

INNOVA JUS

RIVISTA MENSILE DEL CENTRO STUDI INNOVA JUS

Anno I · Numero 6 · Ottobre 2026

TEMA MONOGRAFICO

L'IA tra polizia e processo

Il d.lgs. 9 settembre 2026, n. 160: identificazione biometrica, nuovi reati e risarcimento del danno

Il primo decreto legislativo di adeguamento all'AI Act non comincia dalle autorità né dalle imprese: comincia dal punto in cui l'intelligenza artificiale tocca la libertà personale e il patrimonio delle persone. Letto articolo per articolo, con i regimi autorizzativi, le nuove fattispecie penali, le regole sulla prova nel giudizio civile e la mappa degli adempimenti per ciascun destinatario.

CON UN CONTRIBUTO DI LUCA FRESCURA SULL'AMMINISTRAZIONE AUMENTATA
NEI PICCOLI COMUNI

INNOVA JUS

RIVISTA MENSILE DEL CENTRO STUDI INNOVA JUS · ANNO I · NUMERO 6 · OTTOBRE 2026

TESTATA

Innova Jus. Rivista mensile del Centro Studi Innova Jus.

ISSN

ISSN 3103-8697 (edizione elettronica). Titolo chiave: Innova jus.

DIREZIONE SCIENTIFICA

Prof. Michele Iaselli — Direttore del Centro Studi Innova Jus, docente di Informatica giuridica e Diritto dell'intelligenza artificiale presso l'Università di Cassino e del Lazio Meridionale, già docente presso la LUISS Guido Carli, Coordinatore del Comitato Scientifico di Federprivacy.

TEMA DEL NUMERO

Il decreto legislativo 9 settembre 2026, n. 160, primo decreto di adeguamento al regolamento (UE) 2024/1689 adottato in attuazione dell'art. 24 della legge n. 132/2025: l'impiego dei sistemi di IA nell'attività di polizia, l'identificazione biometrica remota in tempo reale e a posteriori, il nuovo art. 437-bis del codice penale, la responsabilità degli enti e gli strumenti processuali civili per il risarcimento del danno cagionato dall'uso di sistemi di IA. Il numero ospita inoltre il contributo di Luca Frescura sull'intelligenza artificiale e la capacità amministrativa dei piccoli comuni.

PERIODICITÀ

Mensile. Ogni numero è dedicato a un argomento monografico di diritto dell'innovazione, con approfondimenti sistematici, ricognizione delle fonti primarie e profili operativi.

EDITORE

Centro Studi Innova Jus — Via Giovanni Merliani, 19 — 80127 Napoli (Italia).

Sito: innovajus.it — Posta elettronica: info@innovajus.it

LINGUA

Italiano.

SUPPORTO E DIFFUSIONE

Edizione elettronica in formato PDF, diffusa gratuitamente sul sito dell'editore.

AVVERTENZA METODOLOGICA

I riferimenti normativi sono citati sulla base delle fonti ufficiali: EUR-Lex e la Gazzetta ufficiale dell'Unione europea per il diritto dell'Unione; la Gazzetta Ufficiale della Repubblica italiana per il diritto interno. Il d.lgs. n. 160/2026 è commentato sul testo pubblicato nella Gazzetta Ufficiale, Serie generale, n. 214 del 15 settembre 2026, e sulle relative note; ove il testo presenti imperfezioni redazionali, queste sono segnalate. I profili in evoluzione sono espressamente indicati come tali. I contributi ospitati esprimono le valutazioni dei rispettivi autori.

NOTA SUL RAPPORTO CON IL FASCICOLO PRECEDENTE

Il n. 5 (settembre 2026), chiuso il 25 agosto, indicava fra i profili aperti gli estremi di pubblicazione dei decreti legislativi di adeguamento approvati in esame definitivo dal Consiglio dei ministri il 4 agosto 2026. Il presente numero è dedicato al primo di essi a essere pubblicato in Gazzetta Ufficiale; la rubrica di aggiornamento dà conto degli altri profili allora lasciati aperti.

CHIUSURA DEL FASCICOLO

Il fascicolo è chiuso alla data del 25 settembre 2026.

IN QUESTO NUMERO

Sommario

EDITORIALE Cominciare dal punto più delicato

-
- I** L'atto: delega, struttura, decorrenze del d.lgs. n. 160/2026
-
- II** Il perimetro: oggetto, definizioni e clausola di non aggravamento
-
- III** Il controllo umano: revisione qualificata e sorveglianza, due garanzie distinte
-
- IV** La ricerca: collaborazioni, titolarità dei modelli, spazi di sperimentazione
-
- V** La formazione: cinque risultati minimi per il personale di polizia
-
- VI** I dati biometrici: etichettatura, filtraggio e categorizzazione
-
- VII** Il tempo reale: l'identificazione biometrica remota e i suoi due regimi
-
- VIII** Le garanzie: valutazioni d'impatto, registrazioni, notifica al Garante
-
- IX** Il riconoscimento a posteriori: videosorveglianza e riconoscimento facciale
-
- X** Il diritto penale: l'art. 437-bis c.p. e la responsabilità degli enti
-
- XI** Il processo civile: accesso alle prove, presunzione causale, azione diretta
-
- XII** Gli adempimenti: norme transitorie, atti attuativi, destinatari
-

CONTRIBUTO Luca Frescura, L'amministrazione aumentata. Intelligenza artificiale e capacità amministrativa nei piccoli comuni

RUBRICA Aggiornamenti al fascicolo n. 5

APPARATO Riferimenti normativi e fonti

EDITORIALE

Cominciare dal punto più delicato

Il numero di settembre si chiudeva segnalando, fra i profili rimasti aperti, gli estremi di pubblicazione dei decreti legislativi di adeguamento all'AI Act approvati in esame definitivo dal Consiglio dei ministri il 4 agosto 2026. Il primo è ora in Gazzetta Ufficiale: è il decreto legislativo 9 settembre 2026, n. 160, pubblicato nella Serie generale n. 214 del 15 settembre. A esso è dedicato per intero questo fascicolo.

La scelta compiuta dal legislatore delegato merita di essere notata prima ancora di essere commentata. Il primo atto con cui l'ordinamento italiano dà seguito normativo alla delega dell'art. 24 della legge n. 132/2025 non riguarda le autorità di vigilanza, né le imprese, né la pubblica amministrazione in generale. Riguarda le Forze di polizia, il diritto penale e il processo civile. Si è cominciato, cioè, dal punto in cui l'impiego dell'intelligenza artificiale incide più direttamente sulla libertà personale e sul patrimonio delle persone: il volto ripreso da una telecamera e confrontato con una banca dati, il sistema difettoso che cagiona un danno, l'omissione di una cautela che mette in pericolo l'incolumità.

Tre linee attraversano il testo. La prima è la garanzia: l'identificazione biometrica remota in tempo reale è ammessa soltanto previa autorizzazione dell'autorità giudiziaria, per un tempo che non può eccedere quindici giorni, su un'area delimitata e nei confronti di persone indicate, con banche dati costruite per la singola autorizzazione e non alimentabili in modo incrementale; i risultati ottenuti fuori da queste regole non possono essere utilizzati. La seconda è la sanzione: un nuovo delitto, collocato dopo l'art. 437 del codice penale, punisce l'omessa adozione delle misure di sicurezza e di sorveglianza umana sui sistemi ad alto rischio, e la responsabilità degli enti si estende a esso e alla diffusione illecita di contenuti generati con l'IA. La terza è il riequilibrio probatorio: nel giudizio di risarcimento il danneggiato può ottenere l'esibizione della documentazione del sistema, e quando il danno deriva dalla violazione di un obbligo del regolamento il nesso causale è presunto.

La conformità al regolamento, anche se certificata, non esclude di per sé la responsabilità: è la frase del decreto destinata a cambiare il modo di redigere la documentazione tecnica.

