9 Luglio 2026

Intelligenza artificiale: approvato lo schema di decreto legislativo in materia penale e di responsabilità da reato degli enti

1. Premessa

Nella seduta del 10 giugno 2026, il Consiglio dei ministri ha approvato due schemi di decreto legislativo relativi all'adeguamento della normativa nazionale al Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (c.d. AI Act), in attuazione delle deleghe conferite dalla legge 23 settembre 2025, n. 132, recante "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*". Il testo approvato in via preliminare dal Governo è ora sottoposto al parere delle competenti commissioni parlamentari. Il presente contributo si concentra sulle disposizioni penalistiche di maggiore interesse per le imprese: l'introduzione della nuova fattispecie di reato di **"*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*" (art. 437 bis c.p.) e l'ampliamento del catalogo dei reati rilevanti per la responsabilità degli enti** ai sensi del d.lgs. 8 giugno 2001, n. 231.

2. Il nuovo reato di cui all'art. 437-bis c.p.

L'art. 12 dello schema introduce nel codice penale il nuovo art. 437-*bis*, rubricato "***Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi***".

La disposizione prevede due distinte fattispecie:

- La prima fattispecie (comma 1) punisce "*chiunque, nella progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio, omette misure tecniche idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette misure di sorveglianza umana*", qualora dal fatto derivi un pericolo concreto per la vita o l'incolumità individuale (reclusione da uno a cinque anni), ovvero per l'incolumità pubblica o la sicurezza dello Stato (reclusione da due a otto anni). Il comma 3 prevede che, se il fatto è commesso per colpa grave, la pena è ridotta da un terzo a un sesto.

- La seconda fattispecie (comma 2), residuale rispetto alla prima, punisce chiunque "*altera sistemi di intelligenza artificiale ad alto rischio*", salvo che il fatto non costituisca più grave reato, con pene aumentate rispetto al comma 1: reclusione da due a sei anni se dal fatto deriva pericolo concreto per la vita o l'incolumità individuale, da tre a dieci anni se il pericolo riguarda l'incolumità pubblica o la sicurezza dello Stato.

Entrambe le fattispecie si applicano esclusivamente ai sistemi di intelligenza artificiale ad alto rischio ai sensi dell'AI Act e sono strutturate come reati di pericolo concreto: la condotta assume rilevanza penale solo ove produca un effettivo rischio per i beni tutelati dalla norma. Il trattamento sanzionatorio segue una logica di proporzionalità rispetto alla gravità del pericolo: la pena è più contenuta quando il rischio investe la vita o l'incolumità del singolo e si inasprisce significativamente quando il pericolo si estende all'incolumità pubblica o alla sicurezza dello Stato, beni di rango collettivo la cui compromissione giustifica un più severo rigore punitivo.

Nonostante il ricorso all'espressione "chiunque", la fattispecie si configura, nella sua dimensione omissiva, come **reato proprio**: l'obbligo di predisporre adeguate misure tecniche di prevenzione e sorveglianza umana grava, infatti, esclusivamente sui soggetti che intervengono nella filiera dei sistemi di intelligenza artificiale ad alto rischio. La disposizione riflette la c.d. **catena del valore dell'i.a.** delineata dall'AI Act, richiamando le attività di progettazione, addestramento, produzione, immissione sul mercato e utilizzo professionale di tali sistemi. Il Regolamento europeo individua, com'è noto, una pluralità di categorie di operatori - fornitori, rappresentanti autorizzati dei fornitori, importatori, distributori e deployer - ciascuna gravata da obblighi specifici e distinti, la cui violazione può rilevare ai fini dell'integrazione della fattispecie.

Quanto agli elementi oggettivi della condotta, la nozione di **"malfunzionamento"** rilevante ai fini della prima fattispecie non va intesa in senso ampio, come sinonimo di qualsiasi errore o risultato insoddisfacente prodotto dal sistema, ma richiede una lettura ancorata al piano tecnico-funzionale. Poiché il legislatore non ne ha fornito una definizione, l'interprete dovrà verosimilmente fare riferimento al quadro definitorio dell'AI Act, alla disciplina della cybersicurezza e agli orientamenti già maturati in tema di sicurezza dei sistemi informatici.

Un nodo interpretativo di particolare rilievo pratico riguarda poi la riconducibilità alla nozione di "malfunzionamento" delle c.d. allucinazioni e dei fenomeni di bias che caratterizzano i modelli generativi: trattandosi di manifestazioni in larga misura intrinseche a tali sistemi, e non necessariamente imputabili a una specifica omissione del soggetto agente, la loro inclusione nell'ambito applicativo della norma appare tutt'altro che scontata e sarà presumibilmente oggetto di dibattito in sede applicativa.

Diversa è la nozione di **"alterazione del funzionamento"**, che evoca uno scenario distinto: quello in cui un soggetto interviene dall'esterno, o introduce modifiche non autorizzate, mutando il comportamento del sistema rispetto a come era stato originariamente progettato e configurato.

3. Le modifiche al d.lgs. 231/2001

L'art. 17 inserisce nell'elenco dei reati presupposto del d.lgs. 231/2001 il nuovo **art. 25-*vicies*** (rubricato "***Reati commessi con l'uso di sistemi di intelligenza artificiale***"), che ricomprende:

- il nuovo **art. 437-*bis* c.p.** (omessa adozione di misure di sicurezza nei sistemi di i.a. e alterazione illecita dei sistemi), di cui al paragrafo precedente;
- il reato di illecita diffusione di contenuti generati o manipolati artificialmente, cc.dd. "deep-fake" (**art. 612-*quater* c.p.**), introdotto dalla legge 132/2025.

L'inclusione di tali fattispecie nell'elenco dei reati presupposto della responsabilità degli enti comporta la necessità, per le società di valutare la propria esposizione al rischio connesso all'intelligenza artificiale e aggiornare, di conseguenza, i propri Modelli 231, prevedendo protocolli specifici.

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