Sintesi dell'AI Act europeo in 2 pillole (Seconda Parte)

Data 08 ottobre 2025
Categoria Medicinadigitale

Requisiti per i fornitori di sistemi di IA ad alto rischio (Art. 8–17)
I fornitori di sistemi IA ad alto rischio devono:
• istituire un sistema di gestione del rischio per l'intero ciclo di vita del sistema di IA ad alto rischio;
• applicare misure di governance dei dati, assicurandosi che i dataset di addestramento, validazione e testing siano pertinenti, sufficientemente rappresentativi e, per quanto possibile, privi di errori e completi rispetto all'uso previsto;

• redigere una documentazione tecnica che dimostri la conformità e fornisca alle autorità le informazioni necessarie a valutarla;
• progettare il sistema di IA ad alto rischio in modo da registrare automaticamente gli eventi rilevanti per identificare rischi a livello nazionale e modifiche sostanziali durante l'intero ciclo di vita del sistema;
• fornire istruzioni d'uso ai soggetti a valle (utilizzatori) affinché questi possano adempiere ai propri obblighi di conformità;
• progettare il sistema di IA ad alto rischio in modo da consentire agli utilizzatori di implementare una supervisione umana sul suo funzionamento;
• progettare il sistema di IA ad alto rischio per raggiungere livelli adeguati di accuratezza, robustezza e cybersicurezza;
• istituire un sistema di gestione della qualità per assicurare la conformità normativa.

Casi d'uso dell'Allegato III

• **Biometria non vietata:**
– Sistemi di identificazione biometrica remota, esclusi quelli di verifica biometrica che confermano l'identità dichiarata di una persona.
– Sistemi di categorizzazione biometrica che deducono attributi o caratteristiche sensibili o protette.
– Sistemi di riconoscimento delle emozioni.
• **Infrastrutture critiche:**
– Componenti di sicurezza per la gestione e il funzionamento di infrastrutture digitali critiche, del traffico stradale e dell'approvvigionamento di acqua, gas, riscaldamento ed elettricità.
• **Istruzione e formazione professionale:**
– Sistemi di IA che determinano l'accesso, l'ammissione o l'assegnazione a istituti di istruzione o formazione professionale a tutti i livelli.
– Valutazione dei risultati dell'apprendimento, inclusi quelli utilizzati per orientare il processo formativo dello studente.
– Valutazione del livello di istruzione appropriato per un individuo.
– Monitoraggio e rilevamento di comportamenti proibiti degli studenti durante gli esami.
• **Occupazione, gestione del personale e accesso al lavoro autonomo:**
– Sistemi di IA utilizzati per il reclutamento o la selezione del personale, in particolare l'invio mirato di offerte di lavoro, l'analisi e il filtraggio delle candidature, e la valutazione dei candidati.
– Decisioni relative a promozione o risoluzione di contratti, allocazione dei compiti basata su tratti della personalità o caratteristiche comportamentali, e monitoraggio e valutazione delle prestazioni lavorative.
• **Accesso a servizi pubblici e privati essenziali:**
– Sistemi di IA utilizzati da autorità pubbliche per valutare l'idoneità all'accesso a prestazioni e servizi (e per la loro assegnazione, riduzione, revoca o recupero).
– Valutazione dell'affidabilità creditizia, salvo quando effettuata ai fini di rilevare frodi finanziarie.
– Valutazione e classificazione delle chiamate di emergenza, inclusa la definizione delle priorità di invio di polizia, vigili del fuoco, soccorso medico e triage urgente dei pazienti.
– Valutazione dei rischi e calcolo dei premi nelle assicurazioni sanitarie e sulla vita.
• **Forze dell'ordine (law enforcement):**
– Sistemi di IA utilizzati per valutare il rischio che un individuo diventi vittima di un reato.
– Poligrafi (rilevatori di menzogna).
– Valutazione dell'affidabilità delle prove durante indagini o procedimenti penali.
– Valutazione del rischio che un individuo commetta reati o recidivi, non basata unicamente su profiling o su tratti della personalità o precedenti penali.