Su quest'ultimo profilo conviene soffermarsi, perché è quello che investe la platea più ampia. Le regole sull'accesso alle prove si applicano a ogni azione di risarcimento del danno, contrattuale o extracontrattuale, cagionato nell'utilizzo di un sistema di intelligenza artificiale, senza limitazione ai sistemi ad alto rischio. I registri, la documentazione del sistema di gestione dei rischi, la documentazione tecnica e le informazioni sulla supervisione umana entrano nel processo come elementi di prova di cui il giudice può ordinare l'esibizione; e se la parte, senza giustificato motivo, non la esegue, il giudice, valutato ogni altro elemento, ritiene come ammessi i fatti allegati dall'istante. Il filo con il fascicolo precedente è diretto. A settembre si osservava che l'autorità di vigilanza non avrebbe chiesto dichiarazioni di conformità, ma i documenti che esse presuppongono. Ora lo stesso vale davanti al giudice civile, e con una conseguenza più immediata: il documento che manca non è soltanto una lacuna, è un fatto che può essere ritenuto provato contro chi avrebbe dovuto produrlo.

Il fascicolo ospita inoltre il contributo di Luca Frescura sull'«amministrazione aumentata» nei piccoli comuni. Non si tratta di una digressione. Il decreto chiama in causa gli enti locali quando disciplina l'integrazione di componenti di IA nelle piattaforme di videosorveglianza, e fa della formazione del personale e della revisione umana qualificata i presupposti dell'impiego dei sistemi. Il «paradosso della capacità» che Frescura descrive per le amministrazioni comunali — gli enti che più potrebbero giovare dell'IA sono i meno attrezzati per governarla — si ritrova, su altra scala, in ogni amministrazione chiamata a sorvegliare un sistema che non ha progettato.

Un'avvertenza sul metodo. Il commento è condotto sul testo pubblicato in Gazzetta Ufficiale e sulle relative note. Dove il testo presenta imperfezioni redazionali — ve ne sono due, nell'articolo sulle definizioni — lo si segnala, perché la precisione del rinvio non è un dettaglio in un atto che integra il precetto penale e disciplina l'utilizzabilità della prova.

Prof. Michele Iaselli

Direttore del Centro Studi Innova Jus

Il d.lgs. n. 160/2026: delega, struttura, decorrenze

Il decreto consta di ventidue articoli ripartiti in tre titoli ed esercita due deleghe distinte contenute nel medesimo art. 24 della legge n. 132/2025. Tenerle separate è la prima condizione per leggerlo correttamente.

Le due deleghe

Le premesse richiamano l'art. 24, commi 1, 2, lettera h), 3 e 5, della legge n. 132/2025. Il comma 1 delega il Governo ad adeguare la normativa nazionale al regolamento (UE) 2024/1689; fra i criteri specifici del comma 2, la lettera h) prevede un'apposita disciplina per l'utilizzo dei sistemi di IA nell'attività di polizia. È la base del titolo I.

Il comma 3 conferisce una delega diversa: adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale. I criteri del comma 5 trovano riscontro nel titolo II: strumenti, anche cautelari, per inibire la diffusione e rimuovere contenuti generati illecitamente (lettera a), attuata dall'art. 14); autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione di misure di sicurezza quando ne derivi pericolo concreto per la vita, l'incolumità o la sicurezza dello Stato (lettera b), attuata dall'art. 12); criteri di imputazione della responsabilità penale e di quella degli enti (lettera c), cui si collega l'art. 15); strumenti di tutela del danneggiato nella responsabilità civile, anche mediante una disciplina dell'onere della prova (lettera d), attuata dagli artt. 16-20); regolazione dell'uso dell'IA nelle indagini preliminari (lettera e), attuata dall'art. 13).

L'iter

Adottato in esame preliminare dal Consiglio dei ministri il 10 giugno 2026, acquisiti i pareri del Garante per la protezione dei dati personali, della Conferenza unificata (seduta del 20 luglio 2026) e delle Commissioni parlamentari, il decreto è stato deliberato in via definitiva il 4 agosto ed emanato il 9 settembre 2026.

L'entrata in vigore

Il decreto non contiene una disposizione sulla propria entrata in vigore. Opera pertanto l'ordinario termine di quindici giorni dalla pubblicazione, previsto dall'art. 73, terzo comma, della Costituzione e dall'art. 10 delle disposizioni sulla legge in generale: pubblicato il 15 settembre, il decreto è in vigore dal 30 settembre 2026. Per le disposizioni del titolo I la cui applicazione dipende dal regolamento IA si osservano invece i termini di quest'ultimo (art. 21, comma 2).

LA STRUTTURA DEL DECRETO

PARTIZIONE	ARTICOLI	OGGETTO
Titolo I, capo I	1-2	Oggetto, finalità e definizioni.
Titolo I, capo II	3-6	Utilizzo e revisione umana; collaborazioni; spazi di sperimentazione; formazione.
Titolo I, capo III	7-10	Dati biometrici; identificazione in tempo reale; garanzie; riconoscimento a posteriori.
Titolo II, capo I	11-15	Art. 437-bis c.p.; art. 359-ter c.p.p.; art. 104 disp. att. c.p.p.; art. 25-vicies d.lgs. 231/2001.
Titolo II, capo II	16-20	Foro, accesso alle prove, presunzione causale, conformità, azione diretta.
Titolo III, capo I	21-22	Disposizioni transitorie; invarianza finanziaria.

CHE COSA IL DECRETO NON CONTIENE

Il decreto non designa autorità, non attribuisce poteri di vigilanza, non disciplina le sanzioni amministrative dell'art. 99 del regolamento: materie dell'altro schema approvato il 4 agosto. Risponde a due domande diverse: a quali condizioni le Forze di polizia possono usare l'IA, e che cosa accade, sul piano penale e civile, quando un sistema è impiegato illecitamente o cagiona un danno.

Il titolo I: oggetto, definizioni e clausola di non aggravamento

Il titolo I disciplina l'impiego dei sistemi di IA da parte di organi, uffici e comandi delle Forze di polizia, in relazione alle funzioni esercitate. Due scelte ne definiscono il perimetro: il rinvio alle definizioni del regolamento e una clausola che esclude obblighi ulteriori.

I destinatari e le finalità

Destinatarie sono le Forze di polizia di cui all'art. 16 della legge n. 121/1981 (art. 2, lettera o). L'«attività di polizia» coincide con le attività di contrasto definite dall'art. 3, punto 46), del regolamento, svolte dagli organi, uffici e comandi delle Forze di polizia nell'esercizio delle rispettive attribuzioni (lettera p); le «finalità di polizia» sono quelle di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la loro prevenzione (lettera q). L'art. 1, comma 2, richiama i diritti garantiti dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione e dalla CEDU, e i principi dell'art. 3 della legge n. 132/2025.

Le definizioni proprie

Quasi tutte le definizioni dell'art. 2 rinviano al regolamento. Tre meritano attenzione. I *dati operativi sensibili* (lettera h), definiti per rinvio all'art. 3, punto 38), del regolamento, sono la nozione cardine del titolo: ricorrono negli artt. 3, 4, 5 e 9 e segnano il confine di ciò che non può uscire dalla disponibilità delle Forze di polizia. Lo *scraping non mirato* (lettera l) riceve invece una definizione autonoma: l'estrazione e la raccolta automatizzata e indiscriminata, su larga scala, mediante un sistema di IA, di immagini facciali dalla rete internet o da filmati di telecamere a circuito chiuso, allo scopo di creare o ampliare banche dati di riconoscimento facciale. È la condotta che l'art. 5, paragrafo 1, lettera e), del regolamento vieta, e che il decreto assume come causa di inutilizzabilità delle banche dati biometriche. Le *Autorità nazionali per l'intelligenza artificiale* (lettera m) sono l'AgID e l'ACN, ai sensi dell'art. 20, comma 1, della legge n. 132/2025.

