FAZZINI HOLZMILLER & PARTNERS

News 10/2026

Modello 231 e intelligenza artificiale: nuove aree di rischio e strumenti di tutela per le imprese

19 Novembre 2026 • D.Lgs. 231/2001 e D.Lgs. 160/2026

PREMESSA 2
CHE COS'È IL MODELLO 231 E A CHI SI RIVOLGE 2
LE NOVITÀ: L'INTELLIGENZA ARTIFICIALE ENTRA NEL PERIMETRO 231 3
IL SUPPORTO DI FHP 3

NOTA BENE - Le informazioni contenute nella presente circolare sono fornite con l'intendimento che non possano essere interpretate come prestazioni di consulenza legale, contabile, fiscale o di altra natura professionale. Il contenuto ha finalità esclusivamente divulgativa generale e non può sostituire incontri con consulenti fiscali, legali o professionali di altra natura. Prima di adottare scelte o provvedimenti, è necessario consultare consulenti professionali qualificati
Le informazioni contenute nella presente circolare sono di proprietà di Fazzini Holzmiller & Partners e possono essere usate esclusivamente a fini personali e interni; è vietato copiarle, inoltrarle o fornirle comunque a terzi.

PREMESSA

Gentile Cliente,

la disciplina sulla responsabilità degli enti prevista dal D.Lgs. 8 giugno 2001, n. 231 assume crescente rilievo anche per le imprese che utilizzano strumenti di intelligenza artificiale (IA). Le recenti novità legislative offrono l'occasione per ricordare cosa sia il Modello 231, quali tutele possa offrire e quando sia opportuno aggiornarlo.

CHE COS'È IL MODELLO 231 E A CHI SI RIVOLGE

Il D.Lgs. 231/2001 prevede una responsabilità amministrativa dell'ente, accertata dal giudice penale, per determinati reati commessi nel suo interesse o a suo vantaggio da amministratori, dirigenti e altri soggetti apicali, oppure da persone sottoposte alla loro direzione o vigilanza. La responsabilità dell'ente si aggiunge a quella penale della persona fisica che ha commesso il reato.

La disciplina interessa, in particolare, società di capitali e di persone, cooperative, consorzi e associazioni, anche prive di personalità giuridica, indipendentemente dalla dimensione. Sono previste specifiche esclusioni per lo Stato, determinati enti pubblici e gli enti con funzioni di rilievo costituzionale. Non è quindi una materia riservata alle grandi imprese.

La prevenzione si fonda sulla mappatura dei rischi: individuare le attività aziendali nelle quali potrebbero essere commessi i reati rilevanti, valutare i presidi già esistenti e introdurre procedure, deleghe, controlli, flussi informativi, formazione e un sistema disciplinare coerenti con il rischio. Questi elementi confluiscono nel Modello di organizzazione, gestione e controllo (Modello 231), sul cui funzionamento vigila un Organismo di Vigilanza (OdV), dotato dei requisiti previsti dalla legge.

Le principali aree di rischio da esaminare, in funzione dell'operatività aziendale, comprendono rapporti con la Pubblica Amministrazione e corruzione, reati societari, reati tributari, salute e sicurezza sul lavoro, ambiente, riciclaggio e autoriciclaggio, criminalità informatica e trattamento illecito dei dati, oltre a specifici reati in materia di mercato, industria e commercio e altri previsti dal catalogo 231.

Il beneficio è rilevante: nelle condizioni stabilite dagli artt. 6 e 7 del Decreto, l'adozione e l'efficace attuazione preventiva di un Modello idoneo possono consentire all'ente di andare esente da responsabilità per il reato presupposto. È questa la cosiddetta "copertura penale", espressione di uso corrente ma non equivalente a una garanzia automatica. Il Modello, inoltre, aiuta a ridurre il rischio di violazioni, rafforzare i processi decisionali e limitare l'esposizione dell'impresa a sanzioni pecuniarie e interdittive, fermo restando che non elimina la responsabilità personale degli autori dei reati.

