

ADVOCATUS · DIABOLI



DIRITTO · IMPRESA · POTERE

# THEDEVILLAWYER

## IL PUNTO DI VISTA SULLA AI

*«Quello che gli altri non vi dicono»*

NUMERO V · IL PRIMO REATO DELL'IA

*Lunedì 3 agosto 2026*

*«Nove giorni di vita, un articolo nuovo nel codice penale.  
E tre domande a cui nessuno sa ancora rispondere.»*

*D.Lgs. 160/2026: l'art. 437-bis c.p., le società nel 231,  
le regole nuove per chi chiede i danni.*

**AVV. ANTONIO SALERNO**

• ADVOCATUS DIABOLI •

*thedevillawyer.it · Anno Domini MMXXVI*

## In questo numero

*Dal 30 settembre 2026 il codice penale ha un reato in più: l'art. 437-bis, che punisce l'omessa adozione di misure di sicurezza e di sorveglianza umana nei sistemi di IA ad alto rischio. In questo numero: il testo letterale, le pene, le tre questioni interpretative ancora aperte, la responsabilità delle società (art. 25-vicies del D.Lgs. 231/2001), gli strumenti nuovi per chi agisce per i danni (esibizione delle prove, presunzione del nesso, azione diretta contro l'assicuratore) e il capitolo biometrico per la polizia.*

### L'APERTURA

**Il decreto che il codice penale aspettava (e che l'AI Act non sapeva di dover aspettare)** 1

### IL REATO

**Articolo 437-bis del codice penale: il testo, parola per parola** 2

### LE PENE

**Quanto si rischia: la tabella** 3

### LE DOMANDE APERTE

**Tre questioni che la norma non risolve (e noi neppure, per ora)** 4

### LE SOCIETÀ

**Articolo 25-vicies: il 231 impara l'intelligenza artificiale** 5

### I DANNI

**Chi agisce per i danni da IA: gli artt. 16-20, riga per riga** 6

### LA POLIZIA

**Biometria: quello che il giudice deve poter dire «no»** 7

### IL NOSTRO PUNTO DI VISTA

**Cosa fare lunedì mattina** 8

### TRASPARENZA

**Nota metodologica e fonti** 9



## L'APERTURA

# Il decreto che il codice penale aspettava (e che l'AI Act non sapeva di dover aspettare)

Il decreto legislativo 9 settembre 2026, n. 160 è stato pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026 ed è in vigore dal 30 settembre 2026. Il titolo è un programma: adeguamento della normativa nazionale al Regolamento (UE) 2024/1689 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale.

Nasce dalla delega dell'art. 24 della legge 23 settembre 2025, n. 132. Il percorso, ricostruibile dalle premesse: esame preliminare del Consiglio dei ministri il 10 giugno 2026, parere del Garante privacy, parere della Conferenza unificata il 20 luglio, pareri delle Commissioni parlamentari, deliberazione finale del Consiglio dei ministri il 4 agosto 2026. Tre titoli: la polizia (artt. 1-10), le disposizioni penali e processuali (artt. 11-20), le norme transitorie e finanziarie (artt. 21-22).

Una clausola da non perdere: l'art. 1, comma 3, precisa che il Titolo I non comporta nuovi obblighi rispetto a quelli già previsti dal Regolamento europeo. Il legislatore lo dice per le norme di polizia. Per il penale, invece, i nuovi obblighi esistono eccome.

**IL REATO**

## Articolo 437-bis del codice penale: il testo, parola per parola

L'art. 12 del decreto inserisce, dopo l'art. 437 del codice penale (i delitti contro l'incolumità pubblica), la nuova norma. Eccola, nel testo letterale della Gazzetta Ufficiale.

**ART. 437-BIS C.P. — TESTO LETTERALE (commi 1 e 2)**

Omissa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi. Chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana è punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni. Salvo che il fatto costituisca più grave reato, chiunque, al di fuori dei casi indicati al primo comma, altera sistemi di intelligenza artificiale ad alto rischio è punito, qualora dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale, con la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni.

