

Intelligenza artificiale, decreto in Gazzetta: cosa cambia dal 30 settembre

(Fonte: <https://giuricivile.it/> 17 settembre 2026)

Nuove regole sull'intelligenza artificiale in arrivo dal **30 settembre 2026**. È stato pubblicato nella [Gazzetta Ufficiale n. 214 del 15 settembre 2026](#) il decreto legislativo 9 settembre 2026, n. 160, che adegua la normativa italiana all'AI Act europeo in alcuni settori particolarmente delicati: utilizzo dell'AI da parte delle Forze di polizia, riconoscimento facciale, responsabilità penale e risarcimento dei danni causati dai sistemi di intelligenza artificiale.

Il decreto dà attuazione alla delega contenuta nella legge n. 132/2025 e non rappresenta quindi una nuova disciplina generale dell'intelligenza artificiale: interviene su ambiti specifici nei quali l'utilizzo dei sistemi AI può incidere direttamente sui diritti delle persone.

Tra le novità più rilevanti ci sono un **nuovo reato per le omissioni nelle misure di sicurezza dei sistemi AI ad alto rischio**, regole per l'identificazione biometrica in tempo reale, nuovi strumenti per chi chiede il risarcimento di un danno e la possibilità, in determinati casi, di agire direttamente contro l'assicurazione del responsabile.

Indice degli argomenti

- [Decreto AI 2026: cosa cambia dal 30 settembre](#)
- [Polizia e AI: obbligatoria la revisione umana](#)
- [Riconoscimento facciale in tempo reale: quando sarà possibile](#)
- [Nuovo reato per i sistemi AI ad alto rischio: pene fino a 10 anni](#)
- [Responsabilità 231 anche per i reati legati all'AI](#)
- [Danni causati dall'AI: diventa più facile ottenere le prove](#)
- [Danni da AI: scatta la presunzione sul nesso causale](#)
- [Si potrà chiedere il risarcimento direttamente all'assicurazione](#)
- [Cosa succede ai sistemi AI già utilizzati dalla polizia](#)
- [Nuove regole sull'intelligenza artificiale 2026: le domande più frequenti](#)

Decreto AI 2026: cosa cambia dal 30 settembre

Il d.lgs. n. 160/2026 interviene principalmente su quattro fronti:

- utilizzo dell'intelligenza artificiale nelle attività di polizia e riconoscimento biometrico;
- introduzione di nuove responsabilità penali legate ai sistemi AI ad alto rischio;
- estensione della responsabilità amministrativa degli enti ai sensi del d.lgs. 231/2001;
- nuove regole processuali per ottenere il risarcimento dei danni provocati dall'utilizzo dell'intelligenza artificiale.

Il decreto è stato pubblicato il **15 settembre** ed entra formalmente in vigore il **30 settembre 2026**. Per alcune disposizioni del Titolo I relative all'attività di polizia, tuttavia, il legislatore rinvia alle specifiche scadenze di applicazione previste dall'AI Act europeo.

Polizia e AI: obbligatoria la revisione umana

Un primo blocco di norme riguarda l'impiego dell'intelligenza artificiale da parte delle Forze di polizia.

Il principio generale è che i sistemi AI devono avere una funzione **strumentale e di supporto** all'attività umana. Prima che il risultato prodotto automaticamente venga utilizzato in atti o provvedimenti capaci di incidere sulla posizione giuridica delle persone deve essere prevista una **revisione umana qualificata**, che deve anche essere documentata e tracciabile.

Per i sistemi classificati ad alto rischio deve inoltre essere garantita un'effettiva sorveglianza umana e il personale incaricato deve possedere competenze e formazione adeguate.

È quindi esclusa, almeno come principio generale, l'idea di una decisione di polizia affidata autonomamente all'algoritmo.

Riconoscimento facciale in tempo reale: quando sarà possibile

Uno dei capitoli destinati a suscitare maggiore attenzione riguarda il **riconoscimento biometrico remoto in tempo reale** nei luoghi pubblici o aperti al pubblico.

Il decreto ne consente l'impiego solo per finalità determinate, tra cui alcune esigenze di prevenzione e la ricerca di persone scomparse o di specifiche vittime di sequestro, tratta o sfruttamento sessuale.

L'utilizzo deve essere mirato verso persone specificamente individuate o individuabili e non può trasformarsi in un controllo biometrico generalizzato della popolazione. La banca dati utilizzata per il confronto deve inoltre essere creata per il singolo utilizzo e i relativi dati devono essere cancellati alla scadenza dell'autorizzazione. È espressamente vietato l'impiego di banche dati biometriche costruite mediante **scraping indiscriminato di immagini da Internet o da telecamere**. Per le attività di prevenzione l'autorizzazione spetta al procuratore della Repubblica e può avere una durata massima di **15 giorni**, prorogabile se ne permangono i presupposti. Nei casi urgenti sono previste procedure accelerate di autorizzazione e controllo.

