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

Data 30 settembre 2025
Categoria Medicinadigitale

Nella pillola precedente abbiamo commentato un importante editoriale del Jama(1) che criticava la mancata regolamentazione delle Intelligenze Artificiali USA lodando l'impegno europeo concretizzatosi nel AI- Act, documento fondamentale per il nostro futuro ed ancor più per quello dei nostri figli. In questa e nella prossima pillola forniremo una sintesi del documento che si articola in oltre 140 pagine ma che esprime "relativamente pochi" concetti di grandissima rilevanza: eccone la prima parte….

Classificazione del rischio: L'AI Act classifica i sistemi di IA in base al loro livello di rischio:
– **Rischio inaccettabile:** sistemi proibiti (ad es. sistemi di punteggio sociale e IA manipolative).
– **Rischio alto:** la maggior parte del testo si concentra sui sistemi di IA ad alto rischio, che sono regolamentati.
– **Rischio limitato:** una sezione più piccola riguarda i sistemi di IA a rischio limitato, soggetti a obblighi di trasparenza più leggeri. In particolare, sviluppatori e utilizzatori devono assicurare che gli utenti finali siano consapevoli di interagire con un'IA (es. chatbot e deepfake).
– **Rischio minimo: nessuna regolamentazione** (include la maggior parte delle applicazioni di IA attualmente disponibili nel mercato unico dell'UE, come videogiochi con IA e filtri anti-spam – almeno fino al 2021; la situazione sta evolvendo con l'avvento dell'IA generativa).
• **Sviluppatori di IA:** La maggior parte degli obblighi ricade sugli sviluppatori di sistemi di IA ad alto rischio. In particolare coloro che intendono immettere sul mercato o mettere in servizio sistemi di IA ad alto rischio nell'UE, indipendentemente dal fatto che abbiano sede nell'UE o in un paese terzo.
• **Utilizzatori (deployers):** Gli utilizzatori sono persone fisiche o giuridiche che impiegano un sistema di IA in ambito professionale, diversi dagli utenti finali interessati.
– Gli utilizzatori di sistemi di IA ad alto rischio hanno alcuni obblighi, sebbene inferiori a quelli dei fornitori (sviluppatori). Anche questo si applica agli utilizzatori con sede nell'UE, e anche a utilizzatori in paesi terzi quando l'output del sistema di IA è utilizzato nell'UE.
• **IA di uso generale (GPAI):**
– Tutti i fornitori di modelli di IA di uso generale (GPAI) devono fornire documentazione tecnica, istruzioni per l'uso, rispettare la Direttiva sul diritto d'autore e pubblicare un riepilogo del contenuto utilizzato per l'addestramento.
– I fornitori di modelli GPAI con licenza libera e open-source devono solo rispettare la normativa sul diritto d'autore e pubblicare il riepilogo dei dati di addestramento, a meno che tali modelli non presentino un rischio sistemico.– **Tutti i fornitori di modelli GPAI che presentano un rischio sistemico – siano essi modelli aperti o chiusi – devono anche condurre valutazioni del modello, test adversarial (di attacco), tracciare e segnalare incidenti gravi e garantire adeguate protezioni di cybersicurezza.**

