AI Act e macchinari industriali: come si applica il regolamento sull'intelligenza artificiale al mondo delle fabbriche?

A pochi mesi dall'entrata in vigore del Regolamento europeo sull'Intelligenza Artificiale (AI Act) cerchiamo di capire meglio gli impatti della nuova normativa nel mondo dei macchinari industriali, mettendola anche il relazione al nuovo Regolamento macchine 2023. (Ultimo aggiornamento: novembre 2024)

Cos'è l'AI Act, quando è entrato in vigore e quando diventa obbligatorio

Il 1° agosto 2024 è entrato in vigore l'AI Act, ovvero il Regolamento europeo sull'Intelligenza Artificiale. Tuttavia, come per tutte le normative europee, è previsto un periodo di transizione in cui il regolamento è in vigore ma non è ancora obbligatorio adottarlo. La data di piena applicazione dell'AI Act è infatti il 2 agosto 2026, due anni dopo la prima entrata in vigore.

Fanno eccezione alcune disposizioni specifiche che presentano tempistiche diverse, ovvero:

- I divieti, le definizioni e le disposizioni relativi all'alfabetizzazione in materia di IA si applicheranno 6 mesi dopo l'entrata in vigore, il 2 febbraio 2025;
- Le norme in materia di governance e gli obblighi per l'IA per finalità generali diventano applicabili 12 mesi dopo l'entrata in vigore, il 2 agosto 2025;
- Gli obblighi per i sistemi di IA ad alto rischio elencati nell'allegato II si applicano 36 mesi dopo l'entrata in vigore, il 2 agosto 2027.

© 2022 - Tutti i diritti sono riservati

AI Act e macchinari industriali: come si applica il regolamento sull'intelligenza artificiale al mondo delle fabbriche?

Con l'AI Act, l'Unione Europea ha provato in qualche modo a regolamentare un campo completamente nuovo, quello dell'intelligenza artificiale. Le finalità dei legislatori sarebbero quelle di garantire:

- La sicurezza, facendo sì che i prodotti che utilizzano l'intelligenza artificiale non danneggino le persone;
- La trasparenza, assicurando che gli utilizzatori possano capire come funziona l'AI e su quali basi vengono prese le decisioni.

[A questo link trovi il testo completo del regolamento in tutte le lingue dell'UE]

Il condizionale che ho usato fin qui è d'obbligo, perché l'AI Act rappresenta appunto un tentativo dell'Unione Europea di avventurarsi in un campo non solo recentissimo, ma anche in costante espansione ed evoluzione.

Per provare a mappare e normare questo territorio sconosciuto, i legislatori europei hanno tirato fuori dal cassetto uno strumento che conosciamo molto bene: la certificazione CE.

In altre parole, i prodotti che utilizzano l'intelligenza artificiale e che vengono prodotti o venduti nell'Unione Europea dovranno (o dovrebbero) rispettare gli standard di sicurezza europei – compresi quelli sulla valutazione del tipo di rischio – per ottenere la certificazione CE che li rende commerciabili in Europa.

Forse qualcuno ricorderà che già nel Regolamento Macchine si iniziava a parlare di intelligenza artificiale, ma tutti aspettavamo la versione definitiva del regolamento sull'intelligenza artificiale per capire meglio come gestire

© 2022 - Tutti i diritti sono riservati

gli aspetti relativi alla sicurezza.

E quindi ora che è stato approvato l'AI Act è tutto a posto, giusto?

Non proprio. Come cercherò di spiegarti nei prossimi paragrafi, non è ancora del tutto chiaro come applicare la nuova norma, almeno per quanto riguarda i macchinari industriali che sfruttano l'intelligenza artificiale.

Ma partiamo dall'inizio. Quand'è che possiamo parlare di intelligenza artificiale nell'ambito dei macchinari industriali?

> Leggi anche: Nuovo Regolamento Macchine 2023/1230: cosa cambia rispetto alla Direttiva Macchine?

