

ottobre 2026

D.Lgs. 160/2026: responsabilità civile, penale e tutela risarcitoria per i danni da IA

Il 15 settembre 2026 è stato pubblicato in Gazzetta Ufficiale il D.Lgs. 9 settembre 2026, n. 160 (il "**Decreto**"), entrato in vigore il 30 settembre 2026. Il provvedimento adegua la normativa nazionale al Regolamento (UE) 2024/1689 ("**AI Act**") con riguardo, da un lato, all'impiego dei sistemi di intelligenza artificiale nell'attività di polizia e, dall'altro, alla responsabilità civile e penale connessa alla realizzazione e all'uso illecito di tali sistemi.

Il Decreto introduce, in particolare, nuovi strumenti processuali destinati alle azioni di risarcimento dei danni cagionati dall'utilizzo di sistemi di IA. Le disposizioni interessano imprese, professionisti, pubbliche amministrazioni e, più in generale, qualsiasi soggetto che utilizzi sistemi di IA nell'ambito di attività contrattuali o extracontrattuali.

Nuovo art. 25-*vicies* D.Lgs. 231/2001: responsabilità degli enti per i reati commessi con sistemi di IA

Il nuovo art. 25-*vicies* del D.Lgs. 231/2001 estende la responsabilità degli enti ai reati di cui agli artt. 437-*bis* c.p. "*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*" e 612-*quater* c.p. "*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*". I reati riguardano carenze di sicurezza o sorveglianza dei sistemi IA ad alto rischio e la diffusione illecita di c.d. *deepfake*.

Le imprese devono quindi valutare, in base all'esposizione concreta, l'aggiornamento del *risk assessment* nell'ambito dei Modelli Organizzativi 231 in coordinamento con l'analisi dei presidi dell'AI Act, adeguando controlli e flussi informativi verso l'Organismo di Vigilanza.

Un regime processuale dedicato ai danni da IA

Le nuove regole operano su due livelli: le disposizioni generali si applicano a tutte le azioni risarcitorie relative a danni cagionati nell'utilizzo di sistemi di IA; le tutele rafforzate, tra cui la presunzione del nesso causale, presuppongono invece la violazione di uno o più obblighi dell'AI Act.

Foro del danneggiato: quando agisce una persona fisica per finalità estranee all'attività professionale, è competente anche il giudice del luogo di residenza o domicilio del danneggiato.

Rapporto con altre discipline: restano ferme le tutele previste dal GDPR e dalla normativa sulla responsabilità per prodotti difettosi.

Accesso alle prove e ordine di esibizione

Per attenuare l'asimmetria informativa tra il danneggiato e il soggetto che controlla il sistema, il giudice può ordinare alla controparte o a un terzo l'esibizione degli elementi di prova pertinenti al funzionamento del sistema di IA, quando la pretesa sia resa verosimile da fatti e circostanze specificamente allegati.

L'ordine può riguardare, tra l'altro, i registri di *log*, la documentazione sul sistema di gestione dei rischi, le informazioni pertinenti della documentazione tecnica e i parametri della supervisione umana. L'esibizione deve essere necessaria e proporzionata e può essere accompagnata da misure a tutela dei segreti commerciali e della riservatezza.

L'inosservanza ingiustificata dell'ordine consente al giudice di desumere argomenti di prova. Per i documenti tecnici espressamente individuati dal Decreto, i fatti allegati dall'istante possono essere ritenuti ammessi. Il terzo inadempiente può inoltre essere assoggettato a una sanzione pecuniaria da euro 1.500 a euro 10.000.

Presunzione del nesso causale

Quando il danno deriva dalla violazione di obblighi previsti dall'AI Act, il nesso causale tra violazione e danno è presunto, salvo prova contraria. Il danneggiato è quindi tenuto a provare il danno e la violazione, mentre il convenuto deve dimostrare che la violazione non ha causato il pregiudizio o che questo si sarebbe comunque verificato.

La presunzione è relativa e non si applica indistintamente a qualsiasi danno connesso all'IA. È necessario che la violazione dell'AI Act sia allegata con sufficiente specificità e sia causalmente pertinente rispetto al danno lamentato.

