



Studio Previti
ASSOCIAZIONE PROFESSIONALE

AI e Responsabilità 231

Perché i Modelli Organizzativi vanno aggiornati

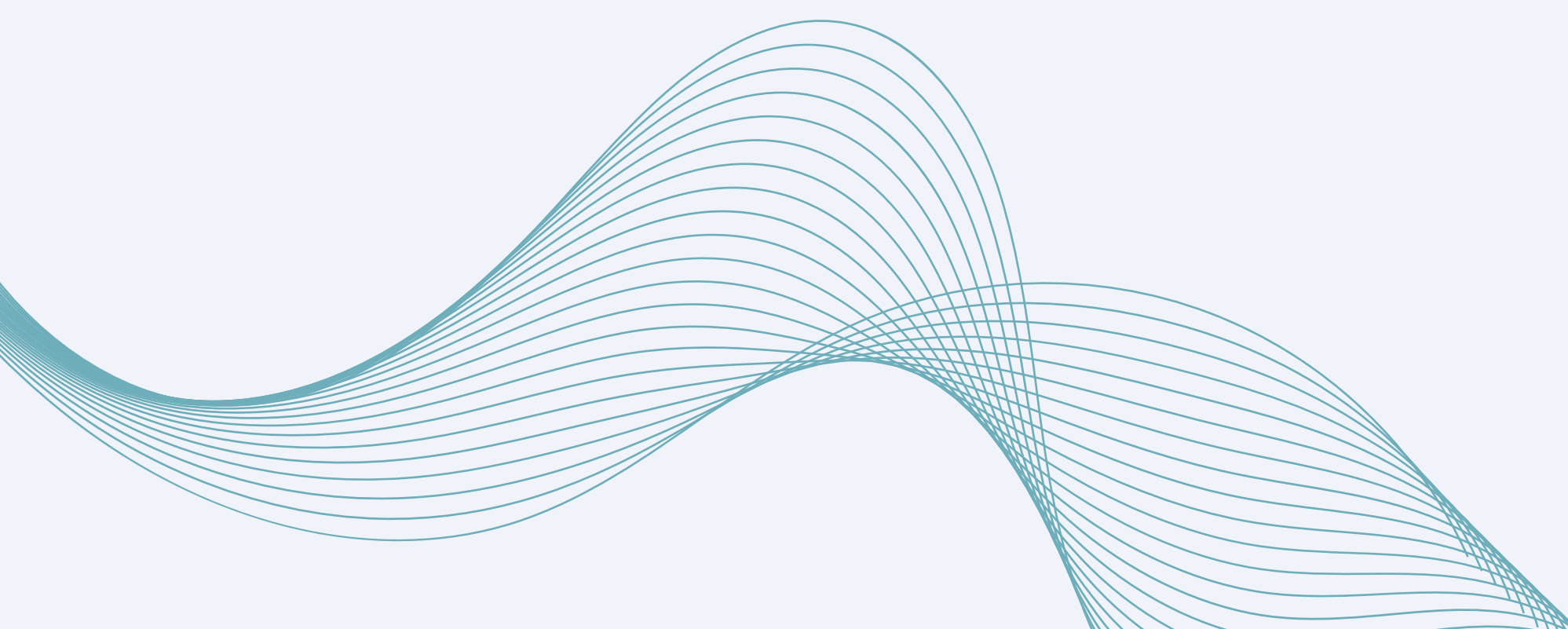
L'AI è già nei processi aziendali.

Selezione del personale, acquisti, controllo di gestione, marketing predittivo.

Meno immediato, ma altrettanto concreto, è l'impatto che questi strumenti hanno sul sistema di responsabilità amministrativa degli enti previsto dal D.Lgs. 231/2001.

La domanda che ogni responsabile compliance deve porsi:

“Il Modello 231 è ancora idoneo a prevenire i reati quando parte delle decisioni è affidata ad algoritmi?”



L'AI non crea nuovi reati.

Ciò che cambia è la modalità con cui i reati già previsti dal D.Lgs. 231/2001 si realizzano — spesso in forme meno visibili rispetto alla condotta umana diretta.

