Novembre, 2026

NEWSLETTER // **Corporate Compliance**

Società tra Avvocati

Health & Safety
Environment
Food
Compliance
Criminal Law



Intelligenza artificiale e responsabilità degli enti

Le novità introdotte dai d.lgs. 160/2026 e 179/2026: nuovi reati presupposto, sicurezza dei sistemi di AI e impatti sulla compliance 231

Contenuti

1. Introduzione
2. Il nuovo art. 437-bis c.p.
3. Il nuovo art. 25-vicies e la responsabilità degli enti
4. Impatti sulla compliance 231

1. Introduzione

Il sistema della responsabilità amministrativa degli enti è chiamato a confrontarsi con i nuovi rischi derivanti dallo sviluppo e dall'impiego dei sistemi di intelligenza artificiale.

In attuazione delle deleghe contenute nella legge del 23 settembre 2025, n. 132, sono stati emanati il d.lgs. 160/2026 (G.U. n. 214 del 15 settembre 2026) ("**Decreto**"), in materia di utilizzo dell'AI per l'attività di polizia e di responsabilità civile e penale, e il d.lgs. 179/2026 (G.U. n. 234 dell'8 ottobre 2026), relativo ai poteri delle autorità nazionali e all'impiego dell'AI nella formazione. Entrambi i provvedimenti sono entrati in vigore e si inseriscono nel quadro del regolamento (UE) 2024/1689 ("**AI Act**").

I due decreti intervengono su ambiti distinti:

- il Decreto, rilevante ai fini della responsabilità amministrativa degli enti, introduce disposizioni in materia di responsabilità penale e civile. In particolare, l'art. 12 inserisce nel codice penale il nuovo art. 437-bis, relativo all'omessa adozione di misure di sicurezza nei sistemi di AI e alla loro alterazione illecita, mentre l'art. 15 amplia il catalogo dei reati presupposto del d.lgs. 231/2001, introducendo il nuovo art. 25-vicies, dedicato ai reati commessi con l'uso di sistemi di AI;

- il d.lgs. 179/2026 completa, su un diverso piano, il quadro nazionale di attuazione dell'AI Act, disciplinando, tra l'altro, i poteri delle autorità competenti. Di particolare rilievo è l'art. 42 che introduce specifiche disposizioni in materia di salute e sicurezza nei luoghi di lavoro, prevedendo che l'utilizzo di sistemi di AI che incidono sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità di esecuzione della prestazione o sui processi decisionali rilevanti ai fini della sicurezza sia valutato nell'ambito della valutazione dei rischi di cui all'art. 28 del d.lgs. 81/2008. La disposizione prevede, inoltre, che i datori di lavoro assicurino un'adeguata informazione e formazione dei lavoratori sui rischi specifici connessi all'utilizzo di tali sistemi e sulle misure di prevenzione e protezione adottate.

2. Il nuovo art. 437-bis c.p.

L'art. 437-bis c.p., rubricato «Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi», prevede una tutela penale rispetto ai pericoli connessi ai sistemi di AI ad alto rischio. La collocazione dopo l'art. 437 c.p. richiama, sul piano sistematico, la tutela preventiva della sicurezza.

Il primo comma punisce con la reclusione da uno a cinque anni chi omette di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi di AI ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del loro funzionamento. La medesima sanzione si applica anche all'omessa predisposizione di adeguati meccanismi di sorveglianza umana, qualora tali condotte omissive determinino una situazione di pericolo per la vita o l'incolumità, individuale o pubblica. Il trattamento sanzionatorio risulta più severo nell'ipotesi in cui il pericolo riguardi la sicurezza dello Stato, essendo prevista, in tal caso, la reclusione da due a otto anni.
Il secondo comma sanziona, salvo che il fatto costituisca più grave reato e al di fuori dei casi del primo comma, l'alterazione di sistemi di AI ad alto rischio: la reclusione è da due a sei anni quando ne derivi pericolo per la vita o l'incolumità pubblica o individuale e da tre a dieci anni quando il pericolo riguardi la sicurezza dello Stato.
Per i fatti del primo comma commessi per colpa grave, il terzo comma prevede una riduzione della pena da un terzo a un sesto.

Il testo definitivo introduce, inoltre, un quarto comma, dedicato alla responsabilità dell'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio. La disposizione estende le sanzioni previste dal primo comma a chi ometta intenzionalmente di adottare le misure di sorveglianza umana, qualora da tale omissione derivi un pericolo per la vita o l'incolumità pubblica o individuale, ovvero per la sicurezza dello Stato, con applicazione delle rispettive pene previste in relazione alla natura del pericolo.

