

DAL 30 SETTEMBRE 2026 IN VIGORE IL D.LGS. N. 160/2026: IA, ATTIVITÀ DI POLIZIA E TUTELE IN SEDE PENALE E CIVILE

2 ottobre 2026

AUTORI

Aurora Agostini

Partner



Giovanni Lombardi

Associate



Il 30 settembre 2026 è entrato in vigore il D.Lgs. 9 settembre 2026, n. 160 di adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2024/1689 (“AI Act”), che stabilisce regole armonizzate sull’intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l’attività di polizia e di responsabilità civile e penale (il “Decreto”). Il Decreto è il primo atto adottato in attuazione della delega di cui all’art. 24 della Legge 23 settembre 2025, n. 132 (“Legge IA”). Un secondo atto, sui poteri delle autorità designate dall’art. 20 della Legge IA, è in procinto di pubblicazione (schema approvato dal Consiglio dei ministri il 4 agosto 2026) in vista del termine del 10 ottobre 2026 fissato dal citato art. 24 della Legge IA.



CONTESTO DEL DECRETO

Il Decreto si colloca in un impianto normativo “antropocentrico”, in cui l’IA è strumento di supporto, non sostitutivo, della decisione umana, nel rispetto dei diritti fondamentali, dei principi di trasparenza, proporzionalità e non discriminazione e delle norme sulla protezione dei dati personali.

In questo contesto, il Decreto interviene su tre direttrici principali:

- (i) impiego dei sistemi di IA da parte delle Forze di polizia;
- (ii) nuove disposizioni penali e processuali in materia di realizzazione e uso illecito di sistemi di IA;
- (iii) rafforzamento degli strumenti processuali civili a tutela dei soggetti danneggiati dall’utilizzo di sistemi di IA.

IA E ATTIVITÀ DI POLIZIA

Il Titolo I del D.Lgs. 160/2026 disciplina l’uso di sistemi e modelli di IA da parte delle Forze di polizia, nel rispetto dei diritti fondamentali e dei principi di proporzionalità, non discriminazione, sorveglianza umana e trasparenza richiamati dalla Legge IA. L’impiego segue un approccio “fondato sul rischio”, coerente con l’AI Act, calibrando le garanzie in base al livello di rischio (inclusi i sistemi ad alto rischio).





Il fulcro è la sorveglianza umana qualificata: prima che gli *output* di un sistema di IA possano essere usati in atti o provvedimenti incidenti sulla sfera giuridica degli interessati, occorre una revisione umana adeguata, documentata e tracciabile, svolta da personale individuato. A tal fine, il Decreto, in attuazione dell'art. 4 dell'AI Act, prevede un obbligo di formazione specialistica per il personale delle Forze di polizia, che assicuri: (i) comprensione dei principi di funzionamento dei sistemi di IA; (ii) conoscenza di limiti e *bias*; (iii) capacità di interpretazione critica degli *output*; e (iv) consapevolezza delle implicazioni giuridiche ed etiche e dei rischi di cybersicurezza.

Il Decreto promuove altresì progetti di ricerca e sperimentazione con università, enti di ricerca e soggetti pubblici o privati per sviluppare e testare sistemi di IA destinati all'attività di polizia, nel rispetto delle norme su concorrenza e aiuti di Stato. Tali collaborazioni devono disciplinare la titolarità dei diritti di proprietà intellettuale e industriale sui risultati della ricerca, sui modelli e sui dati di addestramento, nonché i ruoli *privacy* (titolare, contitolare, responsabile del trattamento) e le relative misure di sicurezza, escludendo la condivisione di dati operativi sensibili e garantendo alle Forze di polizia la titolarità dei modelli addestrati su tali dati.

BIOMETRIA E RICONOSCIMENTO FACCIALE

Tra i profili più delicati del Decreto ci sono l'identificazione biometrica remota in tempo reale nei luoghi pubblici e la videosorveglianza con riconoscimento facciale a posteriori.