**ART. 437-BIS C.P. — TESTO LETTERALE (commi 3 e 4)**

Se taluno dei fatti previsti dal comma primo è commesso per colpa grave, la pena è ridotta da un terzo a un sesto. 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 primo comma, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato.

## LE PENE

## Quanto si rischia: la tabella

Le pene dell'art. 437-bis, ordinate per condotta. Si legge così: la colonna di sinistra dice che cosa si fa (o non si fa), le altre due dicono quanto si rischia a seconda del pericolo che ne deriva.

| Condotta                                                                               | Pericolo per vita /<br>incolumità   | Pericolo per la sicurezza<br>dello Stato |
|----------------------------------------------------------------------------------------|-------------------------------------|------------------------------------------|
| Omessa adozione di misure di sicurezza o di sorveglianza umana (comma 1)               | reclusione da 1 a 5 anni            | reclusione da 2 a 8 anni                 |
| Alterazione di sistemi ad alto rischio (comma 2)                                       | reclusione da 2 a 6 anni            | reclusione da 3 a 10 anni                |
| Colpa grave (comma 3, richiama «i fatti del comma primo»)                              | pena ridotta da un terzo a un sesto | pena ridotta da un terzo a un sesto      |
| Utilizzatore professionale che omette intenzionalmente la sorveglianza umana (comma 4) | pene del comma 1                    | pene del comma 1                         |

La corrispondenza con la delega c'è: l'art. 24, comma 5, lett. b), della legge 132/2025 chiedeva fattispecie autonome centrate sull'omessa adozione di misure di sicurezza, quando dalle omissioni deriva pericolo concreto per la vita, l'incolumità pubblica o individuale o la sicurezza dello Stato.

**LE DOMANDE APERTE**

## Tre questioni che la norma non risolve (e noi neppure, per ora)

Dichiariamo il limite: la norma ha nove giorni di vita e non esiste una sola pronuncia. Quello che segue sono letture del testo, non tesi consolidate.

**Prima questione: quando scatta il reato, se gli obblighi dell'AI Act slittano?** Gli obblighi di sicurezza e sorveglianza dei sistemi ad alto rischio dell'AI Act si applicano, dopo l'Omnibus, dal 2 dicembre 2027 (Allegato III) e dal 2 agosto 2028 (Allegato I). L'art. 437-bis, invece, è già in vigore dal 30 settembre 2026 e non richiama né quelle date né gli articoli del Regolamento. Come si coordinino è la domanda numero uno del primo processo. Nessuna fonte che abbiamo letto la risolve.

**Seconda questione: il pericolo è elemento del reato o condizione?** Il testo dice «quando da tali omissioni derivi pericolo». Si può leggere come reato di pericolo concreto (il pericolo è un elemento costitutivo, da provare) oppure come condizione obiettiva. La differenza, per la difesa, è enorme. La dottrina commenta il parallelo con le omissioni di cautele degli artt. 437 e 451 c.p.

**Terza questione: la colpa grave copre anche l'alterazione?** Il comma 3 riduce la pena «se taluno dei fatti previsti dal comma primo» è commesso per colpa grave. Letteralmente non richiama il comma 2, l'alterazione dei sistemi. È una lettura nostra del testo: da verificare quando arriverà la prima giurisprudenza.



## LE SOCIETÀ

## Articolo 25-vicies: il 231 impara l'intelligenza artificiale

L'art. 15 del decreto aggiunge al D.Lgs. 231/2001 l'art. 25-vicies, «Reati commessi con l'uso di sistemi di intelligenza artificiale». Due reati-presupposto, due fasce di sanzione pecuniaria.

| Reato-presupposto                                                                              | Sanzione pecuniaria per l'ente |
|------------------------------------------------------------------------------------------------|--------------------------------|
| Art. 437-bis c.p. (sicurezza e sorveglianza umana, alterazione)                                | da 600 a 1.000 quote           |
| Art. 612-quater c.p. (illecita diffusione di contenuti generati o alterati con IA: i deepfake) | da 200 a 700 quote             |

Si applicano anche le sanzioni interdittive dell'art. 9, comma 2, lettere b), c), d) ed e): sospensione o revoca di autorizzazioni, divieto di contrattare con la pubblica amministrazione, esclusione da agevolazioni e finanziamenti, divieto di pubblicizzare beni o servizi. Non la lettera a): l'interdizione dall'esercizio dell'attività resta fuori.