– Attività di profiling durante operazioni di individuazione, indagini o azioni penali.
• Gestione di migrazione, asilo e frontiere:
– Valutazione dei rischi di migrazione irregolare o dei rischi sanitari.
– Esame delle richieste di asilo, visti e permessi di soggiorno, e dei relativi ricorsi riguardanti i requisiti di ammissibilità.
– Rilevamento, riconoscimento o identificazione di individui, fatto salvo l'uso per verificare i documenti di viaggio.
• Amministrazione della giustizia e processi democratici:
– Sistemi di IA utilizzati per ricercare e interpretare fatti e applicare la legge a casi concreti, oppure utilizzati in procedure di risoluzione alternativa delle controversie.
– Influenza su elezioni o referendum (esiti o comportamento di voto), esclusi gli output che non interagiscono direttamente con le persone, come strumenti usati per organizzare, ottimizzare o strutturare campagne politiche.

[b] Commento[/b]
[b]Punti di forza e opportunità[/b]
Dal punto di vista tecnico, l'AI Act rappresenta un avanzamento importante introducendo standard uniformi di sicurezza e qualità per gli sistemi di IA in Europa. I requisiti di risk management, controllo dei dati e sorveglianza umana per i sistemi ad alto rischio promuovono uno sviluppo più affidabile degli algoritmi, riducendo bias e malfunzionamenti. Ad esempio, l'obbligo di utilizzare dati rappresentativi e mitigare i rischi incoraggia le aziende ad adottare metodologie di AI più robuste e "by design" (come testing rigorosi, dataset bilanciati, audit algoritmici periodici). Ciò può aumentare la fiducia sia degli utenti sia degli investitori verso l'IA, con effetti positivi sull'adozione su larga scala di queste tecnologie in modo sicuro.

In termini etici, il regolamento pone al centro la tutela dei diritti fondamentali: il divieto di pratiche inaccettabili (dalla sorveglianza biometrica onnipervasiva al social scoring) è un chiaro messaggio a difesa della dignità umana, della privacy e dei principi democraticiosservatori.net. Evitando derive distopiche, l'Europa afferma un modello di IA "etica by design", dove determinati confini non possono essere superati. Allo stesso tempo, la scelta di un approccio basato sul rischio concreto evita di bloccare innovazioni innocue: la maggior parte delle applicazioni a basso rischio rimane libera, salvo trasparenza. Questa proporzionalità è un punto di forza, perché sostiene l'innovazione responsabile anziché frenarla indiscriminatamente. Le misure di trasparenza poi rafforzano il diritto all'informazione degli utenti: sapere di interagire con un'IA o che un video è un deepfake consente scelte più consapevoli e previene manipolazioni, sostenendo l'autonomia individuale.

Anche la governance multilivello è un aspetto positivo: coordinando autorità nazionali, esperti ed enti UE, l'AI Act crea un ecosistema di sorveglianza attiva e scambio di conoscenze. L'istituzione dell'AI Office e del Comitato europeo per l'IA potrà garantire applicazione uniforme in tutti gli Stati membridigital-strategy.ec.europa.eudigital-strategy.ec.europa.eu, evitando frammentazione regolatoria. Questa cooperazione è cruciale anche per affrontare sfide globali: il nuovo quadro normativo UE può diventare un benchmark internazionale (come avvenuto col GDPR), spingendo altri Paesi verso standard simili e prevenendo fenomeni di dumping normativo. In sintesi, l'AI Act fornisce certezze giuridiche (chi sviluppa o usa IA sa quali regole rispettare) e al contempo incardina i valori etici europei nell'era algoritmica, bilanciando sicurezza e innovazione.
[b]Criticità e sfide aperte[/b]
Non mancano tuttavia criticità tecniche e implementative. Un primo aspetto è il costo della conformità: per aziende e sviluppatori, soprattutto se di piccole dimensioni, implementare sistemi di gestione del rischio, documentazione corposa, monitoraggi continui e interfacciarsi con organismi notificati può risultare oneroso. C'è il timore che la burocrazia tecnica richiesta per gli high-risk AI rallenti il ciclo di sviluppo e immissione sul mercato, penalizzando le startup e gli attori europei rispetto a competitor di Paesi con regolamentazioni più permissive. Questa sproporzione di oneri potrebbe spingere alcuni innovatori a evitare l'Europa o a limitare i propri progetti di IA, con potenziali effetti frenanti sulla competitività (il cosiddetto rischio di innovation red tape).

