

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

Questo articolo è stato originariamente creato per la newsletter dedicata a Sicurezza e Lavoro di ARS Edizioni.

L'applicazione del nuovo Regolamento (UE) 2023/1230 sta generando un confronto interpretativo significativo all'interno del comitato incaricato di redigere le linee guida ufficiali, di cui faccio parte. Al centro della discussione si colloca una questione tecnicamente complessa ma dalle implicazioni pratiche rilevanti: quand'è che una macchina che utilizza tecniche di machine learning deve essere sottoposta alla valutazione obbligatoria di un ente notificato?

Il Regolamento Macchine introduce nell'allegato I due categorie di prodotti tecnologicamente avanzati che richiedono la certificazione tramite ente terzo: si tratta dei *componenti di sicurezza e delle macchine che incorporano sistemi con comportamento totalmente o parzialmente auto-evolutivo basato su approcci di machine learning per garantire funzioni di sicurezza*.

La formulazione normativa sta però rivelando margini di interpretazione significativi, che dividono gli esperti coinvolti nella stesura delle linee guida applicative.

Il dibattito

All'interno del Subgroup 2 del comitato editoriale, responsabile di stendere

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

le linee guida relative alle funzioni di sicurezza guidate da intelligenza artificiale, si è sviluppato uno scontro interpretativo tra i membri attivi del gruppo di lavoro, tra cui chi scrive.

La questione riguarda specificatamente le macchine che vengono addestrate utilizzando tecniche di machine learning durante la fase di sviluppo, ma che successivamente, una volta immesse sul mercato, mantengono un comportamento statico e deterministico senza ulteriori evoluzioni o apprendimenti.

I fronti dello scontro vedono, da una parte, principalmente i membri attivi francesi, a cui si oppongono in particolare i membri attivi tedeschi e italiani.

Secondo la posizione sostenuta dai membri attivi francesi, tutte le macchine addestrate con l'intelligenza artificiale – anche quelle che di fatto non la utilizzano nel normale funzionamento in fabbrica – dovrebbero rientrare nell'allegato I e quindi richiedere obbligatoriamente la validazione da parte di un ente notificato. Il criterio proposto si baserebbe, quindi, sul metodo di sviluppo utilizzato: se durante la progettazione è stato impiegato il machine learning, la macchina dovrebbe essere classificata come pericolosa ai sensi del Regolamento, indipendentemente dal suo comportamento durante l'utilizzo effettivo.

Questa interpretazione viene proposta come tutela aggiuntiva per l'utilizzatore finale, ma appare in realtà una forzatura del testo normativo che rischia di estendere arbitrariamente gli obblighi certificativi ben oltre le intenzioni del legislatore. Si tratta, naturalmente, di una posizione che ha radici culturali, nel senso che storicamente la legislazione francese sulle

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

macchine industriali ha sempre spinto per la certificazione tramite ente dei macchinari considerati in qualche modo pericolosi.

La posizione italiana, tedesca e della maggioranza degli altri membri attivi sostiene invece un'interpretazione più fedele alla lettera (e allo spirito) del Regolamento, secondo cui l'obbligo di certificazione tramite ente notificato deve applicarsi esclusivamente ai prodotti che manifestano un comportamento auto-evolutivo dopo l'immissione sul mercato. Se l'intelligenza artificiale viene utilizzata soltanto nella fase di sviluppo e addestramento, mentre durante l'esercizio la macchina opera con parametri fissi e comportamento deterministico, non si configurerebbe dunque l'auto-evoluzione che giustifica l'inserimento nell'allegato I.

Il testo normativo è infatti chiaro: le definizioni 5 e 6 dell'allegato I, parte A, parlano di prodotti *“con comportamento totalmente o parzialmente auto-evolutivo”* che utilizzano approcci di machine learning *“per garantire funzioni di sicurezza”*. Insomma, l'enfasi è sul comportamento del prodotto durante l'uso, non sulle tecniche impiegate durante lo sviluppo.

Il problema della verificabilità

C'è da aggiungere che l'interpretazione francese presenta un difetto fondamentale che ne mina alla radice l'applicabilità: l'acquirente di una macchina non dispone di alcun mezzo per verificare le modalità con cui essa è stata sviluppata e costruita. L'utilizzatore finale non può infatti

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

accertare se durante la fase di progettazione siano stati utilizzati algoritmi di machine learning per addestrare sistemi di controllo, né può distinguere tra un sistema addestrato offline con parametri poi fissati e un sistema effettivamente capace di apprendimento continuo durante l'esercizio.

