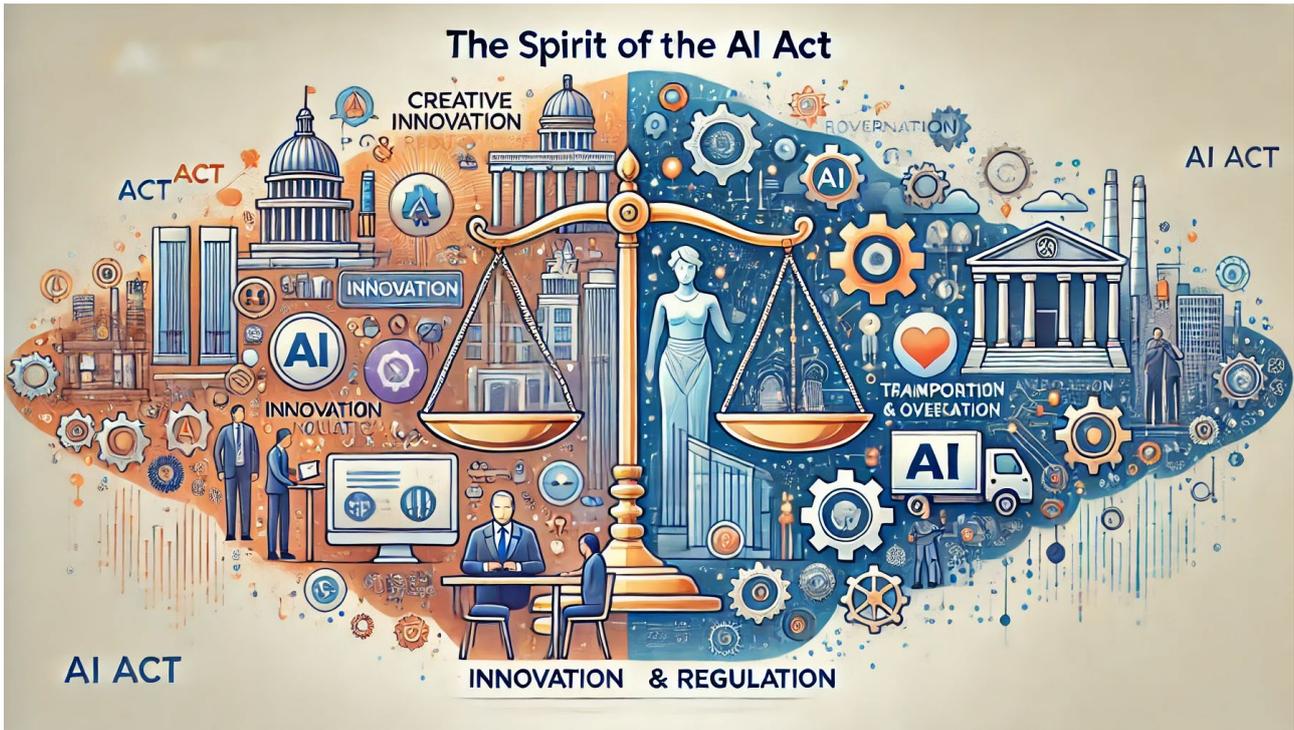


## Prodotti potenziati da sistemi di intelligenza artificiale: panoramica sulle relazioni fra AI Act, Regolamento Macchine e standard ISO/IEC 5469:2024

Primo nel suo genere, l'AI Act, la legge sull'intelligenza artificiale, è un Regolamento della UE approvato dal Consiglio il 21 maggio 2024 e che entrerà in vigore nella prima metà del 2027, così come il nuovo Regolamento Macchine che sostituisce la Direttiva Macchine 2006/42/CE. Nel frattempo a gennaio 2024 è stato pubblicato lo standard ISO/IEC 5469:2024



Abbiamo chiesto a ChatGPT 4o di generare con DALL E una "illustrazione che rappresenti lo spirito dell'AI Act". Ecco il risultato e il commento di ChatGPT 4o: *"Ho creato un'illustrazione che rappresenta lo spirito dell'AI Act. L'immagine mostra un equilibrio tra innovazione e regolamentazione, con una città futuristica in cui la tecnologia avanzata dell'IA è integrata nella vita quotidiana. Da un lato, ci sono soluzioni AI dinamiche che migliorano settori come la sanità, i trasporti e l'istruzione. Dall'altro, ci sono simboli di governance e supervisione, come bilance della giustizia, scudi e persone che collaborano in una riunione. Il tono complessivo è ottimistico e orientato al futuro, con una fusione armoniosa di tecnologia e valori umani"*.