Una precisazione di metodo: l'art. 612-quater non nasce con questo decreto. L'ha introdotto l'art. 26 della legge 132/2025: reclusione da uno a cinque anni, punibile a querela, d'ufficio in alcune ipotesi connesse. Il decreto 160 non lo modifica; lo richiama soltanto per le società.

**I DANNI**

## Chi agisce per i danni da IA: gli artt. 16-20, riga per riga

Il Capo II del Titolo II non crea una nuova responsabilità: crea strumenti processuali. Ed è già molto. Restano ferme l'art. 82 del GDPR e la normativa di recepimento della Direttiva (UE) 2024/2853 sui prodotti difettosi.

| Articolo                                | Che cosa prevede                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Art. 17 — esibizione delle prove        | A istanza di chi allega il danno, il giudice ordina l'esibizione degli elementi di prova specificamente pertinenti al funzionamento del sistema (registri, documentazione sui rischi, documentazione tecnica, parametri della supervisione umana), se l'istante rende verosimile la domanda. Se la parte non esibisce senza giustificato motivo: argomenti di prova; sulla documentazione indicata al comma 2, il giudice ritiene ammessi i fatti allegati. Per il terzo inadempiente: pena pecuniaria da 1.500 a 10.000 euro. |
| Art. 18 — nesso causale                 | Quando il danno deriva dalla violazione di obblighi del Regolamento (UE) 2024/1689, il nesso tra violazione e danno è presunto, salvo prova contraria. Presunzione relativa del solo nesso: non del difetto, non della colpa.                                                                                                                                                                                                                                                                                                  |
| Art. 19 — la conformità non è uno scudo | La conformità del sistema agli obblighi del Regolamento, anche se certificata, non esclude di per sé la responsabilità del convenuto.                                                                                                                                                                                                                                                                                                                                                                                          |
| Art. 20 — azione diretta                | Il danneggiato può chiedere prima se esiste una polizza di responsabilità civile (risposta entro 30 giorni; silenzio o risposta incompleta = argomento di prova), poi agire direttamente contro l'assicuratore nei limiti delle somme assicurate, con litisconsorzio necessario del responsabile.                                                                                                                                                                                                                              |

Il foro: se il danneggiato è una persona fisica che agisce per scopi estranei all'attività professionale, è competente anche il giudice del luogo di residenza o domicilio (art. 16, comma 4).

Un limite, per onestà: la delega parlava di criteri di ripartizione dell'onere della prova; il decreto non dà una regola generale, solo la presunzione del nesso dell'art. 18. E con gli obblighi dell'alto rischio fissati al 2027-28 dall'Omnibus, lo spazio concreto dell'art. 18 oggi è ristretto: molti obblighi ancora non si applicano.

**LA POLIZIA**

## **Biometria: quello che il giudice deve poter dire «no»**

Il Titolo I disciplina l'uso dell'IA da parte delle forze di polizia, con una linea chiara: funzione strumentale e di supporto, revisione umana qualificata dei risultati prima di usarli in atti incidenti sui diritti, formazione obbligatoria del personale.

