Roberto Sammarchi
Parma & Sammarchi Studio Legale Associato, componente della Rete Giuridica AIAS, Coordinatore GTS Mare e 5.0 di AIAS, Socio AIAS

Intelligenza artificiale per la sicurezza sul lavoro. Riflessioni e prospettive nel contesto dell'AI Act

La sfida dell'innovazione: nel contesto della sicurezza sul lavoro, l'intelligenza artificiale (IA) può essere definita come l'insieme delle tecnologie, degli algoritmi e dei sistemi capaci di analizzare e interpretare dati in tempo reale, con l'obiettivo di monitorare, prevenire e mitigare i rischi per la salute e la sicurezza dei lavoratori.

Le misure rese possibili dal nuovo paradigma tecnologico possono comprendere sensori intelligenti, dispositivi indossabili, algoritmi di apprendimento automatico, piattaforme di analisi predittiva e, soprattutto, la loro gestione integrata anche in tempo reale nell'ambito di soluzioni per individuare in modo precoce condizioni pericolose, prevedere incidenti o valutare e correggere tempestivamente comportamenti a rischio.

L'IA, in questo ambito, non si limita alla reazione agli eventi, ma svolge un ruolo con effetti misurabili nell'anticipare potenziali pericoli, migliorando la capacità delle organizzazioni di adottare misure preventive in grado di anticipare le evoluzioni sensibili dei contesti operativi e di progettare ambienti di lavoro più sicuri.

Rispetto alle tradizionali tecniche di sicurezza, l'IA permette un livello superiore di precisione, tempestività e adattabilità nell'identificazione e gestione dei rischi, riducendo l'intervento umano diretto e minimizzando gli errori operativi. L'adozione di sistemi di intelligenza artificiale nei luoghi di lavoro è destinata pertanto a incidere in modo profondo sul concetto stesso di sicurezza. Strumenti di monitoraggio avanzati, tecnologie predittive e sistemi automatizzati di prevenzione trasformano le modalità di gestione del rischio e della sicurezza, con l'obiettivo di migliorare l'ambiente lavorativo e ridurre gli incidenti.

L'evoluzione tecnologica comporta significative implicazioni legali ed etiche, in particolare per quanto riguarda la tutela della privacy e la necessità di garantire l'equità e l'affidabilità delle tecnologie utilizzate.

In questo scenario, l'**AI Act**[1] dell'Unione Europea si presenta come un fondamentale quadro regolatorio, che offre un importante contributo alle applicazioni in ambito di sicurezza sul lavoro.

1. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive UE 2014/90, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Testo rilevante ai fini del SEE, pubblicato in Gazzetta Ufficiale dell'Unione Europea, IT, Serie L, 12/07/2024.

La definizione di intelligenza artificiale

Fra le prime norme al mondo a proporre una definizione di intelligenza artificiale, l'AI Act contiene all'art. 3, comma 1), questa previsione:

> "*«sistema di IA»: 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*".

L'elemento distintivo della definizione risiede nella capacità dei sistemi di IA di apprendere da dati o conoscenza codificata, che li differenzia dai tradizionali sistemi software basati sull'attuazione di regole più o meno rigidamente predefinite.
In particolare, viene evidenziata l'autonomia variabile dei sistemi di IA, cioè la loro capacità di funzionare con una supervisione umana limitata o assente, un aspetto cruciale in ambito lavorativo, dove i sistemi possono monitorare condizioni di sicurezza in tempo reale o supportare decisioni preventive senza un intervento umano continuo.
La definizione comprende l'adattabilità dei sistemi, intesa come la loro capacità di evolversi e apprendere anche dopo essere stati implementati, un aspetto essenziale per rispondere ai cambiamenti dinamici negli ambienti lavorativi.

Dal punto di vista della sicurezza sul lavoro, questa definizione sottolinea come l'IA possa essere utilizzata per migliorare la protezione dei lavoratori, grazie alla capacità di rilevare in tempo reale rischi emergenti, ottimizzare l'uso delle risorse e garantire interventi più efficaci nella prevenzione degli incidenti.

L'espressione "*capaci di influenzare ambienti fisici e virtuali*" fa riferimento al potenziale impatto che i sistemi di intelligenza artificiale possono avere non solo nel mondo "reale", del quale fanno parte anche gli aspetti virtuali purché connessi a un utilizzo operativo "concreto".