\*\*\*

A eccezione del settore militare, l'AI Act si applica a tutti i settori e prende in esame tutti i tipi di intelligenza artificiale, pur concentrandosi su quelli caratterizzati da rischio non accettabile e da alto rischio.

Nell'articolo 1 comma 1 si afferma che lo scopo del regolamento è "promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile", "promuovere l'innovazione" e garantire nel contempo "un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente".

\*\*\*

Alle “**Misure a sostegno dell’innovazione**” sono dedicati gli articoli 57 e 58 dell’AI Act, che istituiscono “Spazi di sperimentazione normativa per l’IA” e illustrano le “Modalità dettagliate e funzionamento degli spazi di sperimentazione normativa per l’IA”, con particolare attenzione al fatto di “agevolare e accelerare l’accesso al mercato dell’Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up” e di coinvolgere in modo corale gli “attori pertinenti nell’ambito dell’ecosistema dell’IA”.

\*\*\*

**Cuore dell’IA Act è il concetto di rischio**, inteso come “combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso” e la conseguente categorizzazione di sistemi e modelli di intelligenza artificiale in base ai rischi che presentano per la salute, la sicurezza e i diritti fondamentali dei cittadini ex articolo 1 comma 1.

Dal punto di vista del rischio i sistemi di intelligenza artificiale sono categorizzati in sistemi di IA che presentano un rischio non accettabile; ad alto rischio; a rischio limitato; altri.

Ai **sistemi di IA a rischio limitato** l’AI Act dedica in particolare l’articolo 50 “Obblighi di **trasparenza** per i fornitori e gli utenti di determinati sistemi di IA”, stabilendo che “i sistemi di IA destinati a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo” (comma 1), che i “fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente” (comma 2), che i “deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un deep fake rendono noto che il contenuto è stato generato o manipolato artificialmente” e che i “deployer di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente”, a meno che esso non sia stato sottoposto a un processo di revisione umana o di controllo editoriale (comma 4).

Per gli **alti sistemi di IA**, cioè per quelli che non ricadono in una delle prime tre categorie (per esempio filtri antispam e giochi potenziati dall’intelligenza artificiale), l’AI Act non prevede obblighi, ma incoraggia l’**adozione volontaria** di quelle **buone pratiche** caldegiate per esempio nell’articolo 50 comma 7 e nell’articolo 56.

\*\*\*

I **sistemi di IA che presentano un rischio non accettabile sono vietati** dall’AI Act, ex articolo 5 “Pratiche di IA vietate”. Si tratta essenzialmente di **sistemi di IA che ledono i diritti fondamentali sanciti dalla Carta europea dei diritti fondamentali**, utilizzando tecniche subliminali o volutamente manipolative; sfruttando le vulnerabilità di persone o specifici gruppi; elaborando punteggi sociali; eseguendo valutazioni basate su profilazione o categorizzazione biometrica; inferendo emozioni di una persona nei luoghi di lavoro e istruzione, ecc.

\*\*\*

A partire dall’articolo 6 “Regole di classificazione per i sistemi di IA ad alto rischio”, l’AI Act si focalizza sui **sistemi di IA ad alto rischio**, declinati come **componenti di prodotti**, come **prodotti in quanto tali** o come **sistemi in quanto tali**.

L’articolo 6, comma 1 a) e b) stabilisce **un legame forte tra l’AI Act e il Regolamento Macchine**. Un **sistema di IA** è categorizzato come **ad alto rischio** “se è destinato a essere utilizzato come componente di

**sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto**, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'**allegato I'** (a).

Che cos'è un "**componente di sicurezza**" per l'AI Act? Nell'articolo 3, comma 14, esso è definito come "un componente di un prodotto o di un sistema che svolge una funzione di sicurezza per tale prodotto o sistema o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni".

Quali sono i **prodotti inclusi nell'allegato I** – Sezione A dell'AI Act? Anzitutto vi sono **quelli che sottostanno alla "Direttiva 2006/42/CE** del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24) [abrogata dal **regolamento sui prodotti macchina**]" . Vi sono poi giocattoli, imbarcazioni da diporto e alle moto d'acqua, ascensori e ai componenti di sicurezza per ascensori, agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, impianti a fune, dispositivi di protezione individuale, sugli apparecchi che bruciano carburanti gassosi e dispositivi medici.

Il comma 1 b) dell'articolo 6 stabilisce che "il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è **soggetto a una valutazione della conformità da parte di terzi** ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto...".

Ex articolo 6, comma 2 **sono inoltre "considerati ad alto rischio i sistemi di IA di cui all'allegato III"** e tutti quelli che effettuano "profilazione di persone fisiche" (comma 3).