Il filo conduttore: quando una decisione è supportata da un algoritmo, il problema è capire chi ne risponde e se l'ente aveva predisposto controlli adeguati a prevenire l'uso distorto o non vigilato di quello strumento.

4 aree dove l'AI amplifica il rischio-reato

Procurement e gare pubbliche

Sistemi AI mal calibrati o addestrati su dati distorti possono produrre forme di corruzione o turbativa.
Rilevanza: reati contro la PA.

Dati e cybersicurezza

L'elaborazione massiva di informazioni aumenta l'esposizione ai delitti informatici (art. 24-bis) quando i sistemi trasferiscono dati senza controlli adeguati.

Gestione finanziaria e contabile

Algoritmi predittivi non supervisionati possono contribuire a rappresentazioni non veritiere rilevanti ai fini dei reati societari.

Sicurezza sul lavoro

AI per safety management seguita acriticamente senza verifica umana effettiva: possibili riflessi sui reati di cui all'art. 25-septies.

“

Quando una decisione aziendale è supportata o generata da un algoritmo, si pone il problema di chi ne risponde e, soprattutto, se l'ente avesse predisposto controlli adeguati a prevenire l'uso distorto o non vigilato di quello strumento.

”

Il raccordo con l'AI Act

In vigore dall'1° agosto 2024. Per i sistemi di AI classificati ad alto rischio impone obblighi che si sovrappongono, nella sostanza, a ciò che un Modello 231 dovrebbe già prevedere.

Gestione
del rischio

Qualità
dei dati

Documentazione
e trasparenza

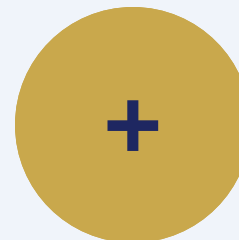
Sorveglianza
umana

Le imprese che adeguano la propria governance all'AI Act hanno l'opportunità di procedere in parallelo con l'aggiornamento del Modello 231, costruendo un sistema di controllo interno coerente in cui i presidi si rafforzano reciprocamente.

Un percorso unico, senza duplicazioni.

Adeguamento all'AI Act

Obblighi di governance, trasparenza e sorveglianza per i sistemi ad alto rischio ai sensi del Reg. UE 2024/1689.



Aggiornamento Modello 231

Presidi preventivi calibrati sui nuovi rischi introdotti dall'uso di sistemi algoritmici nei processi aziendali.

I presidi si rafforzano reciprocamente.

SCHEMA APPROVATO IN VIA PRELIMINARE — NON ANCORA VIGENTE

10 giugno 2026

Il Consiglio dei Ministri approva in via preliminare uno schema di decreto attuativo del Reg. UE 2024/1689 e della L. 23 settembre 2025, n. 132.

Art. 17 — Introduce nel D.Lgs. 231/2001 il nuovo:

Art. 25-vicies — Reati commessi con l'uso di sistemi di intelligenza artificiale

L'iter parlamentare è in corso e il testo potrà essere modificato prima dell'approvazione definitiva.

I due nuovi reati presupposto

Art. 437-bis c.p.

Omessa adozione di misure tecniche idonee a prevenire malfunzionamenti o alterazioni di un sistema di AI ad alto rischio, quando ne derivi un pericolo concreto per la vita o l'incolumità individuale.

Aggravante se il pericolo riguarda l'incolumità pubblica o la sicurezza dello Stato.

Comma 2: ipotesi commissiva dolosa per l'alterazione del sistema.

Art. 612-quater c.p.

Cessione, pubblicazione o diffusione non consensuale di contenuti generati o alterati con sistemi di AI — deepfake: immagini, video o voci — quando ne derivi un danno alla persona ritratta.

Il meccanismo di imputazione all'ente resta quello ordinario

Artt. 5, 6 e 7 D.Lgs. 231/2001 — schema invariato rispetto agli altri reati presupposto

1

Soggetto qualificato

Il reato è commesso da un soggetto apicale o subordinato all'ente.

2

Interesse o vantaggio

La condotta avviene nell'interesse o a vantaggio dell'ente.