La norma si applica pertanto se l'uso dei sistemi coinvolge:

Ambienti fisici

Luoghi e contesti materiali in cui l'IA può operare direttamente o indirettamente. Ad esempio, in un ambiente di lavoro, un sistema di IA potrebbe influenzare l'ambiente fisico rilevando condizioni di pericolo, monitorando lo stato delle attrezzature o gestendo processi industriali complessi.
L'influenza sugli ambienti fisici riguarda anche l'interazione con macchinari, impianti o strutture, il miglioramento della sicurezza, la previsione di incidenti o la gestione di situazioni di emergenza.

Ambienti virtuali

Contesti digitali o informatici, come la gestione dei dati, la simulazione di scenari o l'ottimizzazione di processi tramite software, dove l'intelligenza artificiale può elaborare informazioni, fornire previsioni o prendere decisioni che influenzano, ad esempio, l'efficienza operativa di un'azienda o la sicurezza informatica.

L'attenzione al punto dell'*influenza reale* appare determinante per l'applicazione della norma, la cui applicazione potrebbe ad esempio restare estranea agli utilizzi nell'ambito di ambienti di gioco e di pura simulazione.

La gestione pratica degli adempimenti normativi comporterà tuttavia la soluzione di non pochi problemi, perché qualunque sistema comprende aspetti di interazione o interfaccia che lo rendono in grado di interagire con un contesto fisico e "umano", non fosse altro per problemi di *ergonomia*, possibile accesso a *dati personali* degli utilizzatori, incidenza sugli *aspetti attentivi* e di *interazione con l'ambiente*[2] ecc.

2. Il giocatore che indossa ad esempio un visore VR è esposto a specifici rischi di caduta o di impatto con oggetti ecc.

AI Act e Testo Unico Sicurezza

Confrontando l'ambito soggettivo e oggettivo del Testo Unico Sicurezza e dell'AI Act, emergono alcune possibili sovrapposizioni, in particolare per quanto riguarda i datori di lavoro che utilizzano sistemi di intelligenza artificiale negli ambienti operativi delle organizzazioni.

Esaminiamo le diverse situazioni pratiche.

Ambito soggettivo

Testo Unico Sicurezza (D.Lgs. 81/2008)

Il soggetto principale è il datore di lavoro, che ha la responsabilità primaria di garantire la salute e la sicurezza dei lavoratori all'interno dell'impresa o dell'organizzazione. Gli obblighi si estendono anche a figure come dirigenti, preposti, medici competenti e altre parti coinvolte nella prevenzione degli infortuni sul lavoro.

AI Act (Regolamento UE 2024/1689)

Il regolamento si applica a sviluppatori, fornitori e utenti di sistemi di intelligenza artificiale. Gli utenti includono imprese e organizzazioni che utilizzano l'IA per fini professionali, il che significa che anche i datori di lavoro potrebbero essere inclusi se adottano sistemi di IA nei processi aziendali. Gli obblighi variano in base al livello di rischio associato ai sistemi di IA utilizzati. Risulta centrale il ruolo del ***deployer***.

Ambito oggettivo

Testo Unico Sicurezza

L'ambito oggettivo del decreto si concentra sulla tutela della salute e della sicurezza nei luoghi di lavoro. Regola misure preventive, la gestione dei rischi, la sorveglianza sanitaria e l'adozione di strumenti idonei per evitare incidenti o danni alla salute. Include anche disposizioni relative all'uso di attrezzature e tecnologie che possono impattare sulla sicurezza dei lavoratori.

AI Act

Regola lo sviluppo, la messa in commercio, l'utilizzo e la supervisione dei sistemi di IA, in particolare quelli classificati come "ad alto rischio". I sistemi ad alto rischio comprendono quelli utilizzati in settori come la salute, la sicurezza pubblica, la gestione delle infrastrutture e i trasporti,

tra gli altri. Il regolamento, per garantire che l'IA non crei danni fisici o psicologici agli individui, impone obblighi specifici, come la valutazione dei rischi, la documentazione tecnica e la trasparenza.

Possibili sovrapposizioni di obblighi per il datore di lavoro

Il datore di lavoro, come principale soggetto obbligato in base al Testo Unico Sicurezza, può trovarsi obbligato anche a rispettare l'AI Act nei casi in cui utilizzi sistemi di IA che rientrano nelle categorie "ad alto rischio".

Di seguito alcuni ambiti in cui queste sovrapposizioni di obblighi possono verificarsi.

Sorveglianza e valutazione dei lavoratori tramite IA

Se il datore di lavoro utilizza sistemi di IA per monitorare i lavoratori (ad esempio, IA che analizzano le prestazioni o valutano i rischi legati alla salute e sicurezza), tali sistemi potrebbero essere classificati come ad alto rischio sotto l'AI Act. In questo caso, il datore di lavoro dovrà assicurarsi che i sistemi di IA rispettino i requisiti di trasparenza, non discriminazione e protezione dei dati personali, oltre agli obblighi di sicurezza sul lavoro stabiliti dal Testo Unico.