Dal punto di vista etico-sociale, alcuni critici ritengono che l'AI Act non vada abbastanza lontano su certe pratiche rischiose. Ad esempio, sebbene il riconoscimento facciale in tempo reale sia in generale vietato, le eccezioni previste potrebbero aprire la porta a sorveglianza di massa se abusate: organizzazioni per i diritti civili avrebbero preferito un divieto totale di queste tecnologie nei luoghi pubblici, data la loro invasività. Anche l'emotion recognition è bandito solo in ambito lavoro/istruzione; ma il suo uso commerciale (es. per profilazione dei clienti) rimane lecito con la sola informativa, nonostante molti esperti ne contestino la validità scientifica e l'intrusività. C'è dunque il rischio che alcune zone grigie non completamente vietate possano comunque portare ad abusi o discriminazioni, richiedendo vigile controllo da parte delle autorità.

Un'altra sfida riguarda la definizione stessa di "alto rischio". La lista di usi nell'Allegato III, per quanto ampia, potrebbe rapidamente diventare obsoleta in un campo tecnologico in rapida evoluzione. Nuovi tipi di applicazioni IA (si pensi a quelle creative o in ambito meta-verso) potrebbero emergere fuori dal perimetro normato ma con impatti significativi. Il meccanismo di aggiornamento annuale potrà porre rimedio, ma dipenderà dalla reattività del legislatore. Inoltre, alcuni concetti come "rischio significativo" o "impatti sui

diritti" lasciano margine interpretativo: aziende differenti potrebbero valutare diversamente se il loro sistema ricade o meno nel high-risk, creando incertezza. Una complessità tecnica sta anche nel verificare il rispetto di requisiti qualitativi: come misurare formalmente se un modello ha "accuratezza adeguata" o dataset "sufficientemente rappresentativi"? L'assenza, ad oggi, di standard tecnici dettagliati potrebbe rendere difficoltosa l'armonizzazione. Si dovranno sviluppare norme tecniche (ad es. standard ISO/CEI per l'IA) e linee guida pratiche per dare sostanza a questi requisiti generali.
Infine, c'è la questione della rapida evoluzione tecnologica. L'AI Act nasce in un contesto (2021-2023) e già in corso d'opera è stato aggiornato per includere aspetti come i modelli generativi. In futuro potrebbe dover fronteggiare scenari oggi imprevedibili (ad es. progressi verso un'IA generale, nuove forme di autonomia delle macchine, ecc.). La legge dovrà quindi essere dinamica: sarà essenziale monitorare costantemente l'impatto dell'IA sulla società e, se necessario, adattare le disposizioni. Il rischio, altrimenti, è di trovarsi con norme superate mentre l'innovazione prosegue altrove (il cosiddetto technology lag normativo). In positivo, l'AI Act prevede meccanismi di revisione periodica e l'istituzione di quei gruppi di esperti e forum multi-stakeholder potrà fornire l'intelligenza collettiva per aggiornare le policy.

In conclusione, l'AI Act europeo segna una pietra miliare nel tentativo di conciliare tecnologia e valori umani. Dal punto di vista tecnico introduce processi di qualità e sicurezza nell'IA, e dal punto di vista etico cerca di incardinare il rispetto della dignità e dei diritti fin dalla progettazione degli algoritmi. La sua efficacia dipenderà molto dall'implementazione concreta: dovrà esserci impegno tanto da parte dell'industria, chiamata a integrare la compliance come parte integrante dell'innovazione, quanto da parte delle istituzioni, nel fornire linee guida chiare, supporto alle imprese e un'applicazione rigorosa ma equa. Se ben attuato, il regolamento potrebbe diventare un modello globale per uno sviluppo dell'AI responsabile e umano-centrico. Le sfide non mancano, ma l'auspicio è che questo quadro normativo evolutivo sappia adattarsi ai tempi, garantendo che l'intelligenza artificiale rimanga uno strumento al servizio dell'umanità, e non viceversa.

Riccardo De Gobbi e Giampaolo Collecchia

Bibliografia
1) pillole.org/public/aspnuke/admin_news.asp?id=8815&do=view
2) eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it