Nel procedimento penale viene invece introdotto il nuovo **art. 359-ter c.p.p.**, che disciplina l'identificazione e la localizzazione mediante sistemi AI di riconoscimento biometrico remoto in tempo reale, con autorizzazione del giudice per le indagini preliminari su richiesta del pubblico ministero nei casi previsti dalla legge.

Nuovo reato per i sistemi AI ad alto rischio: pene fino a 10 anni

Sul piano penale arriva una delle novità più rilevanti.

Il decreto introduce nel codice penale il nuovo **art. 437-bis**, dedicato all'"omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi".

Chi omette le misure tecniche di sicurezza previste per sistemi IA ad alto rischio, oppure le misure di sorveglianza umana, può essere punito con la **reclusione da uno a cinque anni** quando dall'omissione deriva un pericolo per la vita o l'incolumità pubblica o individuale.

Se il pericolo riguarda la sicurezza dello Stato, la pena sale da **due a otto anni**.

È punita anche l'alterazione di un sistema AI ad alto rischio: la pena arriva fino a **sei anni** quando ne deriva pericolo per la vita o l'incolumità e fino a **dieci anni** se viene messa in pericolo la sicurezza dello Stato.

La norma coinvolge anche l'**utilizzatore professionale** del sistema AI ad alto rischio che ometta intenzionalmente la necessaria sorveglianza umana, quando dall'omissione derivino i pericoli indicati dalla disposizione.

Responsabilità 231 anche per i reati legati all'AI

Il decreto modifica anche il **d.lgs. n. 231/2001**.

Viene inserito il nuovo art. 25-bis, che prevede la responsabilità dell'ente per il nuovo reato dell'art. 437-bis c.p. e per il delitto di **illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale**, previsto dall'art. 612-quater c.p.

Per il reato relativo alla sicurezza dei sistemi IA la sanzione pecuniaria per l'ente va da **600 a 1.000 quote**; per l'illecita diffusione di deepfake da **200 a 700 quote**. Sono previste anche sanzioni interdittive.

Il reato di diffusione illecita di deepfake non nasce con questo decreto: era già stato introdotto dalla legge italiana sull'intelligenza artificiale n. 132/2025, che prevede la reclusione da uno a cinque anni per chi diffonde senza consenso immagini, video o voci falsificati o alterati con AI, quando ne derivi un danno ingiusto.

Danni causati dall'AI: diventa più facile ottenere le prove

Molto rilevanti per avvocati, imprese e assicurazioni sono gli articoli dedicati alla **responsabilità civile**.

Chi afferma di aver subito un danno causato dall'utilizzo di un sistema di intelligenza artificiale può chiedere al giudice di ordinare alla controparte o a un terzo l'esibizione delle prove relative al funzionamento del sistema, quando abbia fornito elementi sufficienti a rendere verosimile la domanda.

Tra i documenti che possono essere richiesti rientrano i registri del sistema, la documentazione sulla gestione dei rischi, la documentazione tecnica e le informazioni sulla supervisione umana. Se una parte non esegue senza giustificato motivo l'ordine del giudice, quest'ultimo può trarne argomenti di prova e, in determinate ipotesi, considerare ammessi i fatti allegati dal danneggiato. Se a non collaborare è un terzo, è prevista una sanzione da **1.500 a 10.000 euro**.

Danni da AI: scatta la presunzione sul nesso causale

Ancora più incisiva è la regola contenuta nell'articolo 18.

Quando il danno deriva dalla violazione di uno o più obblighi previsti dall'AI Act, il **nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria**.

Si tratta di una disposizione destinata ad avere un impatto significativo sul contenzioso, perché interviene su uno dei problemi più difficili nelle cause relative ai sistemi automatizzati: dimostrare in concreto in quale passaggio del funzionamento del sistema si sia prodotto il danno. Il decreto chiarisce inoltre che la semplice conformità del sistema agli obblighi dell'AI Act, anche quando certificata, **non esclude automaticamente la responsabilità** del convenuto.

Si potrà chiedere il risarcimento direttamente all'assicurazione

Altra novità importante è l'**azione diretta contro l'impresa di assicurazione**.

Il danneggiato può chiedere al soggetto ritenuto responsabile se disponga di una polizza di responsabilità civile relativa al danno contestato. Il destinatario deve comunicare entro **30 giorni** l'esistenza della copertura, gli estremi della polizza e l'impresa assicuratrice.

In presenza della copertura, il danneggiato può agire direttamente contro l'assicurazione, nei limiti del massimale previsto dal contratto.