Utilizzo di robot o macchinari intelligenti

In ambiti come la produzione industriale o la logistica, dove i datori di lavoro utilizzano robot o attrezzature dotate di IA per migliorare l'efficienza e la sicurezza, questi sistemi possono ricadere sotto la categoria di IA ad alto rischio. Se tali sistemi impattano direttamente sulla sicurezza dei lavoratori (ad esempio, macchine autonome utilizzate per il trasporto di materiali o robot collaborativi), il datore di lavoro dovrà rispettare sia le norme del Testo Unico, sia quelle dell'AI Act. Questo include l'obbligo di valutare i rischi per la salute e la sicurezza associati all'utilizzo delle tecnologie intelligenti.

Sistemi di IA nella gestione delle emergenze o prevenzione degli incidenti

Se un datore di lavoro impiega sistemi di IA per la gestione delle emergenze (ad esempio, IA che prevedono potenziali incidenti o ottimizzano i protocolli di evacuazione), tali sistemi potrebbero essere considerati ad alto rischio. Di conseguenza, oltre a rispettare le disposizioni del Testo Unico in materia di gestione delle emergenze, il datore di lavoro dovrà conformarsi ai requisiti di trasparenza, sicurezza e controllo imposti dall'AI Act.

L'utilizzo di sistemi di IA nel contesto lavorativo può influenzare direttamente la sicurezza dei lavoratori, soprattutto se i sistemi sono utilizzati per automatizzare processi pericolosi, monitorare i rischi o assistere nelle decisioni relative alla salute e sicurezza. In questi casi, il datore di lavoro ha un doppio obbligo: da un lato deve garantire la sicurezza dei lavoratori secondo quanto stabilito dal Testo Unico Sicurezza, dall'altro deve rispettare le normative dell'AI Act relative alla sicurezza e all'affidabilità dei sistemi di IA ad alto rischio.

Il ruolo del "deployer" nell'AI Act

Nell'ambito dell'AI Act, il termine *deployer* (art. 3, comma 4) si riferisce a *qualsiasi persona fisica o giuridica*, inclusi autorità pubbliche, agenzie o altre organizzazioni, *che utilizza un sistema di intelligenza artificiale sotto la propria autorità*, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

In molti contesti operativi, la definizione di *deployer* nell'AI Act potrebbe coincidere, nell'ambito di tutte le organizzazioni che impiegano personale, con quella di "datore di lavoro" precisata nel Testo Unico Sicurezza.
Il *deployer* è dunque il soggetto che introduce, gestisce o sfrutta un sistema di IA per uno scopo specifico, che può includere attività commerciali, operative o amministrative. Ciò significa che il *deployer* non è necessariamente lo sviluppatore o il produttore del sistema di IA, ma è chiunque dispone l'utilizzo in un determinato contesto operativo o aziendale. Ad esempio, un'azienda che utilizza un sistema di IA per il reclutamento del personale, la gestione della produzione o la sorveglianza sul luogo di lavoro, si qualifica come *deployer* di quel sistema; dal punti di vista legale, il *deployer* sarà anzitutto il legale rappresentante, la cui posizione di garanzia potrà eventualmente essere gestita tramite lo strumento di **deleghe**, ma mai completamente svuotata restando in ogni caso salvi gli obblighi di diligenza nella scelta dei delegati e nella vigilanza sul loro operato.

È importante notare che il *deployer* ha una serie di obblighi specifici previsti dall'AI Act, che includono la gestione del rischio, la trasparenza nell'uso del sistema di IA e la conformità alle norme relative alla protezione dei dati e ai diritti fondamentali.
Gli obblighi del *deployer* sono pensati per garantire l'uso sicuro e responsabile dei sistemi di intelligenza artificiale, in particolare di quelli classificati come "ad alto rischio", con lo scopo di proteggere i diritti fondamentali, garantire la sicurezza e la trasparenza e prevenire i danni derivanti dall'uso inappropriato dell'IA.

Ricordiamo in particolare i seguenti obblighi del *deployer*:

1. Monitoraggio e gestione del rischio

Il *deployer* deve garantire che il sistema di intelligenza artificiale venga utilizzato in modo sicuro e affidabile, con particolare attenzione ai rischi per la sicurezza, la salute e i diritti fondamentali. Ciò implica una costante valutazione e monitoraggio del sistema durante tutto il suo ciclo di vita operativo, verificando che non insorgano nuovi rischi o vulnerabilità.

2. Trasparenza e informazione

Il *deployer* ha l'obbligo di assicurare che gli utenti o le persone impattate dal sistema di IA siano adeguatamente informati.