Sul primo fronte il legislatore, in linea con l'AI Act, ammette l'identificazione in tempo reale solo previo vaglio dell'autorità giudiziaria e per finalità circoscritte (quali la prevenzione o la ricerca di persone scomparse e di vittime di determinati reati), ed è esclusa qualsiasi forma di controllo generalizzato. Le condizioni di accesso sono inoltre accompagnate da un sistema di garanzie e, in particolare: (i) le banche dati biometriche si costituiscono caso per caso, contengono solo i dati necessari e vanno cancellate quando scade l'autorizzazione; (ii) non è possibile alimentare archivi incrementali né raccogliere dati con *scraping* non mirato; (iii) prima di ogni impiego va svolta una valutazione d'impatto sui diritti fondamentali e sulla protezione dei dati; (iv) ogni utilizzo deve essere inoltre registrato in *log* non modificabili, consultabili dalle autorità di controllo; e (v) dopo l'utilizzo, il titolare del trattamento ne dà notifica al Garante, previo nulla osta dell'autorità giudiziaria.

Per quanto riguarda la videosorveglianza, dove la legge ne consente l'installazione i sistemi possono integrare componenti di IA, ma il riconoscimento facciale si attiva solo dopo l'acquisizione delle immagini e, per la ricerca mirata di un indiziato, previa autorizzazione del giudice per le indagini preliminari, salvo l'identificazione iniziale subito dopo il reato. È vietato ogni utilizzo non mirato o generalizzato e, in



caso di violazione, l'uso cessa e i dati vengono cancellati. Per luoghi ed eventi con particolari esigenze di ordine pubblico, le immagini dei volti sono conservate localmente per sette giorni, senza elaborazione biometrica fino alla commissione di un reato.

NUOVE FATTISPECIE PENALI, RESPONSABILITÀ DEGLI ENTI E RAFFORZAMENTO DELLE AZIONI CIVILI

Il Titolo II attua la delega della Legge IA su realizzazione e impiego illecito di sistemi di IA, intervenendo sul Codice penale, sulla responsabilità amministrativa degli enti ai sensi del D.Lgs. 231/2001 e sul piano processuale penale e civile.

In primo luogo, il Decreto introduce il nuovo art. 437-bis c.p., che punisce: (i) la mancata adozione di misure tecniche di sicurezza o di misure di sorveglianza umana per sistemi di IA ad alto rischio, quando da tale omissione derivi un pericolo per la vita o l'incolumità pubblica o individuale; e (ii) l'alterazione illecita di sistemi di IA ad alto rischio, qualora ne derivi un analogo pericolo. La stessa pena prevista per l'omissione si applica all'utilizzatore professionale di sistemi ad alto rischio che ometta intenzionalmente di adottare misure di sorveglianza umana.

In parallelo, il nuovo art. 25-vicies del D.Lgs. 231/2001 inserisce tra i reati presupposto, con sanzioni pecuniarie e interdittive, l'art. 437-bis c.p. e l'art. 612-quater c.p. (diffusione illecita di contenuti generati o alterati con IA), quest'ultimo già introdotto dalla Legge IA.

Il nuovo art. 359-ter c.p.p. introdotto dal Decreto disciplina identificazione e localizzazione mediante sistemi di IA per l'identificazione biometrica remota in tempo reale nelle indagini preliminari, previa autorizzazione del giudice per le indagini preliminari su richiesta del pubblico ministero, con individuazione di area, persone, tempi e modalità e durata massima di quindici giorni prorogabili. In caso di urgenza provvede il pubblico ministero con decreto, soggetto a convalida del giudice e, solo se non è possibile attenderlo, la polizia giudiziaria. I risultati ottenuti in violazione sono inutilizzabili e vanno cancellati.

