

ESTRATTO INFORMATIVO GRATUITO · SEZIONE A · A CURA DI ADLP

# Le 8 pratiche di Intelligenza Artificiale vietate in Europa

Cosa dice l'art. 5 dell'AI Act, spiegato in parole semplici — e perché può riguardare anche la tua azienda

Dal **2 febbraio 2025** alcune applicazioni di Intelligenza Artificiale sono vietate in tutta l'Unione Europea: non possono essere immesse sul mercato, messe in servizio né utilizzate. In questo estratto trovi, in linguaggio chiaro, quali sono queste pratiche, un esempio concreto per ciascuna e perché possono riguardare anche aziende "comuni" — non solo le big tech. È il primo filtro da conoscere prima di qualsiasi altra valutazione: se un sistema ricade qui, ogni altra analisi passa in secondo piano.

**A cosa serve questo documento.** A darti un orientamento iniziale e a farti capire se la tua organizzazione usa (o sta per usare) qualcosa che merita un approfondimento. Non è un parere legale e non sostituisce l'analisi del tuo caso concreto (vedi avvertenza finale).

## Prima di tutto: perché esiste un elenco di "pratiche vietate"

L'AI Act ( **Regolamento UE 2024/1689** ) classifica i sistemi di IA in base al rischio che pongono per le persone e per i diritti fondamentali. Al gradino più alto ci sono le **pratiche vietate** : usi considerati inaccettabili a prescindere da garanzie tecniche o consenso. Per queste pratiche non esiste una "compliance" che le renda lecite: sono semplicemente fuori legge.

Per questo, quando si valuta un sistema di IA, la prima domanda è sempre la stessa: **ricade tra le pratiche vietate dell'art. 5?** Se la risposta è sì, il sistema non si può usare. Se è no, si passa a valutare se sia "ad alto rischio" e quali obblighi ne derivino.

## LE 8 PRATICHE VIETATE DALL'ART. 5

*In linguaggio divulgativo. Per ogni voce: cosa vieta · un esempio concreto · perché può riguardare anche te.*

### 1 Tecniche subliminali, manipolative o ingannevoli

**Cosa vieta.** Sistemi di IA che agiscono sotto la soglia di consapevolezza della persona, o che usano tecniche manipolative o ingannevoli, per distorcerne il comportamento in modo da causare (o poter ragionevolmente causare) un **danno significativo**.

**Esempio concreto.** Un'app che, con messaggi e stimoli impercettibili, spinge l'utente verso scelte di acquisto o finanziarie che non avrebbe compiuto e che gli arrecano un danno rilevante.

**Perché può riguardare anche te.** Non serve essere una piattaforma globale: anche un sistema di marketing, un chatbot persuasivo o un'interfaccia "dark pattern" potenziata da IA possono finire in quest'area se manipolano la volontà delle persone con potenziale danno.

### 2 Sfruttamento delle vulnerabilità

**Cosa vieta.** Sistemi che traggono vantaggio dalle **vulnerabilità** di una persona o di un gruppo dovute a età, disabilità o a una specifica situazione economica o sociale, per alterarne il comportamento con potenziale danno significativo.

**Esempio concreto.** Un servizio che individua persone anziane o in difficoltà economica e le indirizza, sfruttando la loro fragilità, verso prodotti dannosi o sproporzionati.

**Perché può riguardare anche te.** Chiunque profili clienti per "segmenti deboli" (over 75, persone indebitate, soggetti con disabilità) e usi l'IA per indirizzarli in modo aggressivo può trovarsi in questa categoria.

### 3 Punteggio sociale (social scoring)

**Cosa vieta.** Sistemi che valutano o classificano le persone (o i gruppi) sulla base del comportamento sociale o di caratteristiche personali, generando un trattamento **sfavorevole sproporzionato** o avulso dal contesto in cui i dati erano stati raccolti.

**Esempio concreto.** Una piattaforma che assegna ai clienti un "punteggio reputazionale" unico, combinando dati eterogenei (acquisti, comportamenti online, frequentazioni), e poi nega servizi o applica condizioni peggiori in ambiti che nulla c'entrano con quei dati.