3

Carenza organizzativa

La commissione è stata resa possibile da una carenza organizzativa dell'ente: la cosiddetta colpa di organizzazione.

3 ordini di problemi interpretativi

Riflessioni su una norma non ancora in vigore, destinate a confrontarsi con la prassi applicativa.

1

Imputazione dell'omissione

A chi va imputata l'omissione delle misure di sicurezza? Allo sviluppatore, all'assemblatore o all'ente utilizzatore? Il paradigma della responsabilità da prodotto difettoso appare poco adatto a sistemi che modificano nel tempo il proprio comportamento.

2

Imprevedibilità algoritmica — Black box

L'apprendimento automatico rende difficile individuare la colpa di organizzazione, con il rischio — segnalato in dottrina — di scivolare verso forme di responsabilità sostanzialmente oggettiva.

3

Art. 8 D.Lgs. 231/2001

Se manca il reato per difetto di colpevolezza dell'individuo, viene meno anche il presupposto della responsabilità dell'ente. Un'estensione sarebbe analogia in malam partem: non ammessa nel diritto penale.

I 3 livelli di intervento

Livello 1 — Ricognizione

Mappare tutti i sistemi AI in uso o in sviluppo e classificarli secondo l'AI Act, distinguendo il ruolo dell'ente come fornitore o come utilizzatore. Il tipo di sistema e il ruolo determinano insieme gli obblighi normativi e la natura dei rischi-reato.

Livello 2 — Governance interna

Linee guida formalmente adottate dal vertice aziendale, con attribuzione di ruoli e responsabilità, reportistica periodica sui sistemi ad alto rischio e procedure per la gestione dei rischi e degli incidenti. Possibile istituzione di un AI Governance Officer.

Livello 3 — Aggiornamento Modello 231

Risk assessment specifico, protocolli con verifica umana effettiva, tracciabilità di dati e decisioni, clausole contrattuali con i fornitori, formazione mirata al personale, aggiornamento del Codice Etico e dei flussi informativi verso l'OdV.

4 direttrici per l'aggiornamento del Modello

Risk assessment specifico per AI

Pesare il rischio anche in base all'opacità algoritmica, alla qualità dei dati di addestramento e al grado di autonomia decisionale lasciato alla macchina.

Protocolli con verifica umana effettiva

Disciplinare adozione, configurazione e utilizzo degli strumenti di AI. La validazione non può essere una mera presa d'atto formale dell'output del sistema.

Tracciabilità

Ricostruire quali dati sono stati utilizzati, quale versione del sistema ha prodotto un output e chi ha validato la decisione finale. Presupposto per il controllo dell'OdV.

Gestione dei fornitori terzi

Clausole contrattuali che impongano trasparenza sul funzionamento, sugli aggiornamenti e sulle modalità di addestramento, con possibilità di audit da parte dell'OdV.

Da fare subito

- ✓ Ricognizione di tutti i sistemi AI in uso e classificazione per area di rischio (AI Act)
- ✓ Verifica della rilevanza rispetto ai reati presupposto, inclusa la futura fattispecie dell'art. 25-vicies
- ✓ Controllo dei protocolli di validazione umana per le decisioni automatizzate
- ✓ Revisione delle clausole contrattuali con i fornitori di tecnologia AI
- ✓ Verifica della formazione erogata al personale che utilizza questi strumenti
- ✓ Aggiornamento dei flussi informativi verso l'Organismo di Vigilanza (mappatura AI, audit, anomalie)
- ✓ Monitoraggio dell'iter parlamentare del decreto che introduce l'art. 25-vicies

L'AI non è un rischio nuovo.

È un moltiplicatore dei rischi esistenti — spesso meno visibili e più difficili da attribuire.

L'aggiornamento del Modello Organizzativo non è un adempimento formale.

È un'occasione per costruire una governance più solida, capace di tenere insieme innovazione tecnologica e prevenzione del rischio-reato.



Studio Previti

ASSOCIAZIONE PROFESSIONALE

www.previti.it



06.2324623
02.795587



contatti@previti.it



Via Cicerone 60 - 00193 Roma
Via Stradivari 4 - 20131 Milano

