

# L'Intelligenza Artificiale entra nel D.Lgs. 231/2001

**I nuovi reati presupposto, la sicurezza sul lavoro e gli impatti organizzativi per le imprese**

## INQUADRAMENTO NORMATIVO

**Contesto d'attuazione:** Il Consiglio dei Ministri ha approvato in via definitiva i decreti legislativi di attuazione della delega della **Legge n. 132/2025**, dando attuazione nazionale al **Regolamento (UE) 2024/1689 (AI Act)**. Il decreto inserisce nel D.Lgs. 231/2001 il nuovo **art. 25-vicies**, che disciplina la responsabilità amministrativa degli enti per reati commessi tramite o nell'uso di sistemi di IA.

## 01. I Nuovi Reati Presupposto

### Art. 437-bis c.p. — Sistemi IA ad Alto Rischio

Punisce le violazioni nella gestione di sistemi IA ad alto rischio. La punibilità penale scatta in presenza di un **pericolo concreto**:

- **Pericolo per la vita o l'incolumità individuale:** Reclusione da **1 a 5 anni**.
- **Pericolo per l'incolumità pubblica o la sicurezza dello Stato:** Reclusione da **2 a 8 anni**.

#### Condotte Sanzionate:

1. **Omissione di misure tecniche di sicurezza:** Mancata adozione di misure idonee a prevenire malfunzionamenti o alterazioni durante la progettazione, l'addestramento, la produzione, l'immissione sul mercato o l'utilizzo professionale dei sistemi IA.
2. **Omissione di sorveglianza umana (*Human-in-the-Loop*):** Mancato controllo o presidio umano sui processi operativi gestiti dall'IA ad alto rischio.
3. **Aggressione esterna:** Alterazione del funzionamento del sistema da parte di soggetti estranei al ciclo di vita (pena da **2 a 6 anni** o **3 a 10 anni** nelle ipotesi aggravate).
4. **Omissioni per colpa grave:** Violazioni macroscopiche dei doveri di diligenza in un contesto tecnologico in rapida evoluzione (pena ridotta da un terzo a un sesto).

### Art. 612-quater c.p. — Deepfake

Introdotta dall'art. 26 della L. 132/2025 e inserita anch'essa nel catalogo dei reati 231.

- **Comportamento sanzionato:** Illecita diffusione di contenuti (immagini, video, audio) generati o alterati artificialmente idonei a trarre in inganno sulla loro genuinità.

## 02. Le Sanzioni per l'Ente (Art. 25-vicies)

Le sanzioni pecuniarie sono determinate secondo il sistema delle quote (valore singola quota: da € 258,22 a € 1.549,37).

| Reato Presupposto                                | Sanzione ed Importo Edittale                                                                                             | Misure Interdittive Applicabili                                                                                                                                                                                                            |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Art. 437-bis c.p.</b><br>(IA ad Alto Rischio) | <b>600 – 1.000 quote</b><br>da € 154.932 a € 1.549.370<br>(Fascia alta, equiparata all'art. 25-septies sicurezza lavoro) | <ul style="list-style-type: none"> <li>■ Sospensione / revoca autorizzazioni</li> <li>■ Divieto di contrattare con la PA</li> <li>■ Esclusione da finanziamenti/agevolazioni</li> <li>■ Divieto di pubblicizzare beni o servizi</li> </ul> |
| <b>Art. 612-quater c.p.</b><br>(Deepfake)        | <b>200 – 700 quote</b><br>da € 51.644 a € 1.084.559                                                                      | <ul style="list-style-type: none"> <li>■ Sanzioni interdittive selettive applicabili in base all'impatto dell'illecito</li> </ul>                                                                                                          |

**Principio di Proporzionalità:** Resta esclusa l'interdizione definitiva dall'esercizio dell'attività. La norma punta a colpire la specifica operatività nei settori connessi all'illecito, salvaguardando la continuità dell'impresa.

## 03. Focus Settoriale: Imprese che Commercializzano

Le aziende che importano, distribuiscono o commercializzano sistemi di IA (o prodotti che integrano moduli IA) assumono la qualifica normativamente rilevante di **Distributori** o **Importatori** secondo l'AI Act.

### Profili di Rischio e Condotte Critiche:

- **Mancata verifica delle misure di sicurezza del produttore:** Commercializzare sistemi IA ad alto rischio privi della documentazione tecnica di conformità o senza verificare le garanzie sul controllo umano espone l'ente distributore a responsabilità concorsuale o diretta per *omessa adozione di misure idonee*.
- **Alterazione o errata riconfigurazione:** Se la società di commercializzazione modifica i parametri di fabbrica dell'IA per adattarla ai clienti, può essere riqualificata giuridicamente come "Fornitore/Produttore", rispondendo direttamente di eventuali vizi di sicurezza e dell'art. 437-bis c.p.

### Presidi nel Modello 231 per il Commercio:

- Attuazione di rigorosi protocolli di *Due Diligence sui fornitori tecnologici*.
- Procedure trasparenti per il richiamo dal mercato di sistemi IA difettosi o vulnerabili ad attacchi informatici.
- Divieto assoluto di pubblicità ingannevole (es. tramite Deepfake ex art. 612-quater c.p.).

## 04. Focus Settoriale: Imprese che Producono & Manifattura

### Sicurezza sul Lavoro e Omissione di Controllo Umano su Macchinari e Processi

Nel settore manifatturiero e dell'Industria 4.0/5.0, l'integrazione di algoritmi IA all'interno di robotica collaborativa (cobot), linee di assemblaggio automatizzate, carrelli a guida autonoma (AGV) e impianti di produzione rappresenta il fronte più critico per la **sicurezza sul lavoro (D.Lgs. 81/2008)** e per la **responsabilità penale 231**.