LE NOVITÀ: L'INTELLIGENZA ARTIFICIALE ENTRA NEL PERIMETRO 231

Dal 30 settembre 2026 il D.Lgs. 9 settembre 2026, n. 160 ha inserito l'art. 25-vicies nel D.Lgs. 231/2001, richiamando due reati presupposto specificamente connessi all'IA. La novità non comporta che qualsiasi errore di un sistema IA generi responsabilità 231: occorre la realizzazione degli elementi del reato e la ricorrenza dei presupposti di imputazione all'ente.

• Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di IA e alterazione illecita dei sistemi. La norma riguarda, tra l'altro, omissioni di misure tecniche di sicurezza o di sorveglianza umana nell'ambito di sistemi di IA "ad alto rischio", quando ne derivi un pericolo per la vita o l'incolumità pubblica o individuale; contempla inoltre l'alterazione illecita di tali sistemi e specifiche condotte dell'utilizzatore professionale. Per "alto rischio" non si intende semplicemente un software complesso: si tratta di sistemi ricompresi nelle categorie individuate dall'AI Act europeo, in settori e impieghi sensibili. Un esempio può essere un sistema impiegato in un processo critico per la sicurezza, senza i controlli umani e tecnici richiesti. Per l'ente: sanzione pecuniaria da 600 a 1.000 quote.

• Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con IA. Riguarda la cessione, pubblicazione o diffusione senza consenso di immagini, video o voci falsificati con IA, idonei a ingannare sulla loro autenticità, quando ciò cagioni un danno ingiusto a una persona. È il fenomeno dei "deepfake": per esempio, un video o una registrazione vocale artificiale che attribuisca a una persona dichiarazioni mai rese. Il rischio può interessare comunicazione, marketing, social media e gestione del personale. Per l'ente: sanzione pecuniaria da 200 a 700 quote.

Per entrambe le fattispecie sono inoltre previste sanzioni interdittive, tra cui la sospensione o revoca di autorizzazioni, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni e il divieto di pubblicizzare beni o servizi. La commissione del fatto da parte di un dipendente o fornitore non comporta, da sola, responsabilità della società: occorre verificare anche il collegamento qualificato con l'ente e gli altri requisiti del D.Lgs. 231/2001.

Anche le imprese che acquistano e utilizzano soluzioni IA, senza svilupparle, dovrebbero quindi verificare gli strumenti adottati, la loro funzione, gli eventuali utilizzi ad alto rischio e le regole applicate a contenuti sintetici, fornitori e agenzie esterne. Restano inoltre da considerare i reati informatici già inclusi nel sistema 231 e le altre fattispecie che possono essere agevolate dall'uso dell'IA.

IL SUPPORTO DI FHP

Il nostro Studio è già attivo nell'identificazione e nella mappatura dei rischi aziendali rilevanti ai fini del D.Lgs. 231/2001, nonché nel coordinamento delle attività necessarie alla predisposizione e all'aggiornamento dei Modelli organizzativi, in collaborazione, ove necessario, con professionalità specialistiche.

Tale attività comprende anche l'analisi dei rischi collegati all'intelligenza artificiale e ai reati informatici: ricognizione dei processi e degli strumenti utilizzati, valutazione dell'esposizione alle nuove fattispecie, aggiornamento dei protocolli di controllo e coordinamento con le funzioni aziendali e l'Organismo di Vigilanza.

Qualora desideriate valutare per la prima volta l'adozione di un Modello 231 oppure verificare se quello già in uso necessiti di integrazioni alla luce dei reati recentemente introdotti, rimaniamo a disposizione per un primo confronto e per definire un percorso di intervento proporzionato alle caratteristiche della Vostra organizzazione.

****





Per essere costantemente aggiornati sulle principali novità fiscali, oltre che sugli eventi ed articoli ad opera dei professionisti del nostro Studio, vi invitiamo a seguirci ***sul nostro canale Linkedin****:* *www.linkedin.com/company/fazziniholzmillerpartners*

****

Con i migliori saluti. **Fazzini Holzmiller & Partners**

Riferimenti essenziali: D.Lgs. 231/2001, artt. 5–7, 9, 24-bis e 25-vicies; D.Lgs. 160/2026, artt. 12 e 15; c.p., artt. 437-bis e 612-quater; L. 132/2025, art. 26; Reg. (UE) 2024/1689 (AI Act).