Quali sono i sistemi di intelligenza artificiale listati nell'**allegato III**? Si tratta di sistemi che operano nei settori della biometria; delle infrastrutture critiche; dell'istruzione e formazione professionale; dell'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; dell'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; delle attività di contrasto; della migrazione, asilo e gestione del controllo delle frontiere; dell'amministrazione della giustizia e processi democratici. Si tratta di un **elenco dinamico**, di cui è previsto l'aggiornamento periodico, e da cui restano esclusi i sistemi di IA destinati a "eseguire un compito procedurale limitato", a "migliorare il risultato di un'attività umana precedentemente completata", a "rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è inteso a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana" oppure a "eseguire un compito preparatorio per una valutazione pertinente (articolo 6, comma 3).

Ex articolo 43, comma 1 a) e b), diversamente dai prodotti listati nell'allegato I, i sistemi IA ad alto rischio elencati nell'allegato III possono seguire una **valutazione della conformità** al presente regolamento **basata sul "controllo interno** [da parte del fornitore] di cui all'allegato VI" **oppure** mediante "la valutazione del sistema di gestione della qualità e la valutazione della documentazione tecnica, **con il coinvolgimento di un organismo notificato**, di cui all'allegato VII".

Inoltre, diversamente dai prodotti listati nell'allegato I, ex articolo 49 "Registrazione", comma 1 "prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, il fornitore o, ove applicabile, il rappresentante autorizzato si registra e registra il suo sistema nella banca dati dell'UE" istituita in base all'articolo 71. Da questa banca dati i "i deployer che sono autorità, agenzie o organismi pubblici o persone che agiscono per loro conto si registrano, selezionano il sistema e ne registrano l'uso nella banca dati dell'UE" (articolo 49, comma 3).

Negli articoli passati in rassegna finora sono citati "fornitori" e "deployer" (che l'articolo 3, comma 4 definisce come "persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale).

\*\*\*

Quali sono tutti gli **attori della catena del valore** dei di sistemi di IA ad alto rischio **a cui si applica l'AI Act?**

**Fornitori**, i cui obblighi sono stabiliti dall'articolo 16 e che ex articolo 17 sono tenuti a istituire "un sistema di gestione della qualità che garantisce la conformità al presente regolamento".

Rappresentanti autorizzati dei fornitori, i cui obblighi sono stabiliti dall'articolo 22.

Importatori e distributori, i cui obblighi sono stabiliti dall'articolo 23 e 24.

Deployer, i cui obblighi sono stabiliti dall'articolo 26. Va sottolineato che ex articolo 4 "Alfabetizzazione in materia di IA", "i fornitori e i deployer ... adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione nonché il contesto in cui i sistemi di IA devono essere utilizzati".

Ai fini della **relazione fra AI Act e Regolamento Macchine** è di particolare interesse l'articolo 25, comma 3, secondo cui "**il fabbricante del prodotto è considerato il fornitore del sistema di IA** ad alto rischio ed è soggetto agli obblighi di cui all'articolo 16, in una delle circostanze seguenti: a) se il sistema di IA ad alto rischio è immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto; b) se il sistema di IA ad alto rischio è messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato".

\*\*\*

Sono soprattutto gli articoli da 9 a 15 a definire i "**requisiti per i sistemi di IA ad alto rischio**", cioè quelli che rendono un sistema **conforme** al presente regolamento.

L'articolo 9 tratta del "**Sistema di gestione dei rischi**" che va "inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio".

L'articolo 10 affronta "**Dati e governance dei dati**" di addestramento, convalida e prova, stabilendo che devono essere "pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai quali il sistema di IA ad alto rischio è destinato a essere usato".

L'articolo 11 tratta della "**Documentazione tecnica**" che è "redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti ... e da fornire alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti".

Ai fini della tracciabilità del funzionamento del sistema di IA ad alto rischio, l'articolo 12 tratta della "**Conservazione delle registrazioni**". La registrazione automatica degli eventi ("**log**") avviene per tutta la durata del ciclo di vita del sistema e, ex articolo 19, comma 1 "i log sono conservati per un periodo adeguato alla finalità prevista del sistema di IA ad alto rischio, della durata di almeno sei mesi".

L'articolo 13 obbliga i **fornitori**, e i **fabbricanti laddove equiparati a fornitori**, alla "**Trasparenza e fornitura di informazioni ai deployer**". Secondo il comma 1 "i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente", mentre il comma 2 integra il precedente stabilendo che i sistemi "sono accompagnati da **istruzioni per l'uso** in un formato digitale o non

digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer”.

