lug 30, 2026

Riunione del giorno 30 lug 2026 alle ore 13:04 CEST

Riepilogo

Sintesi dell'AI Act europeo riguardante classificazione dei rischi, obblighi di conformità e scadenze normative di attuazione.

Fondamenti dell'AI Act
Il regolamento definisce ruoli, obblighi e 4 livelli di rischio per i sistemi di intelligenza artificiale. Sono previste esclusioni specifiche per attività di ricerca, difesa e uso personale.

Obblighi e divieti normativi
Vengono vietate pratiche come la manipolazione subliminale mentre gli operatori devono garantire trasparenza e sorveglianza umana. È stato deciso di classificare internamente come rischio significativo i sistemi che impattano la sicurezza operativa.

Governance, sanzioni e scadenze
Agenzia per l'Italia Digitale e Agenzia per la Cybersicurezza Nazionale vigilano sulla conformità con sanzioni pecuniarie elevate. Il calendario attuativo prevede il divieto delle pratiche inaccettabili dal 2 febbraio 2025.

Passaggi successivi

Valutare Personalizzazione: Valutare con ufficio legale la lecita personalizzazione delle offerte. Verificare il carattere manipolativo e il potenziale danno significativo prima di procedere.

Verbalizzare Verifica: Redigere un verbale anche in caso di esito negativo delle verifiche sui sistemi AI. Documentare accuratamente ogni controllo effettuato per scopi di conformità.

Richiedere Documentazione: Esigere dai fornitori documentazione tecnica e piano di gestione rischi. Acquisire tutti i dati necessari per garantire la conformità contrattuale.

Valutare Impatto: Effettuare valutazione impatto sui diritti fondamentali prima di implementare nuovi sistemi. Considerare le implicazioni per i destinatari delle attività aziendali.

Informativa Vocale: Inserire avviso di generazione artificiale negli annunci audio della stazione. Specificare che la voce è sintetica per garantire la massima trasparenza.

Parere Garante: Richiedere parere al Garante della Privacy prima di intraprendere attività biometriche. Documentare la conformità in ogni fase del processo.

Autorizzazione Direzione: Ottenere autorizzazione dalla direzione generale per progetti di biometria. Assicurare il controllo preventivo prima di qualsiasi impegno operativo.

Classificare sistemi IA: Valutare i sistemi esistenti per stabilire se rientrano nelle categorie vietato, alto rischio, limitato o minimo.

Dettagli

- **Obiettivo dell'AI Act**: Il regolamento europeo sull'intelligenza artificiale, emanato nel 2024, non regola la tecnologia in sé, ma l'uso che ne viene fatto, mirando a promuovere sistemi affidabili garantendo al contempo la sicurezza e i diritti fondamentali. Si tratta di un regolamento direttamente applicabile in tutti gli Stati membri dell'Unione Europea, entrato in vigore il 1° agosto 2024.
- **Campo di applicazione ed esclusioni**: La normativa si applica a fornitori, utilizzatori e soggetti extraeuropei che operano nell'Unione, con alcune limitate esclusioni per attività militari, di difesa, sicurezza nazionale, ricerca e sviluppo, oltre a sistemi utilizzati per scopi puramente personali o basati su licenze open source.
- **Interazione con le norme vigenti**: L'AI Act non sostituisce le normative preesistenti, come quelle sulla protezione dei dati personali, la sicurezza sul lavoro, il diritto d'autore o la sicurezza informatica (NIS), ma si integra con esse, aumentando il quadro di obblighi per la messa in commercio dei prodotti.
- **Definizione dei ruoli**: Il regolamento identifica macro-ruoli specifici, tra cui fornitori, utilizzatori, importatori, distributori e rappresentanti autorizzati, ciascuno con obblighi documentali e procedurali distinti in base alla propria funzione rispetto al sistema.
- **Transizione da utilizzatore a fornitore**: Un utilizzatore può assumere il ruolo di fornitore, diventando soggetto a obblighi più rigorosi, in casi di modifica sostanziale del sistema, riaddestramento del modello su dati aziendali propri, o cambio della finalità d'uso prevista originariamente.

