); i processi disponibili per correggere eventuali risultati distorti o errati del sistema; e, non da ultimo, il livello di accuratezza, robustezza e cybersicurezza del sistema stesso. Queste informazioni, che devono essere fornite prima dell'inizio dell'utilizzo del sistema o al momento dell'assunzione, e aggiornate in caso di modifiche significative, rappresentano un passo cruciale. Il Decreto Trasparenza trasforma quella che era percepita come un'impenetrabile opacità in un diritto esigibile alla conoscenza, fornendo ai lavoratori e alle loro rappresentanze uno strumento concreto per comprendere, dialogare e, se necessario, contestare le logiche algoritmiche che incidono sulla loro vita lavorativa. È il primo, indispensabile mattone per costruire un rapporto di fiducia con queste nuove tecnologie.

6. Il quadro dell'AI Act europeo

Questo importante passo nazionale si inserisce in un quadro europeo ancora più ampio e recente, definito dal Regolamento sull'Intelligenza Artificiale (**AI Act** - Regolamento (UE) 2024/1689). Questo Regolamento, il primo al mondo a disciplinare l'IA in modo orizzontale, è stato pubblicato sulla Gazzetta Ufficiale UE lo scorso 12 giugno 2024 ed è entrato in esecuzione a partire dal 2 febbraio 2025. La norma adotta un approccio innovativo basato sulla stratificazione del rischio: classifica i diversi sistemi di IA in base al potenziale danno che possono arrecare ai diritti fondamentali, alla salute e alla sicurezza. È di fondamentale importanza rilevare che molti sistemi di IA comunemente utilizzati o utilizzabili nel contesto lavorativo – si pensi ai software per lo screening dei curricula, per la valutazione periodica delle prestazioni, per il monitoraggio dell'attività o per l'allocazione ottimizzata dei compiti – sono esplicitamente classificati dal Regolamento come "**ad alto rischio**". Per questa categoria di sistemi, l'AI Act impone una serie di requisiti molto stringenti che devono essere soddisfatti *prima* della loro immissione sul mercato o messa in servizio. Questi requisiti riguardano la qualità e la governance dei dati di addestramento (per mitigare i bias), l'obbligo di redigere una documentazione tecnica dettagliata, la capacità di registrare automaticamente le operazioni (logging), un elevato livello di trasparenza informativa verso gli utenti, la previsione di un'adeguata sorveglianza umana, nonché garanzie di accuratezza, robustezza tecnica

e cybersicurezza. Tali obblighi, che si integrano e rafforzano quelli già previsti dal GDPR e dal nostro Decreto Trasparenza, mirano a garantire che l'IA sviluppata e utilizzata nell'Unione sia sicura, affidabile e rispettosa dei valori e dei diritti fondamentali, inclusi quelli dei lavoratori. È importante precisare che, sebbene il Regolamento sia entrato in vigore, l'applicazione concreta di molti specifici obblighi per i sistemi ad alto rischio avverrà in modo progressivo, soprattutto per quanto riguarda gli aspetti sanzionatori. Tuttavia, il quadro giuridico è ormai definito e le imprese che sviluppano, forniscono o utilizzano sistemi di IA in ambito lavorativo devono iniziare fin da ora a pianificare l'adeguamento e a integrare questi requisiti nei loro processi di progettazione, acquisto e implementazione.