Cos'è l'intelligenza artificiale? Quando si può parlare di intelligenza artificiale rispetto ai macchinari industriali?

Nell'ultimo anno mi è capitato spesso che, mentre visitavo una fabbrica, i miei clienti mi dicessero tutti esaltati: "*Guarda, stiamo creando questo prodotto/attivando questo macchinario che usa l'intelligenza artificiale*".

Onestamente, io mi sono spesso sentito un po' a disagio. Eh sì, perché nell'ambito dei macchinari industriali non è facile capire quando possiamo davvero parlare di intelligenza artificiale…

© 2022 - Tutti i diritti sono riservati

Proviamo a leggere allora la definizione di intelligenza artificiale che è stata inserita nell'AI Act:

«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.
[Articolo 3 del Regolamento UE 2024/1689]

Gli elementi chiave per definire un sistema di IA sono quindi:

- Una certa autonomia (si parla di livelli variabili);
- L'adattabilità dopo la diffusione (la famosa autoevoluzione);
- La generazione di output – previsioni, contenuti, raccomandazioni o decisioni – che influenzano l'ambiente circostante, sia esso reale o digitale.

A fronte di tutti i discorsi che si fanno oggi sull'IA, bisogna considerare che questa è, per ora, l'unica definizione di intelligenza artificiale inserita in un quadro normativo.

Il problema è che questa definizione è molto generica. Tanto per dirne una, qualsiasi macchina genera degli output sulla base di input, ad esempio sulla base di vincoli e lavorazioni che abbiamo determinato in precedenza.

Insomma, il rischio è che con questa definizione si possano considerare sistemi di intelligenza artificiale anche dispositivi che esistevano ben prima che si parlasse di AI!

© 2022 - Tutti i diritti sono riservati

Qualche esempio? I magazzini automatizzati che decidono quali articoli prendere e con quale percorso, dove l'operatore ha soltanto un ruolo di supervisione. Oppure le linee di imbottigliamento che in base ad una serie di dati (il tasso di umidità dell'aria, la temperatura ecc.) decidono come gestire la colorazione.

Ma possiamo veramente parlare di intelligenza artificiale per questi tipi di macchinari?

Dopo aver approfondito l'argomento ascoltando vari esperti del settore, la mia risposta personale è: sì e no.

Nei casi che ho citato, così come nella definizione dell'Unione Europea, non si trova traccia di un elemento essenziale delle intelligenze artificiali: l'elaborazione di grandi quantità di dati su base statistica per prendere decisioni.

In questo senso, le forme di intelligenza artificiale che sono presenti oggi nelle fabbriche, sono necessariamente imperfette e immature, per il semplice motivo che *non hanno abbastanza dati a disposizione per prendere decisioni sensate*. Tra cinque anni, probabilmente, questo problema non ci sarà più. Ad oggi, nel 2024, bisogna ancora tenerne conto.

Questo è il motivo per cui, nell'ambito fabbrica, possiamo parlare di intelligenze artificiali solo limitatamente.

Ti potrebbe interessare anche questo articolo: "Chatbot e intelligenza artificiale per l'assistenza tecnica dei macchinari

© 2022 - Tutti i diritti sono riservati

industriali”

Classificazioni di rischio nell’AI Act e macchinari industriali

© 2022 - Tutti i diritti sono riservati

AI Act e macchinari industriali: come si applica il regolamento sull'intelligenza artificiale al mondo delle fabbriche?



Come ho accennato prima, nel Regolamento Macchine si parla di macchine che utilizzano l'intelligenza artificiale ma senza specificare come si devono valutare i rischi di questi macchinari.

© 2022 - Tutti i diritti sono riservati

AI Act e macchinari industriali: come si applica il regolamento sull'intelligenza artificiale al mondo delle fabbriche?