La clausola di non aggravamento

L'art. 1, comma 3, stabilisce che il titolo non comporta nuovi obblighi rispetto a quelli previsti dal regolamento per i sistemi e i modelli utilizzati nelle attività e per le finalità di polizia; l'art. 3, comma 7, lo ribadisce, facendo salve le esclusioni previste dal regolamento stesso. La clausola va presa sul serio, perché chiarisce la funzione dell'intero titolo. Esso non aggiunge requisiti ai sistemi: esercita le scelte che il regolamento rimette agli Stati membri — in particolare la facoltà, prevista dall'art. 5, paragrafo 5, di autorizzare con legge nazionale l'identificazione biometrica remota in tempo reale, e la disciplina dell'autorizzazione all'identificazione a posteriori di cui all'art. 26, paragrafo 10 — e ne fissa le condizioni procedurali, organizzative e formative. La clausola ha anche valore interpretativo: nel dubbio, la disposizione nazionale va letta come specificazione del regolamento, non come requisito aggiuntivo.

Il titolo I non aggiunge obblighi ai sistemi: sceglie, fra le possibilità che il regolamento lascia aperte, quelle che l'ordinamento italiano intende consentire, e a quali condizioni.

NOTA TESTUALE — ART. 2

Il testo pubblicato presenta due imperfezioni redazionali. La lettera q) rinvia alle «attività di polizia di cui alla lettera s)», ma l'elenco si arresta alla lettera q) e le attività di polizia sono definite alla lettera p): il rinvio va riferito a quest'ultima. Le lettere p) e q) citano inoltre il «regolamento (UE) 1689/2024», con inversione di numero e anno rispetto alla citazione corretta — regolamento (UE) 2024/1689 — adottata nel resto dell'atto. Nessuna pone seri dubbi interpretativi; entrambe si prestano a un avviso di rettifica.

III · IL CONTROLLO UMANO

Revisione umana qualificata e sorveglianza: due garanzie distinte

L’art. 3 è la norma di principio del titolo I. Vi convivono due garanzie che la lettura corrente tende a sovrapporre e che hanno invece fonte, ambito e oggetto diversi.

La funzione strumentale

Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo avvengono secondo un approccio antropocentrico, proporzionato e fondato sul rischio, che tenga conto della classificazione dei sistemi e delle diverse categorie di interessati (comma 1). La ricerca è orientata all’affidabilità operativa, per migliorare l’apporto dell’IA alle decisioni umane (comma 2). L’utilizzo dei sistemi e dei loro output avviene in funzione strumentale e di supporto, allo scopo di incrementare efficacia ed efficienza dell’attività (comma 3): è la stessa logica che la legge n. 132/2025 esprime per l’impiego dell’IA nella pubblica amministrazione.

La revisione umana qualificata

Il comma 4 impone, per l’utilizzo di qualsiasi sistema o modello — non soltanto di quelli ad alto rischio — «adeguate forme di revisione umana qualificata» dei risultati delle elaborazioni automatiche prima del loro impiego in atti e provvedimenti incidenti sulla sfera giuridica degli interessati. La revisione è effettuata da personale individuato dalle procedure interne di ciascuna Forza di polizia ed è documentata in modo da assicurarne la tracciabilità, nel rispetto dell’autonomia e delle sfere di competenza dei procedimenti decisionali.

La sorveglianza umana

Il comma 5 riguarda i soli sistemi ad alto rischio: le Forze di polizia assicurano che la sorveglianza umana sia effettiva e conforme all’art. 14 del regolamento, e che il personale preposto possieda le competenze e la formazione necessarie a prevenire e ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali. Il trattamento dei dati personali, compresi i dati operativi sensibili, resta regolato dal d.lgs. n. 51/2018 (comma 6).

REVISIONE E SORVEGLIANZA A CONFRONTO

	REVISIONE UMANA QUALIFICATA	SORVEGLIANZA UMANA
Fonte	Art. 3, comma 4, d.lgs. n. 160/2026.	Art. 3, comma 5, d.lgs. n. 160/2026; art. 14 del regolamento.
Ambito	Tutti i sistemi e i modelli di IA impiegati nell’attività di polizia.	I soli sistemi di IA ad alto rischio.
Oggetto	Il singolo output, prima del suo impiego in atti e provvedimenti incidenti sulla sfera giuridica degli interessati.	Il funzionamento del sistema nel periodo in cui è in uso.
Soggetto	Personale individuato dalle procedure interne di ciascuna Forza di polizia.	Personale dotato delle competenze e della formazione necessarie.
Forma	Documentata, in modo da assicurarne la tracciabilità.	Effettiva e conforme alle misure previste dall’art. 14 del regolamento.

IL PUNTO OPERATIVO

La revisione umana qualificata presuppone tre elementi da predisporre prima dell’impiego del sistema: l’atto interno che individua il personale abilitato alla revisione; la procedura che ne descrive le modalità; il supporto documentale che consente di ricostruire, per ciascun atto, quale output è stato esaminato, da chi e con quale esito. Senza quest’ultimo l’adempimento non è dimostrabile: ed è sulla dimostrabilità che il decreto, fino al processo civile, misura l’effettività del controllo umano.

IV · LA RICERCA

Collaborazioni, titolarità dei modelli e spazi di sperimentazione

Gli artt. 4 e 5 regolano la fase che precede l'impiego: la ricerca condotta con soggetti esterni e la sperimentazione negli spazi di sperimentazione normativa. Il filo conduttore: i dati operativi sensibili, e i modelli addestrati su di essi, restano alle Forze di polizia.

Le collaborazioni

Nell'ambito di specifici progetti di ricerca e sperimentazione, le Forze di polizia possono attivare collaborazioni con università, enti di ricerca e soggetti pubblici e privati, anche per il tramite di società in house o di società a totale partecipazione pubblica controllate dallo Stato, nel rispetto della disciplina europea in materia di concorrenza e di aiuti di Stato (art. 4, comma 1). I rapporti devono contenere clausole determinate.

LE CLAUSOLE NECESSARIE DELL'ACCORDO DI COLLABORAZIONE

CLAUSOLA	FONTE	CONTENUTO
Esclusione della condivisione	Art. 4, c. 2	Nessuna condivisione dei dati operativi sensibili con i partner.
Esclusione dell'acquisizione	Art. 4, c. 2	Nessuna acquisizione o utilizzazione, anche indiretta, da parte dei partner, di sistemi, risorse hardware e software o dispositivi addestrati per l'attività di polizia; salvo il ricorso a dati sintetici o a dati reali mascherati o pseudonimizzati.
Proprietà intellettuale	Art. 4, c. 3	Titolarietà dei diritti di proprietà intellettuale, industriale e di sfruttamento economico su risultati, modelli derivati, dati di addestramento e software (c.p.i.; art. 64 d.P.R. n. 382/1980).
Ruoli nel trattamento	Art. 4, c. 3	Titolari, contitolari e responsabili del trattamento, con obblighi, misure di sicurezza e documentazione (d.lgs. n. 51/2018).
Titolarietà dei modelli	Art. 4, c. 3	In ogni caso alle Forze di polizia i modelli addestrati su dati operativi sensibili.

L'ultima clausola non è negoziabile: la formula «è in ogni caso assicurata» la sottrae all'autonomia delle parti. Ne discende che l'accordo può ripartire liberamente la titolarità dei risultati della ricerca, ma non quella del modello che abbia visto dati operativi sensibili.

La base giuridica negli spazi di sperimentazione

L'art. 5 costituisce la base giuridica richiesta dall'art. 59, paragrafo 2, del regolamento, nonché dal d.lgs. n. 51/2018, per il trattamento di dati personali — inclusi i dati relativi a reati e le categorie particolari di dati — effettuato dalle Forze di polizia negli spazi di sperimentazione normativa, quando necessario per finalità di polizia. La partecipazione è finalizzata allo sviluppo, alla realizzazione e alla prova di sistemi destinati alle attività di polizia, in particolare ad alto rischio. La sperimentazione rispetta le condizioni cumulative dell'art. 59, paragrafo 1, del regolamento, coinvolge il Garante quando comporta trattamento di dati personali ed è raccordata con AgID e ACN, ferma l'esclusiva titolarità del trattamento dei dati operativi sensibili in capo alle amministrazioni. Un regolamento adottato con d.P.C.M., su proposta delle Autorità nazionali per l'IA, di concerto con il Ministro dell'interno e sentiti il Ministro dell'economia e il Garante, definirà il coordinamento con lo spazio di sperimentazione nazionale previsto dall'art. 57 del regolamento.