**Perché può riguardare anche te.** Programmi fedeltà evoluti, sistemi di "scoring clienti" o di valutazione fornitori che cumulano dati di provenienza diversa e producono effetti penalizzanti possono avvicinarsi pericolosamente al social scoring vietato.

### 4 Predizione del rischio di reato basata su profilazione

**Cosa vieta.** Sistemi che valutano o prevedono il rischio che una persona commetta un reato basandosi **esclusivamente** sulla profilazione o sulle caratteristiche della personalità (la cosiddetta "polizia predittiva su base individuale").

**Esempio concreto.** Un software che assegna a singoli individui un "indice di pericolosità" calcolato solo su profilo psicologico, dati anagrafici o comportamentali, senza fatti oggettivi e verificabili.

**Perché può riguardare anche te.** Riguarda soprattutto il settore pubblico e la sicurezza, ma anche soggetti privati che sviluppano o forniscono strumenti di "risk scoring" predittivo sulle persone devono fare attenzione al confine.

## 5 Scraping non mirato di volti per banche dati di riconoscimento facciale

**Cosa vieta.** Creare o ampliare banche dati di riconoscimento facciale mediante **raccolta non mirata (scraping)** di immagini di volti da internet o dalle telecamere di videosorveglianza.

**Esempio concreto.** Un sistema che "aspira" milioni di foto di volti dai social o dalle TVCC e le usa per costruire un database biometrico di riconoscimento.

**Perché può riguardare anche te.** Qualsiasi azienda che alimenti o utilizzi strumenti di riconoscimento facciale costruiti raccogliendo volti in modo indiscriminato è coinvolta, anche se non ha sviluppato lei la tecnologia.

## 6 Riconoscimento delle emozioni sul lavoro e a scuola

**Cosa vieta.** Sistemi di IA che **deducono le emozioni** delle persone sul luogo di lavoro e negli istituti di istruzione, salvo strette eccezioni (es. finalità mediche o di sicurezza).

**Esempio concreto.** Un software che durante le riunioni o le video-call analizza il volto e la voce dei dipendenti per stimarne lo "stato emotivo", il livello di stress o l'attenzione.

**Perché può riguardare anche te.** È una delle pratiche più insidiose per le aziende "comuni": strumenti di HR analytics, di monitoraggio del personale o di valutazione degli studenti che misurano emozioni rientrano nel divieto. Molte imprese non si accorgono di averli attivi.

## 7 Categorizzazione biometrica per dedurre dati sensibili

**Cosa vieta.** Sistemi che, dai dati biometrici, classificano le persone per **dedurre o inferire categorie sensibili**: origine razziale o etnica, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale.

**Esempio concreto.** Un sistema che, dall'analisi del volto o di altri tratti biometrici, prova a stabilire l'etnia, la religione o l'orientamento sessuale di una persona.

**Perché può riguardare anche te.** Qualsiasi soluzione di analisi biometrica usata per segmentare, profilare o indirizzare il pubblico in base a caratteristiche sensibili è a rischio divieto, anche se presentata come "marketing avanzato".

## 8 Identificazione biometrica remota "in tempo reale" in spazi pubblici

**Cosa vieta.** L' **identificazione biometrica a distanza e "in tempo reale"** (es. riconoscimento facciale dal vivo) in spazi accessibili al pubblico, a fini di attività di contrasto (forze dell'ordine). È vietata salvo eccezioni tassative e autorizzate (es. ricerca di vittime, minaccia terroristica imminente, individuazione di autori di gravi reati), con garanzie stringenti.

**Esempio concreto.** Telecamere in piazza che identificano in diretta i passanti confrontando i volti con una banca dati, al di fuori dei casi e delle autorizzazioni previste.

**Perché può riguardare anche te.** Riguarda principalmente le autorità pubbliche, ma anche i fornitori privati di queste tecnologie e i gestori di spazi pubblici/semipubblici devono conoscere i confini molto stretti entro cui è ammessa.

## PERCHÉ TI RIGUARDA (E COSA RISCHI)

**Non è "roba da big tech".** Molte aziende italiane usano già, magari senza saperlo, strumenti che lambiscono queste aree: HR analytics che leggono le emozioni, scoring clienti che cumulano dati eterogenei, marketing che sfrutta le fragilità, soluzioni biometriche "chiavi in mano" acquistate da terzi. Anche chi compra e utilizza un sistema (non solo chi lo sviluppa) può essere coinvolto.