- **Identificazione biometrica remota in tempo reale** (art. 8): richiesta al procuratore della Repubblica del capoluogo di distretto; durata massima 15 giorni, prorogabili con decreto motivato; urgenza con richiesta di autorizzazione entro 24 ore. Violazioni: interruzione, cancellazione dei dati e inutilizzabilità dei risultati.
- **Riconoscimento facciale a posteriori** (art. 10): autorizzazione del GIP su richiesta del PM entro 48 ore dall'avvio, con esclusione quando l'uso serve solo alla prima identificazione di un possibile indiziato su elementi oggettivi; conservazione dei dati 7 giorni.
- **Nuovo art. 359-ter c.p.p.** (art. 13): identificazione e localizzazione mediante IA per i delitti dell'Allegato II del Regolamento puniti con almeno quattro anni nel massimo, la ricerca di latitanti e di vittime di tratta o sfruttamento sessuale; comma 8: i risultati ottenuti fuori dai casi consentiti non sono utilizzabili.

Per la difesa penale la regola è scritta dalla legge stessa: inutilizzabilità. È un'eccezione preliminare da valutare, caso per caso, nel merito di ogni indagine in cui compaiano risultati biometrici.



## IL NOSTRO PUNTO DI VISTA

# Cosa fare lunedì mattina

- **Per l'impresa che sviluppa o usa IA ad alto rischio:** aggiornare il modello 231. La norma c'è, anche se gli obblighi dell'AI Act slittano. Misure tecniche di sicurezza documentate, sorveglianza umana tracciata (chi, quando, con quali poteri di fermare il sistema), controllo dei contenuti sintetici e del consenso per i deepfake.
- **Per l'assicurazione:** controllare subito che le polizze di responsabilità civile non escludano i rischi da IA. Dopo l'art. 20, l'assicuratore è convenibile direttamente.
- **Per chi agisce per i danni:** preparare in anticipo l'istanza ex art. 17, con l'elenco dei documenti che il Regolamento indica (registri, gestione dei rischi, documentazione tecnica, supervisione umana) e il fascicolo che rende verosimile il collegamento tra output e danno. Attenzione: per danni di oggi, parte di quella documentazione potrebbe non essere ancora obbligatoria.
- **Per la difesa penale:** non dare nulla per scontato sull'art. 437-bis. Elemento del pericolo, coordinamento con le date dell'AI Act, ruolo della colpa grave: sono tre eccezioni in attesa di un giudice.

### IL VERDETTO DEL DIAVOLO

L'Unione europea ha spostato gli obblighi dell'alto rischio a dicembre 2027 (Allegato III) e ad agosto 2028 (Allegato I). Il governo italiano, invece, ha messo il carcere subito. Non è una contraddizione: sono due orologi diversi, e il secondo corre. Chi ha un sistema di IA ad alto rischio e pensa «ho tempo fino al 2027» ha letto il calendario europeo e dimenticato il codice penale. Cosa succeda quando i due orologi si incontreranno in un'aula, lo dirà il primo giudice. Noi intanto ci prepariamo per entrambi.

*Il diritto non è una questione di date. È una questione di chi arriva primo all'udienza.*  
*Antonio Salerno*

**TRASPARENZA**

## Nota metodologica e fonti

Fonte primaria letta per intero: D.Lgs. 9 settembre 2026, n. 160, Gazzetta Ufficiale n. 214 del 15 settembre 2026 (testo integrale). Delega: art. 24 della L. 23 settembre 2025, n. 132 (GU n. 223 del 25.9.2025); art. 612-quater c.p. introdotto dall'art. 26 della stessa legge. Date dell'Omnibus: Reg. (UE) 2026/1744 su EUR-Lex. Limiti dichiarati: non abbiamo letto la Relazione illustrativa, quindi non sosteniamo nulla sull'intento del legislatore; non esiste ancora giurisprudenza sul decreto; lo stato di adozione dei decreti attuativi richiamati (DPCM art. 5, comma 4; decreto del Ministro dell'interno art. 9, comma 5) non è stato verificato su fonte primaria. Le tre «questioni aperte» sono letture del testo, non tesi consolidate.

Documento gratuito a scopo divulgativo. Non costituisce parere o consulenza legale, né promessa di risultato: ogni caso va valutato sui suoi fatti.