PER L'UNIVERSITÀ E L'IMPRESA PARTNER

Il partner non riceverà dati operativi sensibili e non potrà acquisire né utilizzare, anche indirettamente, il sistema addestrato per l'attività di polizia. La via praticabile è quella indicata dalla norma — dati sintetici, mascherati o pseudonimizzati — insieme a una definizione precisa, nell'accordo, degli artefatti «addestrati per l'attività di polizia», da cui dipende il perimetro dei suoi diritti.

La formazione del personale di polizia: cinque risultati minimi

L'art. 6 dichiara di dare attuazione, nel settore, all'art. 4 del regolamento. Non fissa ore né programmi: fissa risultati, e per questo è verificabile.

Le Forze di polizia attivano, presso i rispettivi istituti di formazione, specifici corsi in materia di intelligenza artificiale applicata alle attività di polizia, secondo modalità stabilite da ciascuna amministrazione nell'ambito delle risorse disponibili (comma 1). I corsi devono assicurare cinque risultati formativi minimi (comma 2), tre dei quali — quelli delle lettere b), c) ed e) — sono assicurati nell'ambito dei corsi specifici concernenti i sistemi ad alto rischio in uso o destinati a essere utilizzati nelle attività di polizia (comma 3).

I RISULTATI FORMATIVI MINIMI DELL'ART. 6, COMMA 2

LETT.	RISULTATO	SEDE
a)	Comprensione dei principi di funzionamento e delle potenzialità dei sistemi di IA, con particolare riferimento alle applicazioni nelle attività di polizia.	Formazione generale
b)	Conoscenza dei limiti, dei bias e degli errori dei sistemi, con specifica attenzione al riconoscimento biometrico e all'analisi predittiva.	Corsi specifici sui sistemi ad alto rischio
c)	Capacità di interpretazione critica degli output e consapevolezza del ruolo della sorveglianza umana qualificata.	Corsi specifici sui sistemi ad alto rischio
d)	Consapevolezza delle implicazioni giuridiche, etiche e di responsabilità, con riferimento al regolamento IA, al regolamento (UE) 2016/679 e al d.lgs. n. 51/2018.	Formazione generale
e)	Consapevolezza dei rischi di cybersicurezza connessi all'utilizzo dei sistemi, anche con riferimento alle indicazioni dell'ACN.	Corsi specifici sui sistemi ad alto rischio

Perché la sede conta

La collocazione dei risultati b), c) ed e) nei corsi specifici è coerente con la loro natura. La conoscenza dei limiti e degli errori, l'interpretazione critica dell'output e la consapevolezza dei rischi di sicurezza non si apprendono in astratto: si apprendono sul sistema che si userà, con i suoi tassi di errore, le sue condizioni d'impiego, le sue vulnerabilità.

Il risultato c) lega la formazione alla revisione umana qualificata dell'art. 3, comma 4. È il punto su cui insiste anche il contributo ospitato in questo numero, con il richiamo all'automation bias, la tendenza ad accordare eccessivo affidamento al risultato del sistema: una sorveglianza affidata a personale non formato rischia di ridursi a garanzia soltanto formale.

La revisione umana è qualificata soltanto se chi la compie sa dubitare dell'output che rivede.

Sull'assetto dell'obbligo di alfabetizzazione dopo le modifiche introdotte dal regolamento (UE) 2026/1744 si rinvia al n. 4 di questa rivista; qui rileva che il legislatore delegato ha scelto di ancorare l'art. 6 all'art. 4 del regolamento, facendone il parametro della formazione di settore.

IL PUNTO OPERATIVO, ANCHE FUORI DAL SETTORE

L'elenco dell'art. 6 è il primo catalogo normativo di risultati formativi in materia di IA contenuto in una fonte primaria nazionale. Vincolante per le sole Forze di polizia, offre a ogni organizzazione un parametro per strutturare e documentare i propri percorsi: distinguere formazione generale e formazione sul singolo sistema, indicando per ciascun percorso il risultato atteso e il modo di verificarlo.

VI · I DATI BIOMETRICI

Etichettatura, filtraggio e categorizzazione: quattro condizioni

L'art. 5, paragrafo 1, lettera g), del regolamento vieta i sistemi di categorizzazione biometrica che classificano le persone per trarre deduzioni su caratteristiche sensibili; il divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, né la categorizzazione di dati biometrici nel settore delle attività di contrasto. L'art. 7 del decreto disciplina questo spazio.

Nell'ambito delle attività di polizia, l'etichettatura, il filtraggio o la categorizzazione di set di dati biometrici acquisiti in conformità alla normativa vigente sono consentiti a quattro condizioni, che devono ricorrere congiuntamente.

LE CONDIZIONI DELL'ART. 7, COMMA 1

LETT.	CONDIZIONE	FUNZIONE
a)	Le operazioni non sono finalizzate a inferire o dedurre le caratteristiche di cui all'art. 5, paragrafo 1, lettera g), del regolamento.	Impedisce che l'eccezione diventi un varco verso la categorizzazione vietata.
b)	Sono funzionali ad attività di comparazione o ricerca, o ad altre attività conformi alla normativa vigente, esclusivamente per finalità di polizia.	Vincolo di scopo.
c)	Non costituiscono l'unico fondamento di decisioni che producono effetti giuridici nei confronti di persone fisiche.	Divieto di decisione esclusivamente automatizzata.
d)	Il titolare del trattamento adotta misure idonee a prevenire il reimpiego dei dati e dei risultati per finalità incompatibili con quelle della raccolta.	Presidio organizzativo della limitazione della finalità.

Il comma 2 aggiunge che il trattamento tiene conto, ai fini degli obblighi del regolamento, della classificazione dei sistemi, avuto riguardo anche agli orientamenti della Commissione sull'attuazione pratica adottati ai sensi degli artt. 6, paragrafo 5, e 96 del regolamento, ed è svolto nel rispetto del d.lgs. n. 51/2018. Il richiamo agli orientamenti non è di stile: la stessa operazione di categorizzazione può rientrare o meno fra i sistemi ad alto rischio a seconda della sua funzione, e la classificazione determina gli obblighi applicabili.

Il senso della condizione a)

La condizione a) ripete, in apparenza, ciò che il regolamento già dice. Ma la ripetizione ha una funzione precisa: l'eccezione dell'art. 5, paragrafo 1, lettera g), riguarda l'etichettatura, il filtraggio e la categorizzazione come operazioni sui dati, non come strumenti per ricavare dalla biometria la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita o l'orientamento sessuale di una persona. Il decreto rende esplicito che neppure nel settore delle attività di contrasto l'eccezione consente quelle inferenze.

IL PUNTO OPERATIVO

Le condizioni c) e d) sono condizioni organizzative, non tecniche: presuppongono procedure che impediscano l'adozione di decisioni fondate soltanto sul risultato della categorizzazione e misure che impediscano il reimpiego dei dati e dei risultati. La loro esistenza va documentata nel registro dei trattamenti e nella valutazione d'impatto, perché è su quei documenti che si misura l'osservanza dell'art. 7.

L'identificazione biometrica remota in tempo reale: due regimi

Il regolamento vieta l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, salvo tre finalità tassative, e consente agli Stati membri di autorizzarlo con legge nazionale (art. 5, paragrafi 1, lettera h), e 5). Il decreto esercita questa facoltà su due binari distinti: uno preventivo, sotto il controllo del pubblico ministero; uno processuale, sotto il controllo del giudice per le indagini preliminari.

