

INSIGHT | 29 settembre 2026

Intelligenza artificiale: in vigore dal 30 settembre il D.LGS. 160/2026. Nuove responsabilità penali e 231 nell'impiego dei sistemi di AI

Il 30 settembre 2026 entrerà in vigore il D.Lgs. 9 settembre 2026, n. 160, adottato in attuazione della Legge n. 132/2025 recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale” e pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026.

Il decreto adegua la normativa nazionale al Regolamento (UE) 2024/1689 (AI Act) con specifico riferimento all'impiego dei sistemi di intelligenza artificiale nelle attività di polizia e introduce rilevanti novità in materia di **responsabilità penale e civile**, intervenendo anche sul sistema della **responsabilità amministrativa degli enti ai sensi del D.Lgs. n. 231/2001**.

Il testo definitivo porta a compimento il percorso avviato il 10 giugno 2026 con l'approvazione preliminare degli schemi di decreto legislativo; **resta distinto il percorso relativo ai poteri delle Autorità nazionali e alla formazione in materia di AI**.

Per le imprese, il Decreto rende necessario **valutare non soltanto la conformità tecnica dei sistemi di AI, ma anche l'adeguatezza dei presidi organizzativi**, delle misure di sicurezza, dei meccanismi di sorveglianza umana, della documentazione e del **Modello 231** rispetto ai nuovi profili di rischio.

Il nuovo quadro di responsabilità

Il Decreto interviene lungo **tre direttrici principali**:

- la disciplina dell'impiego dell'AI nelle attività di polizia;
- l'introduzione di nuove disposizioni penali e processuali, con riflessi diretti sulla responsabilità degli enti ai sensi del D.Lgs. 231/2001;
- la previsione di strumenti processuali civili specifici per le azioni di risarcimento dei danni causati dall'utilizzo di sistemi di intelligenza artificiale.

Le modifiche al Codice Penale: il nuovo art. 437-bis c.p.

L'art. 12 del Decreto introduce nel codice penale l'art. 437-bis, rubricato “Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi”.

La disposizione distingue quattro ipotesi:

- **Omissione dolosa di misure di sicurezza o di sorveglianza: il primo comma** punisce chi omette di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione o l'immissione sul mercato di sistemi di AI ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento, ovvero omette di adottare misure di sorveglianza umana. La pena è la reclusione da uno a cinque anni quando dall'omissione deriva pericolo per la vita o l'incolumità pubblica o individuale e da due a otto anni quando deriva un pericolo per la sicurezza dello Stato; riguarda il bene nel suo complesso;
- **Alterazione illecita dei sistemi di AI: il secondo comma** punisce, salvo che il fatto costituisca più grave reato, chi **altera sistemi di AI ad alto rischio**. La reclusione è da due a sei anni se ne deriva pericolo per la vita o l'incolumità pubblica

o individuale e da tre a dieci anni se ne deriva un pericolo per la sicurezza dello Stato; è stata comunicata dal produttore al retailer.

- **Omissione colposa di misure di sicurezza o di sorveglianza:** il terzo comma prevede la punibilità per colpa grave dei fatti di cui al primo comma, con la riduzione della pena prevista dalla disposizione;
- **Omissione intenzionale di misure di sorveglianza da parte dell'utilizzatore professionale:** il quarto comma punisce l'utilizzatore professionale di sistemi di AI ad alto rischio che omette intenzionalmente le misure di sorveglianza umana, quando ne deriva, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure per la sicurezza dello Stato.

Rispetto allo schema, il testo definitivo distingue più nettamente i soggetti coinvolti nelle diverse fasi del ciclo di vita dei sistemi di AI ad alto rischio dall'utilizzatore professionale, per il quale la rilevanza penale dell'omessa sorveglianza umana è ricondotta a una condotta intenzionale.

Le modifiche al D.Lgs. 231/2001: il nuovo art. 25-vicies

L'art. 15 del Decreto introduce nel D.Lgs. 231/2001 il nuovo art. 25-vicies, "*Reati commessi con l'uso di sistemi di intelligenza artificiale*", confermando sul punto l'impianto dello schema:

- per il delitto di cui all'art. 437-bis c.p. è prevista a carico dell'ente la sanzione pecuniaria da 600 a 1.000 quote;
- per il delitto di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale c.d. "*Deepfake*" di cui all'art. 612-quater c.p., già introdotto dalla L. 132/2025, è prevista la sanzione pecuniaria da 200 a 700 quote;

in entrambi i casi si applicano le sanzioni interdittive di cui all'art. 9, comma 2, e, in particolare, i) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito (lett. b); ii) il divieto di contrattare con la Pubblica Amministrazione (lett. c); iii) l'esclusione da agevolazioni e finanziamenti con l'eventuale revoca di quelli già concessi (lett. d); iv) il divieto di pubblicizzare beni o servizi (lett. e).

Per le imprese, l'introduzione del nuovo reato-pre-supposto **rende opportuna una verifica della map-**

patura dei rischi 231 connessi ai sistemi di AI, con particolare attenzione ai sistemi ad alto rischio, alle responsabilità lungo il ciclo di vita del sistema, alle misure tecniche di sicurezza, ai presidi di supervisione umana e alla tracciabilità delle decisioni e dei controlli.

