



Intelligenza artificiale: pubblicato il d.lgs. 160/2026 in materia penale e di responsabilità da reato degli enti

1. Premessa

Lo scorso 15 settembre è stato pubblicato nella Gazzetta Ufficiale il d.lgs. 160/2026, attuativo dell'AI Act.

La norma, che entrerà in vigore il prossimo 30 settembre, introduce definitivamente nel codice penale il nuovo reato di **“Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi” (art. 437-bis c.p.)**, rilevante anche ai fini della responsabilità degli enti, ai sensi del nuovo art. 25-vicies del d.lgs. 231/2001, insieme al reato sul c.d. “deepfake” (art. 612-quater c.p.).

2. Il nuovo reato di omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi (art. 437-bis c.p.)

La disposizione, come definitivamente approvata, prevede quanto segue.

Omessa adozione di misure di sicurezza (comma 1). È punito con la reclusione da uno a cinque anni chi, nella progettazione, nell'addestramento, nella produzione o nell'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, omette di adottare le misure tecniche di sicurezza idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi, ovvero omette di adottare misure di sorveglianza umana, quando da tali omissioni derivi un pericolo per la vita o l'incolumità pubblica o individuale. Se dal fatto deriva un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni.

Alterazione illecita dei sistemi (comma 2). Salvo che il fatto costituisca più grave reato, è punito con la reclusione da due a sei anni chi, al di fuori dei casi di cui al comma 1, altera sistemi di intelligenza artificiale ad alto rischio, quando dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale; la pena è della reclusione da tre a dieci anni se il pericolo riguarda la sicurezza dello Stato.

Colpa grave (comma 3). Se i fatti omissivi previsti dal comma 1 sono commessi per colpa grave, la pena è ridotta da un terzo a un sesto.

Utilizzatore professionale (comma 4). L'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio che omette intenzionalmente di adottare misure di sorveglianza umana è punito con le pene previste dal comma 1, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, un pericolo per la vita o l'incolumità pubblica o individuale ovvero un pericolo per la sicurezza dello Stato.

Entrambe le fattispecie si applicano esclusivamente ai sistemi di intelligenza artificiale ad alto rischio, ai sensi dell'art. 3 dell'AI Act, e sono strutturate come reati di pericolo concreto, la cui rilevanza penale è subordinata alla derivazione, dalla condotta, di un pericolo effettivo per i beni tutelati dalla norma (vita, incolumità individuale o pubblica, sicurezza dello Stato). Il trattamento sanzionatorio resta improntato a un criterio di proporzionalità, con pene più severe quando il pericolo si estende a beni di rango collettivo.

3. Le modifiche al d.lgs. 231/2001: il nuovo art. 25-vicies

L'art. 15 del d.lgs. 160/2026 inserisce nel d.lgs. 8 giugno 2001 n. 231 il nuovo art. 25-vicies, rubricato **“Reati commessi con l'uso di sistemi di intelligenza artificiale”**. La disposizione, nel testo definitivo, ricomprende due fattispecie di reato presupposto:

- il delitto di cui al nuovo **art. 437-bis c.p.** (omessa adozione di misure di sicurezza nei sistemi di IA e alterazione illecita dei sistemi), per il quale è prevista, in capo all'ente, la sanzione pecuniaria da seicento a mille quote;
- il delitto di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale, c.d. “deep-fake” (**art. 612-quater c.p.**), introdotto dalla legge 132/2025, per il quale è prevista la sanzione pecuniaria da duecento a settecento quote.

In entrambi i casi, l'art. 25-vicies richiama le sanzioni interdittive di cui all'art. 9, comma 2, lettere b), c), d) ed e), del d.lgs. 231/2001: sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la Pubblica Amministrazione; esclusione da agevolazioni, finanziamenti, contributi o sussidi, con eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

La scelta di collocare le nuove fattispecie in un autonomo art. 25-vicies, piuttosto che ricondurle al già esistente art. 24-bis in materia di delitti informatici, conferma che l'intelligenza artificiale viene ormai considerata una specifica e autonoma area di rischio organizzativo ai fini 231.