Il regime preventivo: l'art. 8

L'uso da parte degli organi, uffici e comandi delle Forze di polizia in luoghi pubblici o aperti al pubblico è ammesso per le finalità di prevenzione dell'art. 5, paragrafo 1, lettera h), punto ii), del regolamento, e per la ricerca di persone scomparse o di vittime specifiche dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale (punto i). È consentito esclusivamente per confermare l'identità delle persone specificamente interessate o per la ricerca mirata, anche dinamica e compresa la localizzazione, di persone individuate o individuabili in relazione alla minaccia da prevenire o alla ricerca da eseguire.

L'uso è subordinato a una richiesta del questore o del comandante provinciale dell'Arma dei carabinieri e della Guardia di finanza, ovvero dei responsabili dei Servizi centrali di cui all'art. 12 del d.l. n. 152/1991, al procuratore della Repubblica presso il tribunale del capoluogo del distretto in cui sono emerse le esigenze. La richiesta indica finalità, durata, area, persone interessate e ricercate, banche dati e tecnologie impiegate. L'autorizzazione è concessa per uno specifico evento o per il tempo strettamente necessario, non oltre quindici giorni prorogabili per periodi di quindici giorni con decreto motivato, per un'area delimitata e previa effettuazione delle valutazioni dell'art. 5, paragrafo 2, del regolamento. Nei casi d'urgenza l'uso può essere avviato su disposizione del questore o dei comandanti, previa comunicazione anche orale al procuratore; la richiesta è trasmessa entro ventiquattro ore dall'inizio delle operazioni, e il procuratore provvede nelle ventiquattro ore successive.

Il modello è dichiaratamente quello delle intercettazioni preventive: stessi soggetti richiedenti, stessa autorità autorizzante, e il comma 9 richiama espressamente l'art. 226, comma 5, delle disposizioni di attuazione del codice di procedura penale, per il quale gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi.

Il regime processuale: l'art. 359-ter c.p.p.

L'art. 13 inserisce nel codice di procedura penale l'art. 359-ter. L'impiego può essere autorizzato per confermare l'identificazione di una persona nei cui confronti vi sono sufficienti indizi di uno dei delitti dell'allegato II del regolamento puniti con la reclusione non inferiore nel massimo a quattro anni, o per la ricerca mirata, compresa la localizzazione, di una persona indiziata dei medesimi delitti; per la localizzazione del latitante ricercato in esecuzione di una misura cautelare coercitiva o di un ordine di carcerazione non sospeso per quei delitti; per la ricerca mirata, nel procedimento penale, di specifiche vittime di sottrazione, tratta o sfruttamento sessuale. L'autorizzazione è chiesta dal pubblico ministero al giudice per le indagini preliminari, che provvede con decreto motivato delimitando l'area, indicando le persone ricercate e fissando un tempo non superiore a quindici giorni, prorogabile.

I DUE REGIMI A CONFRONTO

	ART. 8 D.LGS. N. 160/2026	ART. 359-TER C.P.P.
Natura	Attività preventiva di polizia.	Atto di indagine nel procedimento penale.
Finalità	Prevenzione ex art. 5, par. 1, lett. h), punto ii); ricerca di persone scomparse e di vittime di sequestro, tratta, sfruttamento sessuale.	Identificazione o ricerca di indiziati di delitti dell'allegato II puniti con almeno quattro anni nel massimo; ricerca di latitanti; ricerca di vittime.
Chi chiede	Questore, comandante provinciale CC o GdF, responsabili dei Servizi centrali.	Pubblico ministero.
Chi autorizza	Procuratore della Repubblica presso il tribunale del capoluogo del distretto.	Giudice per le indagini preliminari.

Durata	Evento specifico o tempo strettamente necessario, fino a 15 giorni prorogabili di 15 in 15.	Tempo strettamente necessario, fino a 15 giorni prorogabili di 15 in 15.
Urgenza	Avvio su disposizione dell'autorità di polizia, previa comunicazione anche orale; richiesta entro 24 ore, provvedimento nelle 24 ore successive.	Decreto del PM comunicato entro 24 ore, convalida del GIP entro 48; se non si può attendere il PM, attivazione da parte degli UPG, richiesta entro 12 ore, convalida chiesta entro 24 ore dall'avvio e decisa nelle 48 successive.
Violazione	Interruzione, cancellazione di dati e output, salvo quanto acquisito legittimamente sotto altra base giuridica; risultati inutilizzabili.	Risultati inutilizzabili; cancellazione di dati e output, salvo che costituiscano corpo del reato.

LA BANCA DATI DI RIFERIMENTO: LA REGOLA COMUNE

In entrambi i regimi il confronto biometrico avviene esclusivamente con una banca dati di riferimento adeguata alla finalità. Può essere derivata da banche dati in uso alle Forze di polizia o ad altre amministrazioni, o da immagini e altri elementi acquisiti legalmente; ma il suo contenuto è formato appositamente per ciascun utilizzo, con i soli dati pertinenti, ed è cancellato alla scadenza dell'autorizzazione, così che il set di confronto sia specifico per ciascuna autorizzazione e non si alimenti in modo incrementale. È vietato l'uso di banche dati alimentate, anche in parte, mediante scraping non mirato o costituite in violazione della normativa sulla protezione dei dati. Dagli archivi generali si può attingere; con gli archivi generali non si può confrontare.

VIII · LE GARANZIE

Valutazioni d'impatto, registrazioni, notifica al Garante

L'art. 9 dà attuazione ai paragrafi 2 e 4 dell'art. 5 del regolamento e si applica a entrambi i regimi del tempo reale. Contiene tre garanzie e rinvia la parte tecnica a un decreto ministeriale.

Due valutazioni, non una

Il titolare del trattamento completa in via preventiva una valutazione d'impatto sui diritti fondamentali secondo l'art. 27 del regolamento, ed effettua la valutazione d'impatto sulla protezione dei dati di cui agli artt. 23 e 24 del d.lgs. n. 51/2018 (comma 1). Le due valutazioni sono cumulative: la prima riguarda l'insieme dei diritti fondamentali incisi; la seconda i rischi connessi al trattamento dei dati.

Le registrazioni

Ogni utilizzo è registrato automaticamente in file di log non modificabili, che comprendono necessariamente i dati previsti dall'art. 12, paragrafo 3, del regolamento. I log sono conservati per cinque anni dall'accesso e dall'operazione e sono accessibili esclusivamente alle autorità competenti, per la verifica della liceità del trattamento, per il controllo interno e nell'ambito di un procedimento penale (comma 2). Restano fermi i termini di conservazione dei dati personali previsti dall'art. 10 del d.P.R. n. 15/2018 (comma 3).

La notifica al Garante

Dopo l'utilizzo, il titolare notifica al Garante, in conformità all'art. 5, paragrafo 4, del regolamento. La notifica richiede il nulla osta dell'autorità giudiziaria, differibile per esigenze di segretezza fino a tre mesi, rinnovabili una volta; contiene le informazioni essenziali su autorizzazione e risultato, senza dati operativi sensibili. Per più attivazioni nello stesso contesto operativo o per utilizzi omogenei, la notifica può essere periodica e cumulativa, ferma la necessità del nulla osta (comma 4).

IL CALENDARIO DELLE GARANZIE

ADEMPIMENTO	TERMINE	FONTE
Richiesta dopo l'avvio d'urgenza (preventivo)	24 ore; decisione nelle 24 successive	Art. 8, c. 7
Decreto d'urgenza del PM al GIP	24 ore; convalida nelle 48 successive	Art. 359-ter c.p.p.
Richiesta degli UPG al PM dopo l'attivazione	12 ore; convalida chiesta entro 24 ore, decisa in 48	Art. 359-ter c.p.p.
Conservazione dei file di log	5 anni dall'accesso e dall'operazione	Art. 9, c. 2
Differimento del nulla osta alla notifica	Fino a 3 mesi, rinnovabili una volta	Art. 9, c. 4

Il decreto ministeriale

Un decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, sentiti il Garante e le Autorità nazionali per l'IA, individuerà (comma 5) i requisiti minimi di affidabilità e accuratezza dei sistemi, il monitoraggio periodico delle prestazioni e dei bias, i requisiti delle banche dati di riferimento, le misure di sicurezza, le informazioni tecniche da allegare alla richiesta di autorizzazione, le modalità della notifica e gli ulteriori adempimenti del titolare.