Nel regolamento europeo sull'intelligenza artificiale si stabiliscono 4 diversi livelli di rischio:

1) Rischio inaccettabile

Comprende i sistemi che violano i diritti umani e i valori fondamentali dell'Unione Europea, quali ad esempio la sorveglianza di massa. I sistemi AI di questo tipo sono vietati all'interno dell'Unione Europea.

2) Alto rischio

Comprende sistemi che potrebbero causare danni significativi in caso di malfunzionamento: sistemi di identificazione biometrica e riconoscimento facciale, sistemi di valutazione del credito e scoring, chatbot medici, sistemi di guida autonoma…

3) Rischio limitato

Comprende sistemi che presentano un rischio minore, come chatbot generici o software di elaborazione delle immagini. Il rischio è associato in questo caso alla potenziale mancanza di trasparenza. Nel caso del chatbot, ad esempio, gli utenti devono essere informati che non stanno interagendo con un essere umano, così come deve essere chiaro che le immagini elaborate dal software non sono fotografie reali.

4) Rischio minimo

Si tratta di sistemi con un impatto minimo o nullo sui diritti o la sicurezza delle persone. La loro funzione principale è aiutare a organizzare le attività

© 2022 - Tutti i diritti sono riservati

quotidiane senza incidere su decisioni o attività di rilevanza critica. Un'app di gioco con l'IA per il cellulare potrebbe ad esempio rientrare in questa categoria.

Proviamo ad analizzare meglio queste categorie per capire dove potrebbero rientrare i nostri macchinari industriali.

Nella prima categoria, rischio inaccettabile, sicuramente non rientrano le macchine. Qui si parla di intelligenze artificiali in grado di influenzare le masse, di utilizzo dei dati biometrici e altre tematiche importantissime, ma che nulla hanno a che fare con le fabbriche.
Insomma, per i macchinari non esiste rischio inaccettabile.

Passiamo alle tecnologie ad alto rischio, ovvero i sistemi che possono causare danni significativi in caso di malfunzionamento. In questi casi entrano in gioco questioni di sicurezza e affidabilità del software, che in parte vengono già applicate in campo medicale, dove è necessario essere certi delle diagnosi e dei risultati. Pensate all'importanza di avere risultati certi quando si fa, ad esempio, un'ecografia morfologica in cui si scoprono le malformazioni del feto.

I sistemi di intelligenza artificiale considerati ad alto rischio saranno sottoposti ad una serie di misure di sicurezza più rigorose: dovranno essere certificati da enti esterni, verranno inseriti in un registro pubblico e dovranno essere sottoposti a controlli periodici in seguito all'immissione sul mercato. Inoltre, le richieste relative a sicurezza e affidabilità dei dati, tracciabilità dei risultati e documentazione sono chiaramente più severe.

E i nostri macchinari industriali?

© 2022 - Tutti i diritti sono riservati

AI Act e macchinari industriali: come si applica il regolamento sull'intelligenza artificiale al mondo delle fabbriche?

Se ci limitiamo alla definizione generale, i macchinari potrebbero rientrare in questa categoria: una macchina o un componente di sicurezza può causare un infortunio o addirittura una morte accidentale, quindi potrebbe essere considerata ad alto rischio. Tuttavia, nelle varie tipologie di esempi inserite nell'allegato III dell'AI Act (quello che tratta i sistemi ad alto rischio) non si parla mai di macchinari industriali.

Sistemi a rischio limitato. In questa categoria rientrano le IA che già tutti conosciamo e utilizziamo: chat GTP che ci risponde alle domande, l'IA di Linkedin che elabora un'immagine sulla base del titolo di un messaggio eccetera. Anche qui, tuttavia, l'AI Act non fa riferimenti specifici a macchinari, e lo stesso vale per i sistemi a rischio minimo.

Inizi a capire anche tu qual è il problema dell'AI Act?

