CIRCOLARE 8 SETTEMBRE 2026

D.Lgs. 231/2001 – L'intelligenza artificiale entra nella lista dei reati presupposto

Avv. Luca Degani – Avv. Alice Stendardo
Dott. Alberto Casaccio



D.Lgs. 231/2001 – L'intelligenza artificiale entra nella lista dei reati presupposto

Avv. Luca Degani –Avv. Alice Stendardo – Dott. Alberto Casaccio

Gentili Clienti,

l'intelligenza artificiale entra ufficialmente nel catalogo dei reati presupposto del D.Lgs. 231/2001. Con l'approvazione del decreto legislativo di adeguamento al Regolamento (UE) 2024/1689 (AI Act), adottato in attuazione della delega prevista dall'art. 24 della legge n. 132/2025, viene introdotto un nuovo profilo di responsabilità amministrativa per gli enti che progettano, sviluppano o utilizzano professionalmente sistemi di intelligenza artificiale, in particolare quelli qualificati come ad alto rischio, ossia i sistemi che, secondo l'AI Act, possono incidere sulla salute, sulla sicurezza o sui diritti fondamentali delle persone e sono, quindi, soggetti a obblighi particolarmente rigorosi di gestione del rischio, sicurezza e sorveglianza umana. Si precisa, tuttavia, che il provvedimento è attualmente in attesa di pubblicazione in Gazzetta Ufficiale, alla quale seguirà la sua entrata in vigore definitiva. Si tratta, in ogni caso, di una **novità** destinata ad avere un impatto concreto sui **Modelli 231**, che dovranno essere aggiornati per tenere conto dei nuovi obblighi di sicurezza, controllo e governance dei sistemi di IA.

Il decreto modifica il D.Lgs. 8 giugno 2001, n. 231, **introducendo il nuovo art. 25-vicies**, che richiama **il reato** previsto dal nuovo **art. 437-bis** del codice penale, rubricato "*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi"*. La norma punisce chi omette di adottare le misure tecniche e organizzative necessarie a garantire la sicurezza dei sistemi di IA ad alto rischio nelle fasi di progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale, nonché chi omette la sorveglianza umana richiesta dalla disciplina europea. È, inoltre, sanzionata l'alterazione illecita del funzionamento di tali sistemi da parte di soggetti esterni. Le pene variano in funzione della gravità del pericolo generato e sono previste anche specifiche ipotesi di responsabilità colposa.

Per gli enti la responsabilità è particolarmente significativa. Il nuovo art. 25-vicies prevede una sanzione pecuniaria da 600 a 1.000 quote[1], mentre per il delitto di ***deepfake*** – introdotto con il nuovo

[1]Nel sistema del D.Lgs. 231/2001 le *quote* rappresentano l'unità di calcolo della sanzione economica: il giudice determina sia il numero delle quote, in base alla gravità del fatto, sia il valore di ciascuna quota, tenendo conto delle condizioni economiche dell'ente.

art. 612-quater c.p. – è prevista una sanzione da 200 a 700 quote. In entrambi i casi possono trovare applicazione le principali sanzioni interdittive previste dall'art. 9 del D.Lgs. 231/2001, tra cui la sospensione o revoca di autorizzazioni, il divieto di contrattare con la pubblica amministrazione, l'esclusione da agevolazioni e finanziamenti e il divieto di pubblicizzare beni o servizi. Il rischio, quindi, non riguarda soltanto chi sviluppa sistemi di IA, ma anche tutti gli enti che li utilizzano nello svolgimento della propria attività, **anche quando tali sistemi siano forniti da soggetti terzi**, come avviene sempre più frequentemente nelle nostre realtà.

L'aspetto più rilevante è però un altro, infatti, **questa novità** non si aggiunge semplicemente agli obblighi già esistenti, ma **si intreccia con altri ambiti della compliance**. I sistemi di IA ad alto rischio trattano nella maggior parte dei casi dati personali e restano quindi soggetti anche al **Regolamento (UE) 2016/679 (GDPR),** che impone una base giuridica per il trattamento, valutazioni d'impatto e adeguate misure di sicurezza. Per gli enti che rientrano nel relativo ambito di applicazione, si aggiungono, inoltre, gli obblighi previsti dal **D.Lgs. 138/2024** di recepimento della direttiva **NIS2,** in materia di gestione del rischio informatico e notifica degli incidenti.

Ne consegue che **un unico incidente** di sicurezza che coinvolga un sistema di intelligenza artificiale **può, oggi, attivare contemporaneamente tre distinti regimi di responsabilità**: gli obblighi di notifica al Garante Privacy entro 72 ore previsti dal GDPR, gli obblighi di segnalazione al CSIRT Italia previsti dalla NIS2 e, qualora l'incidente sia riconducibile all'omessa adozione delle misure tecniche di sicurezza richieste, anche la responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001. Privacy, cybersicurezza e responsabilità 231 diventano, così, elementi di un unico sistema di compliance e richiedono un coordinamento sempre più stretto.

Alla luce di queste novità, è opportuno verificare se il Modello di organizzazione, gestione e controllo sia adeguato ai rischi connessi all'utilizzo dell'intelligenza artificiale, aggiornando la mappatura delle attività che impiegano sistemi di IA, i protocolli di controllo e di sorveglianza umana previsti dall'AI Act e il coordinamento con gli adempimenti in materia di protezione dei dati personali e di gestione del rischio informatico.

Restiamo a disposizione per approfondire l'impatto di queste novità sulla vostra organizzazione.

Cordiali saluti.