Questo include:

Chiarezza sull'uso dell'IA
Le persone coinvolte o impattate dall'uso del sistema di IA devono essere informate del fatto

che stanno interagendo con un sistema automatizzato.
Ciò è particolarmente rilevante nei contesti in cui i sistemi di IA prendono decisioni che potrebbero avere un impatto significativo sugli individui.

Informazioni sull'output del sistema

Deve essere chiaro come e perché il sistema produce determinati risultati, e gli utenti devono essere consapevoli dei limiti e delle capacità del sistema.
Tenuto conto degli aspetti non deterministici presenti nei sistemi di IA, gli adempimenti informativi relativi all'output sono ovviamente non banali.

3. Misure di sicurezza

Il *deployer* è responsabile della protezione del sistema di IA contro l'uso improprio o attacchi che potrebbero alterarne il funzionamento. Tale obbligo implica l'adozione di misure di sicurezza tecniche e organizzative per prevenire eventuali incidenti o abusi che potrebbero compromettere la sicurezza o i diritti degli individui coinvolti.

4. Documentazione e registrazione

Il *deployer* deve mantenere una documentazione accurata e completa riguardante il funzionamento del sistema di IA, inclusi i dati utilizzati e le decisioni prese dal sistema. In particolare, per i sistemi ad alto rischio, il *deployer* deve conservare una documentazione tecnica che consenta alle autorità di vigilanza di verificare la conformità con l'AI Act e altre normative pertinenti.

5. Supervisione umana

Il *deployer* deve garantire che i sistemi di IA ad alto rischio siano soggetti a supervisione umana adeguata. Questo significa che le decisioni critiche prese dall'IA devono essere monitorate o verificate da esseri umani, e deve essere possibile per le persone intervenire o modificare i risultati del sistema, se necessario.

6. Limitazione e mitigazione dei danni

Nel caso in cui un sistema di IA provochi danni fisici o psicologici o pregiudichi i diritti fondamentali, il *deployer* è obbligato a intervenire tempestivamen-

te per limitare i danni. Deve adottare misure correttive, interrompere l'uso del sistema se necessario, e segnalare eventuali problemi alle autorità competenti.

7. Conformità con la protezione dei dati

Se il sistema di IA gestisce o tratta dati personali, il *deployer* deve garantire la conformità con le normative esistenti sulla protezione dei dati, come il Regolamento generale sulla protezione dei dati (GDPR). Questo include obblighi legati alla minimizzazione dei dati, alla protezione della privacy e alla gestione sicura delle informazioni sensibili.

8. Responsabilità legale

Il *deployer* è legalmente responsabile per l'uso del sistema di IA sottoposto alla sua autorità. Se il sistema di IA causa danni o violazioni di diritti, il *deployer* può essere ritenuto responsabile e può essere soggetto a sanzioni, obbligo di risarcimenti o altre conseguenze legali, a seconda della natura delle violazioni.

9. Formazione e competenza

Il *deployer* deve assicurarsi che il personale coinvolto nell'uso e supervisione dei sistemi di IA sia adeguatamente formato. Questa formazione deve riguardare non soltanto il funzionamento tecnico del sistema, ma anche le implicazioni etiche e legali del suo utilizzo, specialmente in contesti critici o ad alto rischio.

10. Valutazione d'impatto e aggiornamento continuo

Per i sistemi di IA ad alto rischio, il *deployer* deve effettuare regolari valutazioni d'impatto per garantire che il sistema continui a operare nel rispetto delle normative vigenti. Se emergono nuove minacce, il *deployer* è tenuto a modificare o aggiornare il sistema, includendo nuove misure di sicurezza o procedure di mitigazione.

Le date per l'entrata in vigore degli obblighi previsti dall'AI Act

L'AI Act è entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione Europea, avvenuta il 12 luglio 2024.

L'applicazione generale è prevista dal **2 agosto 2026**, tuttavia:

- I capi I (Disposizioni generali) e II (Pratiche di IA vietate) si applicano a decorrere dal **2 febbraio 2025**.
- Il capo III, sezione 4 (Autorità di notifica e organismi notificati), il capo V (Modelli di IA per finalità generali), il capo VII (Governance), il capo XII (Sanzioni) e l'articolo 78 (Riservatezza) si applicano a decorrere dal **2 agosto 2025**, a eccezione dell'articolo 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali).
- L'articolo 6, paragrafo 1 (Regole di classificazione per i sistemi IA ad alto rischio) e i corrispondenti obblighi di cui al regolamento si applicano a decorrere dal **2 agosto 2027**.

Il regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.