Diciamolo chiaro e tondo: in questo nuovo regolamento europeo i macchinari non compaiono affatto. Non solo, non si parla nemmeno di oggetti che utilizzano la tecnologia!

Come classifichiamo la lavatrice che usa l'AI per suggerirti la migliore modalità di lavaggio?
E il robottino aspirapolvere che individua in modo intelligente gli ostacoli e capisce se sta passando su un tappeto o sul parquet?

Queste sono tutte applicazioni dell'intelligenza artificiale che sono già tra di noi, che si trovano in qualsiasi negozio di elettrodomestici. Ma nell'AI Act tutta l'attenzione si è concentrata sui sistemi di intelligenza artificiale più complessi (e anche più pericolosi) tralasciando le applicazioni più immediate. Certo, verrebbe da dire che con questi oggetti il rischio sarà

© 2022 - Tutti i diritti sono riservati

limitato o minimo, ma qui entriamo nella libera interpretazione della norma…

Lo stesso identico discorso vale per i macchinari. Nell'AI Act non sono presi in considerazione, ad esempio, i software di assistenza dei macchinari, che già esistono e si usano. Inoltre, al momento mancano completamente le norme tecniche necessarie per produrre e classificare il rischio dei macchinari o delle componenti che usano l'IA nelle fabbriche.

Regolamento macchine e macchinari che usano l'intelligenza artificiale

Visto che nell'AI Act non ci sono riferimenti specifici a come trattare i macchinari o le componenti che usano l'intelligenza artificiale, dobbiamo necessariamente andare a vedere i regolamenti di prodotto.

Nel caso dei macchinari, il riferimento fondamentale è il Regolamento macchine 2023/1230.

Effettivamente il Regolamento macchine (approvato prima dell'AI Act) si occupa di intelligenza artificiale, anche se la chiama sistema o comportamento autoevolutivo. Nel Regolamento macchine, in particolare, vengono citati:

- *Macchine che integrano, sistemi con un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza che non sono state immesse in modo indipendente sul mercato, solo per quanto riguarda*

© 2022 - Tutti i diritti sono riservati

tali sistemi.

- *Componenti di sicurezza dotati di un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza.*

Queste definizioni sono tratte dall'allegato I del Regolamento macchine, ovvero l'allegato che dettaglia macchinari e componenti considerati ad alto rischio e che devono necessariamente essere certificati CE da un ente notificato.

Detto in altre parole, un'interpretazione stringente del Regolamento macchine obbligherebbe tutti i macchinari e componenti che usano l'IA a ricevere la certificazione CE solo tramite ente notificato.

Il problema però è che non esistono norme UNI, CEI, ISO o qualsiasi altra norma tecnica che spiega come certificare un software di intelligenza artificiale. E i RES indicati nel Regolamento macchine sono troppo generici rispetto a questo ambito, quindi non risultano funzionali a questo tipo di valutazione.

E quindi come possono fare i consulenti di sicurezza come me, chi lavora negli enti notificati o gli impiegati ministeriali che devono controllare le certificazioni dei macchinari o componenti che utilizzano l'AI?

Di fatto in questo momento (novembre 2024) non abbiamo gli strumenti per muoverci in questo senso.

Come si procede, allora?

© 2022 - Tutti i diritti sono riservati

Bisogna per forza di cose classificare i software di intelligenza artificiale non tanto come "componenti di sicurezza" ma come aventi "funzione di sicurezza".

Vediamo la differenza delle due definizioni nel Regolamento macchine:

- *«componente di sicurezza»: un componente fisico o digitale, compreso un software, di un prodotto rientrante nell'ambito di applicazione del presente regolamento, che è progettato o destinato ad espletare una funzione di sicurezza e che è immesso sul mercato separatamente, il cui guasto o malfunzionamento mette a repentaglio la sicurezza delle persone, ma che non è indispensabile per il funzionamento di tale prodotto, o per il quale componenti normali possono essere sostituiti per il funzionamento di tale prodotto;*
- *«funzione di sicurezza»: una funzione che serve a soddisfare una misura di protezione destinata a eliminare o, se ciò non è possibile, a ridurre un rischio, e che, se ha un guasto potrebbe comportare un aumento di tale rischio;*

Cosa significa questo, in soldoni?