Sistemi di IA proibiti (Cap. II, Art. 5)
Sono considerati "proibiti" dall'AI Act i seguenti tipi di sistemi di IA:
• **tecniche subliminali,** manipolative o ingannevoli impiegate per distorcere il comportamento e compromettere le decisioni informate, provocando un danno significativo al soggetto;
• **sfruttamento di vulnerabilità** legate all'età, alla disabilità o alle condizioni socio-economiche di una persona al fine di distorcerne il comportamento, causando un danno significativo;
• **sistemi di categorizzazione biometrica** che inferiscono attributi sensibili (razza, opinioni politiche, appartenenza sindacale, credo religioso o filosofico, vita sessuale o orientamento sessuale), fatta eccezione per l'etichettatura o il filtraggio di dataset biometrici acquisiti legalmente, o per la categorizzazione di dati biometrici effettuata dalle forze dell'ordine;
• **social scoring,** ovvero la valutazione o classificazione di individui o gruppi basata sul comportamento sociale o caratteristiche personali, che comporti trattamenti negativi o sfavorevoli verso tali persone;
• **valutazione del rischio che un individuo commetta reati basata unicamente sul profiling** o su tratti della personalità, salvo quando sia utilizzata per supportare valutazioni umane basate su fatti obiettivi e verificabili direttamente collegati ad attività criminali;
• compilazione di database per **riconoscimento facciale mediante scraping** indiscriminato di immagini facciali da Internet o da filmati CCTV;
• **inferenza delle emozioni** in luoghi di lavoro o istituti scolastici, eccetto per motivi medici o di sicurezza;
• **sistemi di identificazione biometrica remota "in tempo reale"** in luoghi accessibili al pubblico per scopi di applicazione della legge (forze dell'ordine), salvo quando: 1)si tratti di ricerca di persone scomparse, vittime di rapimento, o persone vittime di tratta di esseri umani o sfruttamento sessuale;
2) sia finalizzata a prevenire una minaccia sostanziale e imminente per la vita o la sicurezza fisica, o un attacco terroristico prevedibile;
3) sia impiegata per identificare sospetti di reati gravi (ad es. omicidio, stupro, rapina a mano armata, traffico di

stupefacenti o di armi illegali, criminalità organizzata, reati ambientali, ecc.).

Note sull'identificazione biometrica remota:
- L'uso di sistemi di RBI (identificazione biometrica remota) in tempo reale abilitati dall'IA è consentito solo quando il mancato utilizzo dello strumento provocherebbe danni considerevoli, e deve comunque tenere conto dei diritti e delle libertà delle persone interessate.
- Prima del dispiegamento, le forze dell'ordine devono effettuare una valutazione d'impatto sui diritti fondamentali e registrare il sistema nel database UE; tuttavia, in casi debitamente giustificati di urgenza, il dispiegamento può iniziare senza registrazione, a condizione che la registrazione avvenga successivamente senza indebito ritardo.
- Prima del dispiegamento, è inoltre necessario ottenere l'autorizzazione da un'autorità giudiziaria o da un'autorità amministrativa indipendente; tuttavia, in casi debitamente giustificati di urgenza, il dispiegamento può iniziare senza autorizzazione, a condizione che l'autorizzazione sia richiesta entro 24 ore. Se l'autorizzazione viene negata, il dispiegamento deve cessare immediatamente, eliminando tutti i dati, i risultati e gli output.

Sistemi di IA ad alto rischio (Cap. III)
Alcuni sistemi di IA sono considerati "ad alto rischio" ai sensi dell'AI Act. I fornitori di tali sistemi saranno soggetti a requisiti aggiuntivi.
Regole di classificazione per i sistemi di IA ad alto rischio (Art. 6)
Si definiscono sistemi di IA ad alto rischio quelli che:
• sono utilizzati come componente di sicurezza di un prodotto disciplinato dalla normativa UE elencata nell'Allegato I E richiedono una valutazione di conformità da parte di terzi secondo le leggi indicate in Allegato I; oppure
• rientrano tra i casi d'uso elencati nell'Allegato III (vedi sotto), fatta eccezione per il caso in cui:
– il sistema di IA svolga un compito procedurale circoscritto;
– migliori il risultato di un'attività umana precedentemente svolta;
– rilevi schemi decisionali o deviazioni da schemi decisionali precedenti e non sia destinato a sostituire o influenzare la valutazione umana già effettuata, in assenza di una corretta revisione umana; oppure svolga un compito preparatorio rispetto a una valutazione rilevante ai fini dei casi d'uso elencati nell'Allegato III.
• I sistemi di IA elencati nell'Allegato III sono sempre considerati ad alto rischio se profilano degli individui, ossia effettuano trattamenti automatizzati di dati personali per valutare aspetti della vita di una persona, come le prestazioni lavorative, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, la posizione o i movimenti.
• I fornitori il cui sistema di IA rientra nei casi d'uso dell'Allegato III ma ritengono che non sia ad alto rischio devono documentare tale valutazione prima di immettere il sistema sul mercato o metterlo in servizio.

… Continua nella Seconda parte

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