L’articolo 14 “**Sorveglianza umana**” stabilisce che “i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche...” (comma 1) e che “la sorveglianza umana mira a prevenire o ridurre al minimo i rischi” (comma 2). Per esercitare in modo efficace la funzione di sorveglianza, la persona va messa nelle condizioni di “comprendere correttamente le capacità e i limiti pertinenti del sistema e ... di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese (comma 4 a), di “restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull’output prodotto” (comma 4 b), di “decidere ... di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l’output (comma 4 d) e attestare il sistema in condizioni di sicurezza (comma 4 e).

Infine, l’articolo 15 affronta “**Accuratezza, robustezza e cybersicurezza**” dei sistemi di IA ad alto rischio, sottolineando la necessità che siano “il più resilienti possibile” a “errori, guasti o incongruenze che possono verificarsi all’interno del sistema o nell’ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi” (comma 4) e “ai tentativi di terzi non autorizzati di modificarne l’uso, gli output o le prestazioni sfruttando le vulnerabilità del sistema”.

La **conformità del sistema di IA ad alto rischio a questi requisiti** sta alla base per il rilascio della “**Dichiarazione di conformità UE**” (articolo 47) e della “**Marcatura CE**” (articolo 47) per il sistema stesso.

\*\*\*

Oltre ai **rischi** dei sistemi di intelligenza artificiale, l’AI Act affronta anche quelli derivanti dai **modelli di IA** su cui i sistemi si basano.

L’AI Act distingue tra “fornitori di **modelli di IA per finalità generali**” – obbligati ex articolo 53 a redigere e mantenere aggiornata “la documentazione tecnica del modello, compresi il processo di addestramento e prova e i risultati della sua valutazione, che contiene almeno gli elementi di cui all’allegato XI” (comma 1 a) e ad elaborare, mantenere aggiornate e mettere a disposizione “informazioni e documentazione per i fornitori di sistemi di IA che intendono integrare il modello” (comma 1 b) e i “fornitori di **modelli di IA per finalità generali con rischio sistemico**”.

L’articolo 52 definisce con rischio sistemico i modelli di IA per finalità generali che presentano “capacità di impatto elevato” (comma 1 a) e in cui “l’importo cumulativo del calcolo utilizzato per il suo addestramento misurato in FLOP è [attualmente] superiore a  $10^{25}$ ” (comma 2). Oltre a dover informare la Commissione, che iscrive il modello in un apposito elenco (articolo 52), i fornitori di modelli di IA per finalità generali con rischio sistemico sottostà, in aggiunta agli obblighi ex articolo 53, anche a quelli ex articolo 55: “valutano e attenuano i possibili rischi sistemici a livello dell’Unione” (comma 1 b), “tengono traccia, documentano e riferiscono senza indebito ritardo le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio” (comma 1 c), “garantiscono un livello adeguato di protezione della cybersicurezza per quanto riguarda il modello di IA ... e l’infrastruttura fisica del modello” (comma 1 d).

\*\*\*

**In sintesi sono in particolare gli articoli 2 comma 1, 3 comma 14, 6 comma 1 a), 13 e 25 a collegare l’AI Act al Regolamento Macchine.**

Nell’ambito della normazione dell’uso di sistemi di intelligenza artificiale all’interno di prodotti va considerato con attenzione anche lo **standard ISO/IEC 5469:2024**, pubblicato a gennaio 2024.

Lo standard ISO/IEC 5469:2024 si focalizza sull'uso dell'intelligenza artificiale nelle funzioni legate alla sicurezza, sull'uso di funzioni di sicurezza non AI per garantire la sicurezza di apparecchiature controllate dall'AI, e sull'uso di sistemi AI per progettare e sviluppare funzioni legate alla sicurezza, indipendentemente dal settore industriale.

Lo standard ISO/IEC 5469:2024 descrive i metodi per garantire che i sistemi AI operino in modo sicuro e affidabile, includendo principi come l'acquisizione dei dati, l'inferenza della conoscenza e la generazione degli output.

Lo standard ISO/IEC 5469:2024 indica tecniche di verifica e validazione, misure di controllo e mitigazione dei rischi, nonché processi e metodologie per integrare la sicurezza funzionale nei sistemi AI che possono essere efficacemente supportati dall'implementazione di un sistema di gestione AI come definito da ISO/IEC 42001:2023. Questo approccio garantisce che i sistemi AI siano sviluppati e gestiti con un alto livello di sicurezza funzionale lungo tutto il loro ciclo di vita.

*Autore: Petra Dal Santo | [dalsanto@keanet.it](mailto:dalsanto@keanet.it)*