Conformità certificata e responsabilità

La conformità del sistema agli obblighi dell'AI Act, anche se attestata nell'ambito della procedura di valutazione prevista dal regolamento, non esclude automaticamente la responsabilità civile. La conformità può rilevare nella valutazione complessiva della condotta, ma non impedisce al giudice di verificare in concreto l'esistenza del danno e il relativo collegamento con l'utilizzo del sistema.

Azione diretta nei confronti dell'assicuratore

Il Decreto introduce un'azione diretta del danneggiato nei confronti dell'impresa che assicura la responsabilità civile del potenziale responsabile, nei limiti del massimale di polizza. La copertura non è obbligatoria, ma il danneggiato può chiedere al potenziale responsabile se esista una polizza applicabile al danno contestato.

Il destinatario della richiesta deve rispondere entro 30 giorni, comunicando esistenza, estremi della polizza e denominazione dell'assicuratore; l'omessa o incompleta risposta può essere valutata dal giudice ai fini probatori.

L'assicuratore può opporre al danneggiato soltanto le eccezioni contrattuali anteriori al sinistro e conserva il diritto di rivalsa verso l'assicurato nei limiti previsti dal contratto.

Il soggetto indicato come responsabile è litisconsorte necessario; il termine di prescrizione coincide con quello dell'azione esercitabile nei suoi confronti.

Implicazioni operative

Il nuovo quadro accresce il rilievo della tracciabilità tecnica e organizzativa dei sistemi di IA. In vista di possibili contestazioni, imprese e professionisti dovrebbero verificare la coerenza tra obblighi regolatori, processi interni, gestione documentale e coperture assicurative.

- Mappare i sistemi di IA utilizzati, individuandone finalità, soggetti coinvolti e classificazione ai sensi dell'AI Act.
- Conservare log, documentazione tecnica, valutazione dei rischi e registrazioni delle attività di supervisione umana in modo completo e reperibile.
- Definire procedure interne per la gestione delle richieste di esibizione, assicurando un equilibrio tra collaborazione processuale, protezione dei dati e tutela dei segreti commerciali.
- Verificare le polizze di responsabilità civile esistenti, con particolare attenzione all'ambito di copertura, alle esclusioni, ai massimali e agli obblighi informativi connessi a danni derivanti dall'uso di IA.
- Alla luce della mappatura, condurre la valutazione del rischio reato e coordinare i presidi di compliance all'AI Act con il Modello Organizzativo ex D.Lgs. 231/2001 e i flussi informativi

all'Organismo di Vigilanza.

Alla luce delle nuove regole probatorie e dell'azione diretta, la corretta conservazione della documentazione e la tempestiva verifica delle coperture assicurative assumono rilievo anche nella prevenzione e gestione del contenzioso.

* * *

Lo Studio resta a disposizione per assistere imprese e professionisti nella valutazione dell'impatto del Decreto, nella revisione dei presidi documentali e organizzativi e nell'analisi delle coperture assicurative applicabili.

* * *

RIEPILOGO SCADENZE

Adempimento	Termine
Adeguamento dei sistemi di IA già in uso o in sviluppo per finalità di polizia alle disposizioni del Titolo I	1 anno dall'entrata in vigore (entro settembre 2027)
Emanazione del decreto ministeriale sui requisiti tecnici dei sistemi di identificazione biometrica remota in tempo reale	Da definire (decreto Ministro Interno/Giustizia)
Adozione del D.P.C.M. di coordinamento degli spazi di sperimentazione	Da definire

Contatti

Torino Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121

Milano Via Bigli 2, 20121 | T. +39 02 303049

info@pavesioassociati.it – www.pavesioassociati.it

Per maggiori informazioni:

AreaLegaltech@pavesioassociati.it

AreaCompliance@pavesioassociati.it

AreaLitigation@pavesioassociati.it

Disclaimer

Il presente documento è redatto in termini generali, unicamente a fini divulgativi e di aggiornamento normativo.