A parer mio (e della "fazione" italo-tedesca) questa opacità risulta radicalmente incompatibile con i principi fondamentali della marcatura CE. Il sistema di conformità europeo si basa sulla valutazione del *prodotto come immesso sul mercato e utilizzato nelle condizioni d'uso previste e ragionevolmente prevedibili*, non su caratteristiche interne al processo produttivo che rimangono invisibili all'utilizzatore finale.

Legare l'obbligo di certificazione tramite ente notificato al metodo di sviluppo anziché al comportamento effettivo del prodotto crea una situazione paradossale e inaccettabile. Ad esempio, due macchine identiche nel comportamento operativo potrebbero trovarsi in regimi normativi completamente diversi in base a scelte di sviluppo interne al fabbricante, invisibili e non verificabili dall'esterno.

Come può l'acquirente esercitare il proprio diritto a verificare la conformità? Come possono gli organi di vigilanza accertare il rispetto degli obblighi? La risposta è semplice: non possono, perché il criterio proposto dai francesi non è verificabile.

Questo non è un dettaglio tecnico marginale. Pretendere di applicare obblighi certificativi sulla base di caratteristiche non verificabili mina la credibilità dell'intero sistema di marcatura CE e introduce elementi di arbitrarietà difficilmente compatibili con i principi di certezza del diritto e

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

trasparenza del mercato.

A questo proposito, non posso che consigliare [l'analisi condotta da Stefano Boy](#), ispettore dell'Ispettorato Nazionale del Lavoro e membro del gruppo editoriale delle linee guida del Regolamento macchine, che evidenzia come una lettura combinata delle definizioni dell'allegato I, dei considerando (32) e (55) e dei requisiti dell'allegato III orienti decisamente verso l'interpretazione basata sul comportamento post-commercializzazione.

Stefano Boy fornisce anche un esempio concreto che chiarisce la questione, quello di un sistema di controllo di stabilità per un escavatore idraulico che utilizza una rete neurale artificiale addestrata offline su dati di simulazione e registrazioni reali. Una volta addestrata, la rete opera solo come mappatura deterministica input-output, senza alcun aggiornamento dei pesi durante il funzionamento; in pratica, il sistema è incapace di apprendere o evolvere dopo la messa in servizio.

Secondo l'interpretazione italiana e tedesca, questo prodotto non dovrebbe rientrare nell'allegato I perché non presenta comportamento auto-evolutivo durante l'uso. Secondo l'interpretazione francese, dovrebbe invece essere sottoposto a certificazione tramite ente notificato perché sviluppato con tecniche di machine learning, anche se tale caratteristica non si manifesta durante il ciclo di vita operativo.

Conseguenze pratiche dell'interpretazione francese

L'intervento obbligatorio dell'ente notificato non è solo una formalità burocratica trascurabile: esso comporta costi significativi, tempistiche di certificazione più lunghe e l'obbligo di rispettare norme tecniche armonizzate – che, per questi prodotti avanzati, al momento non esistono ancora in forma compiuta. Estendere questo obbligo anche a prodotti con comportamento statico in esercizio significa, dunque, imporre oneri sproporzionati rispetto al livello di rischio effettivo e penalizzare l'innovazione tecnologica senza ottenere corrispondenti benefici in termini di sicurezza!

La differenza tra certificazione tramite ente notificato e autocertificazione incide profondamente sulle dinamiche di mercato, sui livelli di tutela effettiva e sulla concorrenza tra operatori, anche a livello internazionale. Un'interpretazione estensiva, che include nell'allegato I anche prodotti che il Regolamento non intendeva inserire, rischia di creare distorsioni competitive, appesantire inutilmente le procedure certificative e ostacolare lo sviluppo europeo di tecnologie innovative che, pur utilizzando machine learning in fase di sviluppo, offrono in esercizio comportamenti perfettamente deterministici e verificabili.

Macchinari addestrati con l'intelligenza artificiale ed enti notificati: il dibattito interpretativo sul nuovo Regolamento Macchine

In sintesi...

Il dibattito in corso nel comitato editoriale richiede una scelta di responsabilità. L'interpretazione italiana e tedesca rispetta la lettera del Regolamento, mantiene coerenza sistemica con l'impianto normativo europeo e preserva *il principio fondamentale della verificabilità* che sta alla base della marcatura CE. L'interpretazione francese, pur presentata come tutela aggiuntiva per il consumatore, rappresenta una forzatura del testo che introduce *criteri non verificabili e oneri sproporzionati*.

La questione non è accademica. Le linee guida che verranno adottate definiranno le regole per i prossimi anni nell'ambito cruciale dell'intelligenza artificiale applicata alla sicurezza delle macchine. È fondamentale che queste regole siano tecnicamente rigorose ma anche praticamente applicabili.