Semplice: gli elementi che espletano una funzione di sicurezza non devono passare al vaglio di un ente notificato. La certificazione CE resta, come nella maggior parte dei casi, un'autocertificazione.

Il software IA che muove il robot automatizzato, l'intelligenza artificiale che serve per fare la manutenzione preventiva e predittiva alle valvole dell'oil e gas, il software documentale con AI che integra i manuali cartacei sono

© 2022 - Tutti i diritti sono riservati

tutti esempi di software che non vengono venduti separatamente, ma che sono integrati al macchinario o al componente. Di conseguenza possono essere esclusi dalla definizione di componenti di sicurezza ed essere considerati elementi che espletano funzioni di sicurezza.

Tutto chiaro fin qua?

Attenzione, però. Questa soluzione che sto indicando non è una scappatoia per rendere più semplice il processo di certificazione. *Semplicemente, sto constatando che allo stato attuale della normativa questa è l'unica soluzione possibile per arrivare a immettere sul mercato macchinari e componenti che utilizzano l'intelligenza artificiale.*

Quando arriveranno le norme tecniche, che sicuramente arriveranno, saremo tutti più sereni. I produttori avranno degli standard a cui attenersi, e chi si occupa di sicurezza avrà dei riferimenti precisi. Per ora, però, la situazione è questa.

Consideriamo anche che, per quanto abbiamo visto in precedenza, la maggior parte degli utilizzi dell'intelligenza artificiale in fabbrica va probabilmente a rientrare nella classificazione di rischio minimo dell'AI Act (classificazione che non richiede l'intervento di un ente certificato).

Nel Regolamento macchine, al contrario, ogni macchinario o componente di sicurezza con comportamento autoevolutivo viene automaticamente considerato ad alto tasso di pericolo e richiederebbe il passaggio dell'ente certificato.

Però il Regolamento macchine è uscito prima dell'AI Act. Quindi è l'AI Act

© 2022 - Tutti i diritti sono riservati

che dovrebbe fare da riferimento?

Insomma, c'è una contraddizione tra i due regolamenti che al momento non si sa bene come gestire o risolvere, se non utilizzando la strada della "funzione di sicurezza" che ti ho indicato prima.

In sintesi…

Ci siamo detti tante cose. Proviamo a riassumerle:

- L'AI Act non fa specifici riferimenti a come valutare il rischio di macchinari e componenti di macchinari che utilizzano l'intelligenza artificiale. È quindi necessario risalire alla normativa di prodotto, in questo caso il Regolamento macchine 2023;
- Il Regolamento macchine inserisce macchinari e componenti che usano l'IA nell'elenco di macchine che richiedono l'intervento di un ente terzo per ricevere la certificazione CE;
- Al momento non esistono norme tecniche a cui fare riferimento per la sicurezza dei software di AI utilizzati nelle fabbriche. Questo rende di fatto impossibile far certificare tali software da un ente esterno;
- Se i software che usano l'IA sono integrati al macchinario o al componente, è possibile considerarli come elementi che hanno una "funzione sicurezza" anziché "componenti di sicurezza". In questo caso si può seguire la strada dell'autocertificazione per la conformità CE.

Lo so, la materia è complessa e spinosa. Anche noi consulenti stiamo cercando di capire come muoverci e seguire le evoluzioni mentre

© 2022 - Tutti i diritti sono riservati

accadono. Da parte mia continuerò a trattare questo argomento qui sul blog e sul mio canale YouTube. Se hai domande, però, non esitare a contattarmi!

© 2022 - Tutti i diritti sono riservati