

- Luca Barbieri e Andrea Rossetti analizzano gli obblighi del datore di lavoro per sistemi IA ad alto rischio

SISTEMI D'INTELLIGENZA ARTIFICIALE AD ALTO RISCHIO ALLA LUCE DELLE PREVISIONI DEL REGOLAMENTO UE*

• A CURA DI **LUCA DI SEVO** CONSULENTE DEL LAVORO IN BOLLATE (MI) •

Il Regolamento UE del 13 giugno 2024 nasce con lo scopo di delineare le linee guida per l'utilizzo dell'intelligenza artificiale. L'articolo in commento, si concentra in particolare sui sistemi di IA classificati "ad alto rischio" ed esplora gli obblighi che ricadono sul datore di lavoro in qualità di utilizzatore di tali sistemi (*deployer*), in particolare laddove impiegati per la formazione professionale, la gestione, selezione e assunzione dei lavoratori. Il Regolamento, entrato in vigore il 1° agosto 2024, prevede un'applicazione progressiva delle sue disposizioni con tempistiche differenziate: i Capi I e II sono operativi dal 2 febbraio 2025, l'impianto sanzionatorio sarà applicabile dal 2 agosto 2025, mentre le disposizioni sui sistemi di IA ad alto rischio entreranno in vigore dal 2 agosto 2027. Nonostante questa gradualità, gli Autori suggeriscono l'opportunità per i datori di lavoro di adottare sin da subito misure preventive per gestire i rischi derivanti dall'utilizzo dell'IA, conformemente ai principi di prudenza e diligenza.

1. OBBLIGHI ORGANIZZATIVI E TECNICI DEL DEPLOYER

Il datore di lavoro che utilizza un sistema di IA ad alto rischio (*deployer*) è tenuto ad adottare misure tecniche e organizzative idonee per garantire un impiego conforme alle istruzioni fornite con il sistema stesso.

Un aspetto cruciale riguarda la valutazione

dei rischi per la salute e sicurezza dei lavoratori, poiché l'introduzione di sistemi di IA nei processi produttivi può comportare rischi specifici, in particolare di natura psicosociale. Ad esempio, è realistico il rischio di eccessivo affidamento (*over-relying*) da parte del lavoratore sugli *output* del sistema di IA.

2. LA SORVEGLIANZA UMANA COME ELEMENTO ESSENZIALE

La sorveglianza umana rappresenta una misura fondamentale nell'utilizzo di sistemi di IA ad alto rischio. Ciò mira a prevenire o ridurre i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere sia nell'uso conforme che in quello improprio seppure prevedibile.

Il *deployer* deve affidare questa funzione a persone fisiche con competenze adeguate ed è auspicabile che le persone designate per la sorveglianza umana partecipino anche alla fase di analisi, valutazione e selezione del sistema di IA.

3. MONITORAGGIO E CONTROLLO DEL FUNZIONAMENTO DEL SISTEMA DI IA

Un obbligo cruciale per il datore di lavoro è il controllo dei dati di *input*, che devono essere pertinenti e sufficientemente rappresentativi. Inoltre, deve monitorare costantemente il funzionamento del sistema seguendo le istruzioni del fornitore. ➤

* Sintesi dell'articolo pubblicato in *D&PL*, 15/2025, pag. 869 ss, dal titolo *Sistemi d'intelligenza artificiale ad alto rischio: obblighi del datore di lavoro utilizzatore*.

▪ SISTEMI D'INTELLIGENZA ARTIFICIALE AD ALTO RISCHIO ALLA LUCE DELLE PREVISIONI DEL REGOLAMENTO UE ▪

Quando vengono rilevate anomalie, il *deployer* deve informare il fornitore. Se il *deployer* ritiene che il sistema esponga a rischi inaccettabili per la salute e sicurezza delle persone, sul posto di lavoro o per l'ambiente, deve sospendere l'uso e informare sia il fornitore (o distributore) sia l'Autorità di vigilanza del mercato competente.

4. TRACCIABILITÀ E CONSERVAZIONE DEI LOG GENERATI DAL SISTEMA

Per garantire la tracciabilità del funzionamento dei sistemi di IA ad alto rischio, il Regolamento prevede l'obbligo di conservare i *log* generati per almeno 6 mesi, con la finalità di identificare situazioni di rischio grave per la salute e sicurezza, monitorare il sistema dopo la sua immissione sul mercato, garantire trasparenza nell'impiego del sistema e conformità normativa, supportare attività di *audit* interno o ispezioni da parte delle Autorità.

5. OBBLIGHI DI COMUNICAZIONE VERSO LAVORATORI E RAPPRESENTANTI SINDACALI

Prima di utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, il datore di lavoro deve informare sia i rappresentanti dei lavoratori sia i lavoratori direttamente o indirettamente interessati.

La contrattazione collettiva può integrare questi obblighi, come ad esempio quanto fatto con l'accordo dell'11 febbraio 2025 per i lavoratori del settore elettrico, che prevede incontri preventivi tra datore di lavoro e organizzazioni sindacali in caso di introduzione di sistemi di IA nel processo produttivo.

6. L'IMPIANTO SANZIONATORIO PREVISTO DAL REGOLAMENTO

Il Regolamento affida a ciascuno Stato membro il compito di introdurre sanzioni per le violazioni delle sue norme.

Sono previste sanzioni amministrative fino a 35 milioni di euro o al 7% del fatturato me-

dio annuo dell'esercizio precedente.

Per la violazione degli obblighi del *deployer* di un sistema di IA ad alto rischio (art. 26), le sanzioni possono arrivare a 15 milioni di euro o al 3% del fatturato mondiale annuo per le imprese. Per PMI e *start-up*, le sanzioni sono commisurate al fatturato, ma non possono superare i limiti massimi stabiliti.

Il rigoroso impianto sanzionatorio evidenzia l'importanza che il legislatore attribuisce alla conformità con queste disposizioni. I datori di lavoro sono quindi chiamati a una riflessione attenta e ad un'accorta pianificazione prima di implementare sistemi di IA ad alto rischio nei processi produttivi e gestionali.

7. CONSIDERAZIONI

Il tema trattato è di sicuro interesse ed attualità. Personalmente ho l'occasione di partecipare ad alcuni gruppi di lavoro e analisi sia nell'ambito del Centro Studi della Fondazione CDL di Milano, sia nell'ambito dell'associazione Manager Italia Lombardia. Con piacere riporto quanto sia elevato il grado di attenzione che viene riservato all'intelligenza artificiale rispetto all'impatto che può avere nell'ambito lavorativo. A mio modesto parere l'aspetto primario da evidenziare e porre all'attenzione di tutti è la conoscenza di questo strumento innovativo: conoscere vuol dire essere consapevoli e permette di operare con discernimento e intelligenza (in questo caso mi riferisco all'intelligenza umana e ancor di più a quella emotiva), discriminando gli usi corretti che si possono mettere in opera. Al contrario, un utente che ignora i rischi a cui si espone o espone l'organizzazione di cui fa parte, risulta notevolmente pericoloso e difficile da monitorare (e questo vale anche in ambito privato), con possibili conseguenze di notevole peso. Pertanto, è assolutamente necessario promuovere la formazione finalizzata ad ottimizzare l'uso dell'intelligenza artificiale a nostro vantaggio.