3. Il nuovo art. 25-vicies e la responsabilità degli enti

L'art. 15 del Decreto inserisce nel d.lgs. 231/2001 il nuovo art. 25-vicies, rubricato «Reati commessi con l'uso di sistemi di intelligenza artificiale», ampliando il catalogo dei reati presupposto.

Per il delitto di cui all'art. 437-bis c.p. è prevista a carico dell'ente la sanzione pecuniaria da seicento a mille quote, ferma restando la necessità di accertare i presupposti generali della responsabilità dell'ente ai sensi del d.lgs. 231/2001.

La disposizione include, inoltre, il delitto di cui all'art. 612-quater c.p., relativo all'illecita diffusione di contenuti generati o manipolati artificialmente, per il quale la sanzione pecuniaria a carico dell'ente è da duecento a settecento quote.

La disciplina individua, dunque, due distinti ambiti di rilevanza penale: da un lato, la sicurezza dei sistemi di intelligenza artificiale ad alto rischio; dall'altro, l'impiego dell'AI nella produzione o alterazione di contenuti potenzialmente lesivi dei diritti della persona. L'inserimento delle relative fattispecie nel catalogo dei reati presupposto del d.lgs. 231/2001 amplia l'ambito della responsabilità degli enti, rendendo possibile l'applicazione delle sanzioni previste dal decreto anche in relazione a determinate condotte illecite connesse all'intelligenza artificiale. Tale responsabilità non discende, tuttavia, dal semplice utilizzo illecito della tecnologia, ma richiede la sussistenza dei presupposti generali di imputazione previsti dal decreto, tra cui la commissione di un reato presupposto nell'interesse o a vantaggio dell'ente da parte di soggetti a esso funzionalmente collegati.

Per entrambe le fattispecie l'art. 25-vicies richiama le sanzioni interdittive dell'art. 9, comma 2, lett. b), c), d) ed e), del d.lgs. 231/2001: sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Non è richiamata la lett. a), relativa all'interdizione dall'esercizio dell'attività.

4. Impatti sulla compliance 231

L'ampliamento del catalogo dei reati presupposto rende opportuno, per gli enti esposti alle relative fattispecie, aggiornare la valutazione dei rischi e verificare l'adeguatezza dei modelli di organizzazione, gestione e controllo. Particolare attenzione meritano le attività di progettazione, addestramento, produzione, immissione sul mercato e impiego professionale di sistemi di AI ad alto rischio, nonché i processi di produzione e diffusione di contenuti mediante AI.

Sul piano operativo assumono rilievo la mappatura delle attività sensibili, l'attribuzione delle responsabilità interne, i controlli sulle misure tecniche di sicurezza e sulla sorveglianza umana, la formazione del personale e i flussi informativi verso l'Organismo di Vigilanza. Tali presidi dovranno essere calibrati sull'effettiva attività dell'ente e sui rischi concretamente identificati.

In tale prospettiva, assume rilievo anche l'art. 42 del d.lgs. 179/2026, le cui previsioni richiedono un coordinamento tra la gestione dei rischi connessi all'impiego dell'AI e il sistema aziendale di prevenzione e protezione. Il coordinamento risulta particolarmente significativo anche ai fini dell'adeguatezza dei presidi organizzativi rilevanti nell'ambito dell'art. 25-septies del d.lgs. 231/2001, relativo ai reati in materia di salute e sicurezza sul lavoro.

L'adeguamento della compliance 231 richiede, pertanto, una revisione dei presidi organizzativi e di controllo alla luce dei nuovi rischi connessi all'impiego dell'intelligenza artificiale, in coordinamento con gli obblighi previsti dall'AI Act e dalla disciplina nazionale. Tale processo dovrà essere condotto secondo un approccio proporzionato e basato sul rischio, distinguendo gli obblighi regolatori dai presupposti di imputazione della responsabilità amministrativa dell'ente.

Contatti

B-HSE Società tra Avvocati a r.l.

Indirizzo: Corso d'Italia, 29, 00198, Roma
Sito: www.b-hse.it
E-mail: info@b-hse.law

Pec: b-hselaw@pec.it
Cod.fisc. 15944151008
P.iva 15944151008
Crea 1625132

Società tra Avvocati

Health & Safety
Environment
Food
Compliance
Criminal Law