7. I riferimenti nel Testo Unico Sicurezza

Come si collega, dunque, tutto questo complesso quadro normativo alla nostra disciplina fondamentale in materia di **salute e sicurezza sul lavoro**, ovvero il Decreto Legislativo 81/2008 (il Testo Unico Sicurezza)? La connessione è diretta e imprescindibile. Il D.Lgs. 81 impone al datore di lavoro l'obbligo generale e non delegabile di valutare *tutti* i rischi per la salute e la sicurezza dei lavoratori presenti nell'ambiente di lavoro, compresi quelli legati allo stress lavoro-correlato e quelli derivanti dall'organizzazione del lavoro. L'introduzione di sistemi algoritmici e di automazione avanzata introduce nuovi potenziali rischi o modifica in modo significativo quelli preesistenti, che devono essere esplicitamente considerati. Pensiamo ai **rischi psicosociali**: l'aumento del carico mentale dovuto all'interazione continua con sistemi complessi, l'ansia da prestazione indotta da un monitoraggio pervasivo e da valutazioni algoritmiche opache, il possibile isolamento sociale derivante da una minore interazione umana, la perdita di significato del lavoro dovuta a un'eccessiva parcellizzazione o de-skillizzazione, e lo stress specifico derivante dalla cosiddetta "gestione algoritmica". Ma non solo: possono emergere anche **rischi ergonomici**, legati alle nuove interfacce uomo-macchina o a posture e movimenti ripetitivi imposti dai sistemi automatizzati, e **rischi di natura organizzativa**, che impattano sulle competenze richieste, sulle dinamiche di comunicazione interna e sulla struttura stessa del lavoro. Tutti questi rischi, nuovi o modificati, devono essere specificamente identificati, analizzati e valutati all'interno del Documento di Valutazione dei Rischi (DVR), e conseguentemente gestiti attraverso l'adozione di adeguate misure tecniche, organizzative e procedurali di prevenzione e protezione. In questo processo, il Rappresentante dei Lavoratori per la Sicurezza (RLS) gioca un ruolo cruciale, in quanto deve essere consultato preventivamente sulla valutazione e può farsi portavoce delle percezioni e delle preoccupazioni dei lavoratori. La trasparenza garantita dal D.Lgs. 104/2022 diventa, in questo contesto, uno strumento essenziale non solo per la tutela contrattuale, ma anche per permettere una valutazione dei rischi più completa ed efficace.

8. Come favorire la cultura dell’automazione

Le norme, sebbene fondamentali, forniscono solo la cornice; da sole non bastano a creare quella che ho chiamato "cultura dell'automazione". Per superare realmente la paura, costruire fiducia e cogliere appieno le opportunità offerte dalla tecnologia in modo sicuro, etico e sostenibile, servono passi ulteriori, che chiamano in causa l'organizzazione del lavoro e le relazioni industriali. È necessario innanzitutto promuovere la **partecipazione attiva** dei lavoratori e delle loro rappresentanze (siano esse RSU o RLS) fin dalle fasi iniziali di progettazione, selezione e implementazione dei sistemi algoritmici. Un approccio di co-progettazione può aiutare a creare sistemi più equi, più accettati e, in definitiva, più efficaci nel raggiungere gli obiettivi prefissati senza compromettere il benessere dei lavoratori.
Fondamentale è poi investire nella **formazione**: non una formazione meramente tecnica sull'uso degli strumenti, ma una formazione più profonda, che aiuti i lavoratori a comprendere i meccanismi decisionali degli algoritmi, quali diritti sono implicati (incluso il diritto all'informazione sancito dal Decreto Trasparenza e dal GDPR), e i nuovi rischi presenti, fornendo risorse per interagire consapevolmente con i sistemi, con le altre persone coinvolte e con i datori di lavoro.
Dobbiamo poi coltivare un approccio basato sull'**etica e sulla responsabilità**, assicurando che le decisioni finali, specialmente quelle con impatti significativi sulla vita lavorativa delle persone, rimangano sempre sotto il controllo umano, anche quando supportate da un algoritmo. Infine, il **dialogo sociale** e la **contrattazione collettiva**, a livello nazionale, settoriale o aziendale, rappresentano uno strumento privilegiato per definire regole più specifiche e tutele aggiuntive rispetto a quelle minime previste dalla legge, adattando l'uso degli algoritmi alle peculiarità dei diversi contesti produttivi e negoziando soluzioni che bilancino le esigenze di efficienza con la tutela dei diritti e del benessere dei lavoratori.

9. Conclusione

Possiamo concludere che il percorso dalla "paura dell'algoritmo" alla "cultura dell'automazione" è complesso, ma assolutamente necessario se vogliamo governare l'innovazione tecnologica anziché subirla passivamente. Richiede una profonda consapevolezza dei rischi multidimensionali che essa comporta – privacy, controllo, sicurezza informatica, impatti sulla salute fisica e soprattutto psicosociale. Richiede l'applicazione rigorosa degli strumenti normativi che abbiamo a disposizione e di quelli che si stanno consolidando – dallo Statuto dei Lavoratori al GDPR, dal Testo Unico sulla Sicurezza alla normativa sulla Cybersecurity, dal fondamentale Decreto Trasparenza fino al quadro definito dall'AI Act europeo. Ma, soprattutto, richiede un vero e proprio cambio di paradigma culturale e organizzativo, che ponga al centro la trasparenza, la partecipazione dei lavoratori, la formazione continua, la responsabilità etica e un dialogo sociale costruttivo. Solo governando attivamente l'innovazione tecnologica attraverso questo approccio integrato potremo assicurarci che essa sia al servizio di un lavoro più sicuro, più sano, più dignitoso e più giusto per tutti.