4. Impatti sull'aggiornamento dei modelli 231 e sull'attività dell'odv

L'entrata in vigore dell'**art. 25-vicies** impone agli enti che utilizzano sistemi di IA una valutazione del relativo impatto sul Modello 231, che non può limitarsi al mero inserimento formale dei nuovi reati presupposto.

Il primo passaggio deve consistere in un censimento dei sistemi di IA effettivamente in uso, del ruolo assunto dall'ente nella filiera (fornitore, importatore, distributore, deployer) e dell'eventuale qualificazione come sistemi “ad alto rischio”, con particolare attenzione alle attività di progettazione, addestramento, produzione, immissione sul mercato e utilizzo professionale richiamate dall'art. 437-bis c.p.

Occorrerà poi mappare i processi e le attività sensibili, non solo in relazione alle nuove fattispecie, ma anche considerando che l'impiego degli strumenti di IA censiti possa costituire una modalità di commissione di altri reati presupposto già rilevanti ai fini del d.lgs. 231/2001: l'intelligenza artificiale diviene, in questa prospettiva, una possibile modalità di commissione dei vari reati 231, oltre che delle fattispecie di cui agli artt. 437-bis e 612-quater c.p.

Una volta mappato il rischio 231, andrà verificata l'adeguatezza dei controlli esistenti, resolvendo le eventuali carenze riscontrate. Un presidio centrale è certamente la sorveglianza umana, da tracciare in termini di soggetti responsabili, competenze, momenti di intervento ed evidenza documentale; sul fronte dell'art. 612-quater c.p., andranno inoltre regolati i processi di utilizzo dell'IA generativa per contenuti manipolabili (deep-fake).

Non potrà mancare, infine, la ridefinizione dei percorsi di formazione per la popolazione aziendale, volti ad assicurare una piena consapevolezza delle potenzialità e dei limiti dei sistemi di intelligenza artificiale e delle responsabilità connesse - obbligo già previsto dall'art. 4 dell'AI Act (la c.d. “AI literacy”) - da integrare necessariamente con contenuti di sensibilizzazione sui rischi di commissione dei reati presupposto 231.

Sul piano della vigilanza, l'OdV dovrà necessariamente verificare quanto sopra indicato, calibrandone la portata sull'effettiva esposizione dell'ente.

Questo complesso di attività, oltre a minimizzare il rischio di commissione di reati tramite l'utilizzo di sistemi di IA, consente all'ente di predisporre una solida linea di difesa, dimostrando di aver fatto quanto ragionevolmente possibile per prevenirne la commissione, sia in caso di contestazione dei reati di cui agli artt. 437-bis e 612-quater c.p., sia in relazione ai diversi reati presupposto che possano essere commessi mediante l'utilizzo di sistemi di intelligenza artificiale.

Il presente documento viene consegnato esclusivamente per fini divulgativi. Esso non costituisce riferimento alcuno per contratti e/o impegni di qualsiasi natura.

Per ogni ulteriore chiarimento o approfondimento Vi preghiamo di contattare:

Ciro Pellegrino
Partner

Responsabile Dipartimento di
Diritto Penale Societario
Roma
+39 06 478751
cpellegrino@gop.it



INFORMATIVA EX ART. 13 del Reg. UE 2016/679 - Codice in materia di protezione dei dati personali

I dati personali oggetto di trattamento da parte dallo studio legale Gianni & Origoni (lo "Studio") sono quelli liberamente forniti nel corso di rapporti professionali o di incontri, eventi, workshop e simili, e vengono trattati anche per finalità informative e divulgative. La presente newsletter è inviata esclusivamente a soggetti che hanno manifestato il loro interesse a ricevere informazioni sulle attività dello Studio. Se Le fosse stata inviata per errore, ovvero avesse mutato opinione, può opporsi all'invio di ulteriori comunicazioni inviando una e-mail all'indirizzo: relazioniesterne@gop.it. Titolare del trattamento è lo studio Gianni & Origoni, con sede amministrativa in Roma, Via delle Quattro Fontane 20.