Intelligenza artificiale nelle attività di polizia

Il Titolo I del D. Lgs. n. 160/2026 disciplina l'utilizzo dei sistemi di AI da parte delle Forze di polizia secondo **un approccio antropocentrico, proporzionato e basato sul rischio**. Ai sensi dell'art. 3, i sistemi e i relativi output hanno funzione di **supporto all'attività umana**: quando i risultati delle elaborazioni automatiche sono utilizzati in atti o provvedimenti incidenti sulla sfera giuridica degli interessati, è richiesta una **revisione umana qualificata e documentata**. Per i sistemi ad alto rischio deve inoltre essere assicurata una sorveglianza umana effettiva da parte di personale adeguatamente formato.

Identificazione biometrica e riconoscimento facciale

Il Decreto dedica particolare attenzione all'**identificazione biometrica remota in tempo reale**, distinguendo tra finalità di prevenzione e finalità investigative:

- per le **finalità di prevenzione**, l'art. 8 consente l'identificazione biometrica remota in tempo reale, nei casi individuati dalla norma, per la ricerca mirata di persone specificamente individuate o individuabili. L'utilizzo è subordinato all'**autorizzazione del Procuratore della Repubblica competente**, con indicazione della finalità, dell'area territoriale, delle persone interessate, delle banche dati utilizzate e della durata, comunque non superiore a quindici giorni, salvo proroga motivata. Sono previste specifiche procedure per i casi d'urgenza;
- per le **finalità investigative**, il nuovo **art. 359-ter c.p.p.**, introdotto dall'art. 13 del Decreto, consente l'identificazione o la localizzazione biometrica in tempo reale nei casi espressamente previsti, tra cui la ricerca di persone indiziate di determinati delitti, di latitanti e di specifiche vittime. L'impiego è autorizzato dal Giudice per le indagini preliminari su richiesta del pubblico ministero. Nei casi urgenti è prevista un'attivazione anticipata soggetta a successiva convalida.

A tali presidi si aggiungono specifiche garanzie sul **trattamento dei dati**. È, infatti, vietato l'utilizzo di

banche dati biometriche alimentate mediante *scraping* non mirato.

L'art. 10 disciplina separatamente il **riconoscimento facciale a posteriori** mediante sistemi di videosorveglianza integrati con componenti di AI. La tecnologia può essere attivata soltanto dopo l'acquisizione delle immagini e, quando è utilizzata per la ricerca mirata di una persona indiziata, è previsto un meccanismo di **autorizzazione del GIP su richiesta del Pubblico Ministero**. Fa eccezione l'utilizzo, successivo alla commissione del reato, finalizzato esclusivamente alla prima identificazione di una persona potenzialmente indiziata sulla base di elementi oggettivi e verificabili connessi al fatto.

Per tali sistemi sono inoltre previsti una **valutazione d'impatto preventiva**, la conservazione dei dati per **sette giorni** e dei log per cinque anni. Nessuna decisione produttiva di effetti giuridici negativi può essere fondata esclusivamente sui risultati del riconoscimento facciale ed è vietato qualsiasi impiego non mirato o finalizzato al controllo o all'identificazione biometrica generalizzata e indiscriminata delle persone.

Cosa fare

Il D.Lgs. n. 160/2026 rafforza l'esigenza di integrare la **governance dell'AI con i sistemi di controllo interno e con il Modello 231**. In particolare, appare opportuno:

- censire i sistemi di AI utilizzati dall'organizzazione e verificarne la classificazione, con specifica attenzione ai sistemi ad alto rischio;
- individuare ruoli, responsabilità e poteri di controllo lungo il ciclo di vita dei sistemi, distinguendo la posizione dell'utilizzatore professionale da quella degli altri operatori;
- verificare e documentare le misure tecniche di sicurezza, i meccanismi di supervisione umana, le procedure di escalation e la tracciabilità degli interventi;
- coordinare la governance AI con la mappatura dei rischi e i protocolli del Modello 231, nonché con i flussi informativi verso l'Organismo di Vigilanza.

Nel complesso, il testo pubblicato conferma che la compliance AI non può essere trattata come un adempimento esclusivamente tecnico. Il Decreto collega, infatti, in modo diretto la sicurezza e la supervisione dei sistemi di AI alla responsabilità penale e 231. È quindi su questo **intreccio tra governance, responsabilità e prova** che deve oggi concentrarsi l'attenzione delle imprese.

Contatti



Giovanni Morgese
giovanni.morgese@lcalex.it



Paolo Erik Liedholm
paolo.liedholm@lcalex.it



Chiara Mammola
chiara.mammola@lcalex.it

LCA è uno studio legale indipendente e full service, specializzato nell'assistenza legale e fiscale d'impresa, composto da circa 350 persone.

MILANO

Via della Moscova 18
20121 Milano

ROMA

Piazza del Popolo 18
00187 Roma

GENOVA

Via XX Settembre 31/6
16121 Genova

TREVISO

Via Sile 41
31056 Roncade (TV)

BRUXELLES

Place Poelaert 6
1000 Bruxelles

DUBAI

IAA Middle East Legal Consultants LLP
Liberty House, Office 514, DIFC

www.lcalex.it
info@lcalex.it