UN PROFILO APERTO

Il decreto ministeriale non ha un termine di adozione, e il testo non vi subordina espressamente l'operatività degli artt. 8 e 359-ter. Ma senza requisiti minimi di accuratezza e senza le informazioni tecniche da allegare alla richiesta, l'autorità giudiziaria dovrebbe valutare la proporzionalità dell'impiego di un sistema di cui ignora l'affidabilità: è ragionevole attendersi che la prassi autorizzativa ne risenta fino all'adozione.

Videosorveglianza e riconoscimento facciale a posteriori

L'art. 10 è la disposizione del titolo I destinata alla diffusione più ampia: non riguarda sistemi nuovi, ma l'integrazione di componenti di IA negli impianti di videosorveglianza già consentiti dalla legge, compresi quelli degli enti locali.

L'integrazione e l'attivazione differita

Dove specifiche disposizioni di legge consentono l'installazione di sistemi di videosorveglianza, questi possono essere integrati con componenti di IA. Le componenti destinate al riconoscimento facciale non possono essere attivate se non nei casi e alle condizioni dei commi 2 e 3, e l'attivazione avviene dopo l'acquisizione delle immagini, con un intervallo tale da non configurare un'identificazione in tempo reale (comma 1).

L'autorizzazione del giudice

Per il riconoscimento a posteriori di una persona oggetto di ricerca mirata in quanto indiziata di un reato, il pubblico ministero, su istanza degli ufficiali di polizia giudiziaria che hanno avviato i sistemi, chiede l'autorizzazione al GIP senza ritardo e comunque entro quarantotto ore dall'avvio; il giudice provvede con decreto motivato nelle quarantotto ore successive. In difetto, l'uso è interrotto e dati, risultati e output sono cancellati, salvo che costituiscano corpo del reato (comma 2).

L'identificazione iniziale

In conformità all'art. 26, paragrafo 10, primo comma, del regolamento, l'autorizzazione non è richiesta quando le tecnologie sono utilizzate esclusivamente dopo la commissione di un reato, al solo fine dell'identificazione iniziale di una persona potenzialmente indiziata, sulla base di elementi oggettivi e verificabili direttamente connessi al fatto. L'utilizzo avviene sotto la diretta ed esclusiva responsabilità dell'ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine pubblico o, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria di cui all'art. 57, comma 1, lettere a) e b), c.p.p. che procede. In caso di inosservanza, i risultati sono inutilizzabili e i dati cancellati (comma 3).

Luoghi ed eventi con particolari esigenze di sicurezza

Per i luoghi e gli eventi individuati secondo i criteri di un decreto del Ministro dell'interno, il sistema tratta automaticamente le immagini del volto delle persone che vi accedono, senza elaborazione dei dati biometrici, e le memorizza a livello locale in una base dati di riferimento, insieme ai dati anagrafici e all'eventuale posto assegnato, acquisiti mediante scansione elettronica dei titoli di accesso. Soltanto dopo la commissione di un reato l'attivazione del riconoscimento facciale comporta l'elaborazione biometrica delle immagini memorizzate, per il confronto con quelle della persona indiziata (comma 4). I dati sono conservati per sette giorni e cancellati automaticamente (comma 7).

LE REGOLE COMUNI DELL'ART. 10

PROFILO	DISCIPLINA
Titolare	Ministero dell'interno – Dipartimento della pubblica sicurezza (comma 5).
Valutazione d'impatto	Preventiva, con consultazione del Garante ex artt. 23 e 24 d.lgs. n. 51/2018; ammessa un'unica valutazione per sistemi analoghi (comma 6).
Registrazioni	Accessi e operazioni soltanto da persone autorizzate, registrati in log non modificabili conservati cinque anni (comma 8).
Decisioni	Nessuna decisione con effetti giuridici negativi fondata unicamente sul riconoscimento facciale; garanzie dell'art. 8 d.lgs. n. 51/2018 (comma 10).
Divieti	Nessuna attivazione non mirata, senza collegamento con un reato o un procedimento, o a fini di identificazione generalizzata o indiscriminata (comma 11).

Installazione

Gestori dei luoghi, organizzatori o promotori degli eventi, chi dispone delle strutture, in accordo con i proprietari, con particolare riferimento agli enti locali per le loro piattaforme; i sistemi sono concessi in comodato gratuito alla questura, che ne acquisisce la completa ed esclusiva disponibilità (comma 13).

UNA NOTA PER GLI ENTI LOCALI

Il comune che dispone di una piattaforma di videosorveglianza può essere coinvolto nell'installazione e nella manutenzione delle componenti di IA, ma la titolarità del trattamento resta al Ministero dell'interno e il sistema passa in comodato gratuito alla questura, con disponibilità completa ed esclusiva. Il comma 13 richiede che i ruoli nel trattamento siano definiti nel rispetto del d.lgs. n. 51/2018, e il comma 14 esclude nuovi o maggiori oneri. Ne discende la necessità di un accordo che regoli ruoli, manutenzione, responsabilità e cessazione del comodato: esattamente il tipo di capacità di governo — giuridica prima che tecnica — che il contributo di Luca Frescura, in questo numero, individua come la risorsa più scarsa nelle amministrazioni di minori dimensioni.

L'art. 437-bis c.p. e la responsabilità degli enti

Il capo I del titolo II attua il criterio della lettera b) del comma 5 dell'art. 24: autonome fattispecie incentrate sull'omessa adozione di misure di sicurezza. La collocazione del nuovo delitto subito dopo l'art. 437 c.p. — rimozione od omissione dolosa di cautele contro infortuni sul lavoro — ne dichiara il bene giuridico: l'incolumità pubblica.

LE QUATTRO IPOTESI DELL'ART. 437-BIS C.P.

COMMA	CONDOTTA	PENA
Primo	Chiunque omette di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione o l'immissione sul mercato di sistemi ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni, ovvero omette di adottare misure di sorveglianza umana.	Da 1 a 5 anni se ne deriva pericolo per la vita o l'incolumità pubblica o individuale; da 2 a 8 anni se ne deriva pericolo per la sicurezza dello Stato.
Secondo	Salvo che il fatto costituisca più grave reato, chiunque, fuori dei casi del primo comma, altera sistemi ad alto rischio.	Da 2 a 6 anni per il pericolo per la vita o l'incolumità; da 3 a 10 anni per il pericolo per la sicurezza dello Stato.
Terzo	Fatti del primo comma commessi per colpa grave.	Pena ridotta «da un terzo a un sesto».
Quarto	L'utilizzatore professionale di sistemi ad alto rischio che omette intenzionalmente di adottare misure di sorveglianza umana.	Le pene del primo comma, secondo il tipo di pericolo.

Quattro nodi interpretativi

L'elemento soggettivo. Il terzo comma estende la punibilità alla colpa grave per i soli fatti del primo comma: se ne ricava che la fattispecie base è dolosa e che la colpa lieve resta fuori dall'area penale. La formula della riduzione — «da un terzo a un sesto», con la sequenza delle frazioni invertita rispetto all'uso consueto — è destinata a porre un problema di determinazione del trattamento sanzionatorio che la giurisprudenza dovrà sciogliere.

Il pericolo. La norma richiede che dall'omissione «derivi pericolo»: si tratta di un reato di pericolo concreto, in coerenza con il criterio di delega, che lo esigeva espressamente. Non basta l'omissione della misura: occorre accertare che essa abbia prodotto una situazione di pericolo effettivo.