- **Classificazione dei livelli di rischio**: I sistemi di intelligenza artificiale sono classificati in quattro livelli di rischio: inaccettabile (vietato), alto rischio (ammesso con requisiti rigorosi), rischio limitato (obblighi di trasparenza) e rischio minimo (nessun obbligo specifico).
- **Categoria di rischio significativo**: A livello aziendale, viene introdotta una quinta categoria di "rischio significativo" per presidiare sistemi che incidono sulla sicurezza operativa aeroportuale o sui destinatari delle attività, pur non rientrando esplicitamente nell'Allegato 3 del regolamento.
- **Pratiche vietate**: L'articolo 5 elenca otto fattispecie di pratiche vietate in modo assoluto, tra cui tecniche manipolative subliminali, sfruttamento di vulnerabilità, punteggio sociale (social scoring), previsione di reati basata su profilazione, e utilizzo di banche dati di riconoscimento facciale non mirate.
- **Divieti biometrici**: È severamente vietato l'uso di sistemi di categorizzazione biometrica che deducano dati sensibili (politici, religiosi, orientamento sessuale) e l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, salvo specifiche eccezioni per le forze dell'ordine.
- **Sistemi ad alto rischio**: Questa categoria comprende sistemi incorporati in prodotti regolati (Allegato 1) e sistemi che incidono sulle persone, come quelli usati in infrastrutture critiche, istruzione, occupazione e servizi essenziali (Allegato 3).
- **Filtri di esclusione dall'alto rischio**: È possibile escludere un sistema dall'alto rischio se soddisfa almeno una delle condizioni previste, come l'esecuzione di compiti procedurali limitati, il miglioramento di un risultato umano o lo svolgimento di un'attività preparatoria.
- **Obblighi per i fornitori**: I fornitori devono implementare un sistema di gestione dei rischi iterativo, garantire la governance dei dati, redigere documentazione tecnica, assicurare la sorveglianza umana e mantenere registri automatici degli eventi.
- **Obblighi per gli utilizzatori**: Gli utilizzatori sono tenuti a seguire le istruzioni fornite, garantire la sorveglianza umana, monitorare il funzionamento del sistema, sospenderne l'uso in caso di rischi emergenti e informare lavoratori e soggetti impattati.
- **Trasparenza e obblighi informativi**: Indipendentemente dalla classe di rischio, esiste l'obbligo di trasparenza per i sistemi che interagiscono con persone fisiche e per i contenuti generati artificialmente (testo, audio, immagini, video), inclusi i deep fake, che devono essere chiaramente marcati.
- **Modelli di AI per finalità generali**: I fornitori di tali modelli sono soggetti a obblighi specifici riguardanti la documentazione tecnica, il rispetto del diritto d'autore e la pubblicazione di sintesi sui dati di addestramento.

- **Autorità di vigilanza e sanzioni**: A livello europeo operano l'Ufficio per l'Intelligenza Artificiale e il Comitato europeo, mentre in Italia sono state designate l'AGID e l'ACN come autorità competenti; le sanzioni per violazioni possono arrivare fino a 35 milioni di euro o al 7% del fatturato mondiale.
- **Legislazione italiana e moratoria biometrica**: La legge nazionale 132 del 2025 integra la disciplina europea, mantenendo una moratoria sull'uso della videosorveglianza con riconoscimento facciale in luoghi pubblici per soggetti privati, salvo rigorose procedure di autorizzazione.
- **Spazi di sperimentazione normativa**: Il regolamento prevede l'istituzione di ambienti controllati in cui è possibile testare sistemi innovativi sotto la supervisione delle autorità competenti prima della loro immissione sul mercato.
- **Scadenze principali**: Il calendario di attuazione prevede i divieti delle pratiche inaccettabili dal 2 febbraio 2025, obblighi di trasparenza dal 2 agosto 2026, e l'applicazione degli obblighi per i sistemi ad alto rischio tra il 2027 e il 2028.