#### FLUSSO DEL RISCHIO PENALE E SANGUINOSO IN FABBRICA

[ Sistema IA ad Alto Rischio ]



**Omissione Sorveglianza Umana**

(Disattivazione sensori / Alert ignorati / Automation Bias)



**Pericolo Concreto Incolumità**

(Rischio d'infortunio in catena di montaggio / Annullamento spazi di frenata)



**REATO ex Art. 437-bis c.p. + Sanzioni 231 all'Ente (fino a € 1,5 Mln)**

### Modalità Concrete di Commissione del Reato in Fabbrica:

#### 1. Omissione della Sorveglianza Umana sui Macchinari (*Automation Bias*):

- Abbandono del presidio o disattivazione degli allarmi sonori/visivi da parte dei preposti perché ritenuti ostacolo al ritmo produttivo.
- Affidamento cieco a sistemi di *Computer Vision* o algoritmi predittivi che gestiscono la fermata d'emergenza delle macchine senza mantenere una supervisione umana (*Human-in-the-Loop* o *Human-on-the-Loop*).

#### 2. Manomissione e Bypassing dei Sensori di Sicurezza:

- Forzatura dei parametri dell'algoritmo che governa bracci robotici o macchine utensili per aumentarne la velocità di lavoro, annullando i margini di frenata o di rilevamento del personale all'interno delle celle di lavoro.

#### 3. Mancato Aggiornamento Tecnico e Manutenzione dei Modelli IA:

- Utilizzo di software di manutenzione predittiva non aggiornati con le relative *patch* di sicurezza, con conseguente errata diagnosi dei guasti meccanici e potenziale cedimento improvviso di parti di impianto.

### Adempimenti Indispensabili per le Imprese Produttive:

- **Integrazione del DVR (Documento di Valutazione dei Rischi):** Mappatura specifica dei rischi derivanti da interazione uomo-macchina guidata da IA ex D.Lgs. 81/2008 e Regolamento Macchine.
- **Protocolli di Controllo Umano Effettivo:** Definizione formale di ruoli, turni e procedure operative che garantiscano il potere di intervento d'emergenza e l'arresto manuale prioritario rispetto alla decisione algoritmica.

- **Formazione Obbligatoria degli Operatori:** Addestramento del personale di linea sui limiti dell'IA per contrastare l'assuefazione all'automazione.

## 05. Focus Operativo: Servizi, PA e Gestione Documentale

---

### L' "Utilizzo Professionale" dell'IA (*Deployer*)

La norma colpisce non solo chi sviluppa l'IA, ma chiunque ne faccia un **utilizzo professionale**, escludendo solo l'uso personale o domestico:

- **Aziende di servizi e datori di lavoro:** Integrazione di IA per gestione personale, monitoraggio o efficientamento processi.
- **Professionisti:** Avvocati, commercialisti, ingegneri, medici che usano l'IA come supporto decisionale o per la redazione di pareri, consulenze e atti.
- **Pubblica Amministrazione:** Enti che impiegano algoritmi nell'istruttoria dei procedimenti amministrativi, nel supporto decisionale agli organi deliberanti, nell'erogazione di servizi o nella valutazione degli utenti.
- **Utilizzo per Studio e Approfondimento (PA e Professionisti):** L'impiego dell'IA per lo studio, la ricerca e l'approfondimento normativo, tecnico o scientifico costituisce un'estensione dell'attività professionale/istituzionale. Ai fini dell'art. 437-bis c.p., tale utilizzo **non genera di per sé rischio penale** in quanto privo del requisito del *pericolo concreto per l'incolumità*, salvo il caso in cui l'analisi venga trasfusa senza controllo umano in procedimenti ad alto rischio o comporti la violazione del GDPR e del segreto d'ufficio/aziendale.

### Il Rischio nell'Elaborazione Documentale

Nel lavoro ordinario d'ufficio (traduzioni, sintesi email, bozze non critiche) il rischio penale ex art. 437-bis **è nullo** poiché manca il presupposto del *pericolo concreto per l'incolumità*.

Tuttavia, l'elaborazione documentale tramite LLM rientra nell'**Alto Rischio Penale** se applicata a contesti sensibili:

- **Medicina:** Elaborazione di referti per diagnosi o dosaggi farmaceutici.
- **Infrastrutture Critiche:** Analisi di report di manutenzione (dighe, reti elettriche, trasporti).
- **Giustizia e PA:** Valutazione di individui, ordine pubblico o rischio di recidiva.

### Rischi Extra-Penali: Privacy (GDPR) e Responsabilità Civile

- **Sanzioni Privacy (GDPR):** L'inserimento di dati di persone fisiche (dipendenti, clienti, pazienti) in sistemi IA commerciali non protetti espone l'azienda a sanzioni del Garante fino a **20 milioni di euro o al 4% del fatturato globale**. I dati aziendali puramente societari (es. bilanci, P.IVA) esulano dal GDPR ma pongono gravi rischi di violazione del **Segreto Industriale**.
- **Responsabilità Civile:** L'affidamento cieco a report o contratti redatti da IA affetti da "allucinazioni" (errori o fatti inventati) comporta responsabilità civile diretta per danni economici causati a terzi o clienti.

**CONCLUSIONI PER LA COMPLIANCE AZIENDALE**

La responsabilità dell'ente corre alla velocità dell'algoritmo. Per evitare sanzioni pecuniarie ed interdittive ex D.Lgs. 231/2001, le imprese devono adeguare tempestivamente i propri **Modelli Organizzativi 231**, mappando le tecnologie IA in uso ed istituendo presidi concreti di sorveglianza e sicurezza.