Il rinvio al regolamento. Le misure tecniche di sicurezza e le misure di sorveglianza umana «previste» sono quelle che il regolamento impone per i sistemi ad alto rischio: la fattispecie è integrata dalla disciplina europea. Ne discende un problema intertemporale che il decreto non risolve espressamente. Secondo il calendario risultante dal regolamento (UE) 2026/1744, gli obblighi sui sistemi ad alto rischio si applicano dal 2 dicembre 2027 per quelli dell'allegato III e dal 2 agosto 2028 per quelli integrati nei prodotti dell'allegato I; fino ad allora il precetto integrativo non è, in tutto o in parte, applicabile, e con esso lo spazio operativo del primo e del quarto comma.

L'utilizzatore professionale. L'espressione non coincide con quella di deployer impiegata dal regolamento, le cui definizioni l'art. 11 dichiara applicabili al titolo II. La lettura più piana è che il legislatore abbia inteso riferirsi al deployer che usa il sistema nell'ambito di un'attività professionale; resta che, per lui, rileva la sola omissione intenzionale delle misure di sorveglianza umana, non quella colposa.

L'omissione della misura non basta: occorre che ne derivi un pericolo concreto per la vita, l'incolumità o la sicurezza dello Stato.

La responsabilità degli enti: l'art. 25-vicies

L'art. 15 inserisce nel d.lgs. n. 231/2001, dopo l'art. 25-undevicies, l'art. 25-vicies, rubricato «Reati commessi con l'uso di sistemi di intelligenza artificiale». Per il delitto dell'art. 437-bis c.p. si applica all'ente la sanzione pecuniaria da seicento a mille quote; per il delitto dell'art. 612-quater c.p. — l'illecita diffusione di contenuti generati o alterati con sistemi di IA,

introdotta dalla legge n. 132/2025 — da duecento a settecento quote. In entrambi i casi si applicano le sanzioni interdittive dell'art. 9, comma 2, lettere b), c), d) ed e): sospensione o revoca di autorizzazioni, licenze o concessioni; divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi; divieto di pubblicizzare beni o servizi. Resta esclusa l'interdizione dall'esercizio dell'attività.

Il sequestro dei contenuti online

L'art. 14 modifica la lettera e-bis) dell'art. 104, comma 1, delle disposizioni di attuazione del codice di procedura penale, relativa all'esecuzione del sequestro preventivo sui contenuti online mediante ordine ai prestatori di servizi di hosting, alle piattaforme, ai motori di ricerca e agli altri intermediari di rimuovere i contenuti o disabilitare l'accesso: le parole «del profilo personale» sono sostituite da «generati anche con sistemi di intelligenza artificiale». È l'attuazione del criterio della lettera a) del comma 5 dell'art. 24.

CHE COSA FARE, IN CONCRETO, SE SI È UN ENTE

Aggiornare la mappatura dei rischi-reato del modello di organizzazione e gestione per le due nuove fattispecie presupposto: individuare i processi in cui l'ente progetta, addestra, produce, immette sul mercato o utilizza professionalmente sistemi ad alto rischio, e quelli in cui produce o diffonde contenuti sintetici; definire protocolli che rendano documentata l'adozione delle misure di sicurezza e di sorveglianza umana; prevedere flussi informativi verso l'organismo di vigilanza. La stessa documentazione avrà una seconda funzione nel giudizio civile, dove le informazioni sulla supervisione umana figurano fra gli elementi di cui il giudice può ordinare l'esibizione.

XI · IL PROCESSO CIVILE

Il danno da IA: accesso alle prove, presunzione causale, azione diretta

Il capo II del titolo II attua il criterio della lettera d) del comma 5 dell’art. 24. È la parte del decreto con la platea più ampia: le sue regole non riguardano le Forze di polizia né i soli sistemi ad alto rischio, ma chiunque sia convenuto per un danno cagionato nell’utilizzo di un sistema di intelligenza artificiale.

L’ambito e il foro

L’art. 16 distingue due cerchi. Le regole sull’accesso alle prove dell’art. 17 si applicano a tutte le azioni di risarcimento del danno, contrattuale o extracontrattuale, cagionato nell’utilizzo di un sistema di IA (comma 1). La presunzione causale dell’art. 18 e la regola dell’art. 19 si applicano soltanto quando il danno deriva dalla violazione di uno o più obblighi del regolamento (comma 2). Restano ferme la responsabilità dell’art. 82 del regolamento (UE) 2016/679 e la normativa nazionale di recepimento della direttiva (UE) 2024/2853 sui prodotti difettosi (comma 3). Quando il danneggiato è una persona fisica che agisce per scopi estranei alla propria attività professionale, è altresì competente il giudice del luogo di residenza o domicilio (comma 4): un foro concorrente, non esclusivo.

L’accesso alle prove

Su istanza di chi allega di aver subito il danno, il giudice ordina all’altra parte o al terzo che ne dispone l’esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema, quando l’istante presenta fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche quanto al collegamento fra il risultato prodotto dal sistema e il danno (art. 17, comma 1). L’ordine è limitato a quanto necessario e proporzionato; il giudice tiene conto degli interessi di tutte le parti, in particolare della tutela dei segreti commerciali, e adotta le misure idonee a proteggerli, con applicazione dell’art. 121-ter del codice della proprietà industriale (commi 3 e 4).

GLI ELEMENTI DI PROVA DELL’ART. 17, COMMA 2

ELEMENTO	FONTE NEL REGOLAMENTO	CHI, DI REGOLA, LO DETIENE
Registri (log)	Art. 12	Il fornitore, che progetta la registrazione automatica; il deployer, che conserva i log generati sotto il proprio controllo (art. 26, par. 6).
Documentazione del sistema di gestione dei rischi	Art. 9	Il fornitore.
Informazioni pertinenti della documentazione tecnica	Art. 11	Il fornitore.
Parametri e modalità della supervisione umana	Art. 14	Il fornitore, che progetta le misure; il deployer, che le attua affidando la sorveglianza a persone competenti (art. 26, par. 2).

Due osservazioni. L’elenco è esemplificativo («rientrano»): l’ordine può avere a oggetto altri elementi pertinenti. E gli elementi elencati sono documenti che il regolamento prescrive per i sistemi ad alto rischio; per gli altri sistemi l’art. 17 resta applicabile, ma con oggetto necessariamente diverso.

Le conseguenze dell’inottemperanza sono graduate. Se la parte non adempie senza giustificato motivo, il giudice può desumerne argomenti di prova ai sensi dell’art. 116 c.p.c.; se l’inadempimento riguarda la documentazione del comma 2, il giudice, valutato ogni altro elemento, ritiene come ammessi i fatti allegati dall’istante (comma 5). Il terzo inadempiente è condannato a una pena pecuniaria da 1.500 a 10.000 euro (comma 6).

Nel giudizio civile il documento non esibito non è soltanto una lacuna: è un fatto che il giudice può ritenere ammesso.

La presunzione del nesso causale

Quando il danno deriva dalla violazione di uno o più obblighi del regolamento, il nesso di causalità fra la violazione e il danno è presunto, salvo prova contraria (art. 18). La presunzione riguarda il collegamento, non la violazione, che resta da provare a carico del danneggiato; ma l'accesso alle prove e la regola del «ritenere ammessi» i fatti allegati rendono quella prova sensibilmente meno ardua.

La conformità non esonera

Ferma la disciplina di recepimento della direttiva sui prodotti difettosi, la conformità del sistema agli obblighi del regolamento, anche se certificata secondo il capo III, sezione 5, non esclude di per sé la responsabilità del convenuto (art. 19). È la stessa logica che il fascicolo precedente ricostruiva per il Codice di buone pratiche: un percorso che agevola la dimostrazione, non una causa di esclusione della responsabilità.