**Cosa rischi — le sanzioni per le pratiche vietate (art. 5).** La violazione del divieto dell'art. 5 è punita con la sanzione più severa prevista dall'AI Act: **fino a 35 milioni di euro** oppure **il 7% del fatturato mondiale annuo** dell'esercizio precedente, se superiore (art. 99 AI Act).

**Nota per PMI e start-up.** Per le piccole e medie imprese e le start-up si applica il **minore** tra la cifra fissa e la percentuale del fatturato (non il maggiore): un "tetto" più basso a tutela delle imprese di minori dimensioni.

*Importi massimi previsti dal Reg. (UE) 2024/1689 (art. 99). L'autorità competente modula la sanzione effettiva in base a gravità, durata e circostanze della violazione. Timeline e regole soggette a possibili modifiche normative UE in corso.*

## Come capire se devi approfondire

Poniti queste domande, riferendole a **ciascun sistema di IA** che la tua organizzazione sviluppa, acquista o utilizza:

- Il sistema influenza o orienta il comportamento delle persone con tecniche poco trasparenti?
- Tratta in modo speciale gruppi vulnerabili (per età, disabilità, condizione economica o sociale)?
- Assegna punteggi o classificazioni alle persone combinando dati di natura diversa?
- Prevede comportamenti o rischi delle persone (incluso il rischio di reato) su base di profilazione?
- Usa dati biometrici o volti per identificare, classificare o dedurre caratteristiche delle persone?
- Legge le emozioni di dipendenti o studenti?

Se anche una sola risposta è **"sì"** o **"non lo so"**, è il caso di approfondire con metodo, prima di proseguire l'uso del sistema.

## Il primo passo: l'AI Act Assessment — Livello 1

Un **servizio informativo e di orientamento**, progettato e validato da un avvocato, che ti aiuta a inquadrare in via preliminare la posizione dei tuoi sistemi di IA rispetto all'AI Act: se possono ricadere tra le pratiche vietate, se sono "ad alto rischio", quale ruolo rivesti e quali obblighi, in linea generale, ne discendono.

- **Primo risultato di orientamento entro 48–72 ore** dalla ricezione del questionario compilato in modo completo.
- **Inquadramento per categorie tipizzate** + elenco dei punti da approfondire.
- **Non è un parere legale** e non promette alcun esito: ti dà un orientamento chiaro per decidere il passo successivo con consapevolezza.



**Scopri il servizio AI Act Assessment — Livello 1 ·**

<https://adlpstudio.it/soluzioni/ai-act-assessment/>

## AVVERTENZA FINALE

**Natura di questo documento.** Il presente è un documento informativo e divulgativo, aggiornato al 1° giugno 2026, predisposto quale prima informazione sul tema delle pratiche di IA vietate dall'art. 5 dell'AI Act.

Esso **non costituisce un parere legale** né una consulenza individualizzata, non instaura alcun rapporto professionale con l'avvocato o lo studio e non sostituisce l'analisi del caso concreto. Le qualificazioni dipendono dalla finalità prevista, dal contesto d'uso e dai dettagli del singolo sistema, e richiedono una verifica puntuale.

**Nessuna decisione rilevante** dovrebbe essere assunta sulla sola base di questo documento. Per una valutazione professionale completa — parere motivato e firmato dall'avvocato — è disponibile un percorso dedicato, distinto dal servizio informativo di orientamento (Livello 1).

## Riferimenti normativi

- **Regolamento (UE) 2024/1689 (AI Act)** — in particolare art. 5 (pratiche di IA vietate) e art. 99 (sanzioni).
- **Legge 23 settembre 2025, n. 132** — disposizioni nazionali in materia di intelligenza artificiale, in vigore dal 10 ottobre 2025.
- **Decorrenza del divieto delle pratiche dell'art. 5** — 2 febbraio 2025. Timeline e regole soggette a possibili modifiche normative UE in corso (es. pacchetto di semplificazione "Digital Omnibus").

ADLP Digital S.r.l. · Via Polibio 22, 00136 Roma · Estratto informativo gratuito — riproduzione consentita citando la fonte.