Cosa succede ai sistemi AI già utilizzati dalla polizia

Il decreto contiene infine una disciplina transitoria.

I sistemi di intelligenza artificiale che al momento dell'entrata in vigore sono già utilizzati dalle Forze di polizia, sono oggetto di contratti oppure si trovano in fase di sviluppo o sperimentazione dovranno essere resi compatibili con le nuove disposizioni **entro un anno**.

Il **30 settembre 2026** segna quindi un passaggio importante nell'attuazione italiana dell'AI Act. Per imprese, professionisti e operatori del diritto, il punto da osservare non riguarda soltanto i nuovi poteri delle Forze di polizia: la parte destinata probabilmente a produrre il maggiore contenzioso è quella relativa a **responsabilità, prova e risarcimento dei danni provocati dall'intelligenza artificiale**.

Nuove regole sull'intelligenza artificiale 2026: le domande più frequenti

Quando entrano in vigore le nuove regole sull'intelligenza artificiale?

Il decreto legislativo n. 160/2026 entra formalmente in vigore il **30 settembre 2026**, anche se alcune norme sull'utilizzo dell'AI da parte delle Forze di polizia seguono le scadenze specifiche previste dall'AI Act europeo.

Che cosa cambia dal 30 settembre 2026 per l'intelligenza artificiale?

Cambiano le regole su AI e attività di polizia, riconoscimento facciale, sicurezza dei sistemi ad alto rischio, responsabilità degli enti e risarcimento dei danni causati dall'intelligenza artificiale.

Il riconoscimento facciale sarà vietato in Italia?

No. Il riconoscimento biometrico remoto in tempo reale sarà possibile solo in casi specifici, per finalità determinate e con le autorizzazioni previste dalla legge. Non potrà essere utilizzato per un controllo generalizzato della popolazione.

Chi può autorizzare il riconoscimento facciale in tempo reale?

Per le attività di prevenzione l'autorizzazione spetta al procuratore della Repubblica, mentre nel procedimento penale è previsto l'intervento del giudice per le indagini preliminari su richiesta del pubblico ministero.

Quanto può durare l'autorizzazione per il riconoscimento biometrico?

Per le attività di prevenzione l'autorizzazione può durare al massimo **15 giorni**, con possibilità di proroga quando continuano a sussistere i presupposti previsti dalla legge.

Quali sono le pene per chi non protegge un sistema AI ad alto rischio?

L'omessa adozione delle misure di sicurezza o della sorveglianza umana può comportare la reclusione da **uno a cinque anni**. Se è messa in pericolo la sicurezza dello Stato, la pena può arrivare fino a **otto anni**.

Quanti anni di carcere sono previsti per l'alterazione di un sistema AI?

L'alterazione illecita di un sistema AI ad alto rischio può essere punita fino a **sei anni** di reclusione quando mette in pericolo la vita o l'incolumità. Se riguarda la sicurezza dello Stato, la pena può arrivare fino a **dieci anni**.

Come si può chiedere il risarcimento per un danno causato dall'AI?

Il danneggiato deve dimostrare la plausibilità della propria domanda e può chiedere al giudice di ordinare l'esibizione di documenti sul funzionamento del sistema, sui rischi, sulla documentazione tecnica e sulla supervisione umana.

Chi deve provare il funzionamento del sistema di intelligenza artificiale?

Il giudice può ordinare alla controparte o a un terzo di esibire le prove disponibili. In caso di mancata collaborazione ingiustificata, il comportamento può essere valutato contro la parte inadempiente.

Il nesso causale tra violazione dell'AI Act e danno è automatico?

Non è automatico, ma quando il danno deriva dalla violazione di obblighi dell'AI Act il nesso causale è presunto, salvo prova contraria.

La conformità all'AI Act esclude la responsabilità per i danni?

No. La conformità agli obblighi europei, anche se certificata, non esclude automaticamente la responsabilità civile del soggetto convenuto.

Si può chiedere il risarcimento direttamente all'assicurazione?

Sì, quando il responsabile dispone di una polizza di responsabilità civile che copre il danno. Il danneggiato può agire direttamente contro l'assicurazione entro i limiti del massimale previsto dal contratto.

Entro quanto tempo il responsabile deve comunicare i dati della polizza?

Il soggetto interpellato deve comunicare entro **30 giorni** l'esistenza della copertura assicurativa, gli estremi della polizza e i dati dell'impresa assicuratrice.

Le nuove regole si applicano anche ai sistemi AI già usati dalla polizia?

Sì. I sistemi già utilizzati, oggetto di contratti o in fase di sviluppo e sperimentazione dovranno essere adeguati alle nuove disposizioni entro **un anno** dall'entrata in vigore, salvo le diverse scadenze previste dall'AI Act.