Per imprese e danneggiati, il Decreto rafforza gli strumenti processuali civili in caso di danni da sistemi di IA e prevede:

- (i) una competenza territoriale agevolata per il danneggiato persona fisica che agisce per scopi estranei alla propria attività imprenditoriale o professionale, riconoscendo la competenza anche del giudice del luogo di residenza o domicilio del danneggiato;
- (ii) un meccanismo di accesso alle prove, che consente al giudice di ordinare alla controparte o a terzi l'esibizione di elementi di prova pertinenti relativi



al funzionamento del sistema di IA, qualora l'attore renda verosimile la fondatezza della domanda;

- (iii) una presunzione relativa del nesso di causalità tra violazione degli obblighi previsti dall'AI Act e danno, salvo prova contraria;
- (iv) la possibilità per il danneggiato di chiedere informazioni circa l'esistenza di una copertura assicurativa per la responsabilità civile relativa al danno dedotto e di esercitare, in presenza di tale copertura, un'azione diretta nei confronti dell'impresa di assicurazione nei limiti delle somme assicurate;
- (v) la conformità all'AI Act, anche se certificata, non esclude di per sé la responsabilità.

CONCLUSIONI E IMPLICAZIONI PRATICHE

Il Decreto ridisegna i processi interni di Forze di polizia, imprese che sviluppino o usino sistemi di IA e operatori assicurativi.

Per le Forze di polizia, le priorità operative possono includere:

- (i) la mappatura dei sistemi di IA in fase di sviluppo, sperimentazione o già in uso;
- (ii) la revisione dei rapporti contrattuali con fornitori tecnologici e *partner* di ricerca;
- (iii) la definizione e documentazione delle procedure di sorveglianza umana, con chiara individuazione dei ruoli e responsabilità;
- (iv) l'istituzione e l'aggiornamento dei programmi formativi obbligatori.

Alle imprese che forniscono o utilizzano sistemi di IA negli ambiti toccati dal Decreto (quali videosorveglianza, analisi predittiva, sistemi biometrici), possono essere richiesti:

- (i) un *audit* tecnico-giuridico dei sistemi offerti o integrati nelle soluzioni per le Forze di polizia;
- (ii) la revisione dei contratti con i clienti pubblici per includere clausole specifiche su responsabilità, ripartizione dei rischi e gestione degli incidenti;
- (iii) l'adozione di una documentazione tecnica e organizzativa che consenta di dimostrare la conformità agli obblighi dell'AI Act e del Decreto, in particolare in relazione alla gestione dei dati biometrici, alla tracciabilità degli *output* e alle misure di mitigazione dei bias.

Per gli operatori assicurativi potrà essere necessario:

- (i) sviluppare prodotti assicurativi specifici per i rischi connessi all'uso di sistemi di IA;
- (ii) integrare nei questionari informativi domande mirate sulla classificazione dei sistemi di IA, sulle procedure di sorveglianza umana, sulle valutazioni di impatto e sulla *governance* complessiva;
- (iii) predisporre procedure di gestione dei sinistri che tengano conto dei nuovi strumenti processuali.

In regime transitorio, i sistemi di IA già contrattualizzati, in uso o in sperimentazione per finalità di polizia alla data di entrata in vigore del Decreto devono essere resi compatibili con le disposizioni del Capo II del Titolo I entro un anno. Per le disposizioni del Titolo I la cui applicazione dipende dall'AI Act valgono invece i termini di entrata in vigore e di attuazione dell'AI Act stesso.

TEAM



Aurora Agostini

Partner



Giulietta Minucci

Partner



Marco Grechi

Senior Associate



Giovanni Lombardi

Associate



Alessandro Carlini

Associate



Francesca Costarelli

Associate



Questo documento è fornito a scopo informativo generale e non intende fornire consulenza legale sui temi trattati. I destinatari di questo documento non possono fare affidamento sui suoi contenuti. LEXIA e/o i professionisti dello studio non possono essere ritenuti responsabili in alcun modo per i contenuti di questo documento, né sulla base di un incarico professionale né per qualsiasi altra ragione.