L'azione diretta verso l'assicuratore

Chi intende agire può chiedere preventivamente al presunto responsabile se è assistito da un'assicurazione della responsabilità civile per quel danno; la richiesta non è condizione di procedibilità. Il destinatario comunica entro trenta giorni esistenza ed estremi del contratto e denominazione dell'impresa; l'omessa o incompleta comunicazione è valutabile ai sensi dell'art. 116 c.p.c. Il danneggiato ha azione diretta contro l'assicuratore nei limiti del massimale; gli sono opponibili le eccezioni contrattuali anteriori al sinistro; l'impresa che paga ha rivalsa verso l'assicurato nella misura in cui avrebbe potuto rifiutare o ridurre la prestazione; il responsabile è litisconsorte necessario; la prescrizione è la stessa dell'azione verso il responsabile (art. 20).

CHE COSA FARE, IN CONCRETO

Riesaminare i contratti di fornitura dei sistemi: le clausole di consegna documentale proposte nel n. 5 acquistano una seconda funzione, probatoria, perché il deployer convenuto dovrà poter esibire ciò che il fornitore detiene. Verificare le polizze di responsabilità civile quanto alla copertura dei danni da IA e alle eccezioni opponibili, e predisporre la procedura per rispondere entro trenta giorni alla richiesta preventiva. Organizzare la conservazione dei log e della documentazione in modo da poterli esibire selettivamente, con le cautele a tutela dei segreti commerciali che il giudice può disporre.

XII · GLI ADEMPIMENTI

Norme transitorie, atti attuativi, destinatari

Il titolo III chiude il decreto con due disposizioni. Il resto dell’attuazione è affidato a tre atti secondari e alle procedure interne delle amministrazioni.

Il regime transitorio

I sistemi di IA che all’entrata in vigore del decreto sono oggetto di rapporti contrattuali, in sviluppo o sperimentazione, o già in uso nell’attività di polizia, sono resi compatibili con le disposizioni del capo II del titolo I entro un anno da quella data (art. 21, comma 1): dunque entro il 30 settembre 2027. Il termine riguarda il capo II, non il capo III sui dati biometrici e sull’identificazione biometrica, che non beneficia di un analogo differimento. Per le disposizioni che dipendono dal regolamento valgono i termini di quest’ultimo (comma 2); l’art. 22 reca l’invarianza finanziaria.

GLI ATTI ATTUATIVI PREVISTI

ATTO	ADOZIONE	OGGETTO
d.P.C.M. (art. 5, c. 4)	Proposta AgID e ACN; concerto Interno; sentiti MEF e Garante.	Coordinamento con lo spazio di sperimentazione ex art. 57 del regolamento.
D.M. (art. 9, c. 5)	Interno, di concerto con Giustizia; sentiti Garante, AgID, ACN.	Requisiti tecnici, bias, banche dati, richiesta di autorizzazione e notifica per il tempo reale.
D.M. (art. 10, c. 12)	Ministro dell’interno, sentito il Garante.	Luoghi ed eventi, trattamento delle immagini, sicurezza, adempimenti del titolare.
Procedure interne (artt. 3, 6)	Ciascuna Forza di polizia.	Individuazione del personale addetto alla revisione umana qualificata; corsi di formazione.

LA MAPPA DEGLI ADEMPIMENTI

DESTINATARIO	CHE COSA LO RIGUARDA	NORME
Forze di polizia	Revisione umana documentata; sorveglianza; formazione; valutazioni d’impatto, log, notifica; adeguamento dei sistemi esistenti.	Artt. 3-10, 21
Autorità giudiziaria	Autorizzazioni, proroghe, convalide; nulla osta alla notifica al Garante.	Artt. 8-10; 359-ter c.p.p.
Università, enti di ricerca, imprese partner	Clausole necessarie negli accordi di collaborazione.	Art. 4
Gestori di luoghi ed eventi, enti locali	Installazione e manutenzione; comodato alla questura; ruoli nel trattamento.	Art. 10, cc. 4, 13
Fornitori e utilizzatori di sistemi ad alto rischio	Omissione di misure di sicurezza e di sorveglianza; alterazione.	Art. 437-bis c.p.
Enti ex d.lgs. n. 231/2001	Aggiornamento del modello per i reati degli artt. 437-bis e 612-quater c.p.	Art. 25-vicies
Chiunque impieghi un sistema di IA	Esibizione; presunzione causale; conformità; assicurazione (anche per le imprese assicuratrici: azione diretta e rivalsa).	Artt. 16-20

IL CRITERIO PRATICO DI ORIENTAMENTO

Il decreto parla a tre pubblici: alle Forze di polizia e all’autorità giudiziaria; a chi produce o usa professionalmente sistemi ad alto rischio, con un diritto penale legato al calendario del regolamento; a chiunque impieghi un sistema di IA, con regole processuali civili applicabili dal 30 settembre 2026. Il terzo è il più ampio, e il meno consapevole.

CONTRIBUTO

L'amministrazione aumentata

Intelligenza artificiale e capacità amministrativa nei piccoli comuni

LUCA FRESCURA

1. Il problema: intelligenza artificiale e piccoli comuni

Il presente contributo affronta il tema dell'intelligenza artificiale nella pubblica amministrazione assumendo come punto di osservazione i piccoli comuni¹, in particolare quelli caratterizzati da strutture organizzative ridotte, difficoltà di reclutamento e crescente complessità degli adempimenti amministrativi. Si tratta di una prospettiva particolarmente significativa, considerando che i comuni sotto i 5.000 abitanti rappresentano circa il 70% del totale.

Proprio in tali amministrazioni l'intelligenza artificiale può assumere una funzione peculiare, compensando la scarsità di personale. Al tempo stesso, l'introduzione di tali sistemi richiede competenze adeguate per selezionarli, verificarne l'affidabilità e controllarne gli output.

Il tema ha acquisito rilievo normativo con la legge 23 settembre 2025, n. 132, innestata nella cornice delineata dal Regolamento europeo sull'intelligenza artificiale. In particolare, l'art. 14 della legge citata, nel consentire l'impiego dell'IA nella pubblica amministrazione, ribadisce la responsabilità umana e la necessità di adeguate misure organizzative e formative.

La questione investe il principio di buon andamento di cui all'art. 97, secondo comma, Cost., e quello di adeguatezza di cui all'art. 118 Cost., poiché la disponibilità di risorse e competenze costituisce una condizione di effettività dell'azione amministrativa.

Emerge così il «paradosso della capacità»: i comuni che potrebbero beneficiare maggiormente dell'IA sono spesso quelli meno attrezzati per governarne l'impiego.

Il lavoro intende verificare se, e a quali condizioni, questo quadro possa tradursi in un rafforzamento della capacità amministrativa dei piccoli enti, piuttosto che in un ulteriore fattore di divario tra amministrazioni più e meno strutturate. In questa prospettiva, l'«amministrazione aumentata» indica un modello nel quale la tecnologia non sostituisce il funzionario, ma ne amplia le capacità operative e conoscitive.

2. Rischi e limiti giuridici dell'automazione amministrativa

La neutralità dei sistemi di IA non può essere presunta, soprattutto quando gli algoritmi sono applicati a un'attività amministrativa soggetta ai principi di imparzialità e non discriminazione. L'IA è infatti addestrata su dati prodotti o selezionati dall'uomo e può quindi riprodurre, o persino amplificare, pregiudizi già esistenti.

Lo mostra l'esperienza statunitense della polizia predittiva, introdotta per orientare l'attività di controllo delle forze dell'ordine. Un'inchiesta di The Markup ha evidenziato come PredPol raccomandasse più frequentemente pattugliamenti nei quartieri a prevalenza afroamericana o ispanica, con il rischio di riprodurre disuguaglianze già presenti nei dati e nelle prassi amministrative.²

Anche il contenzioso sulla mobilità dei docenti del 2016, pur riguardando forme di automazione amministrativa diverse dall'odierna IA generativa, ha evidenziato la necessità che il funzionamento dell'algoritmo sia conoscibile e la decisione sottoposta a controllo.³

Davanti a questa situazione è fondamentale richiamare l'art. 1 della l. 241/1990, il quale stabilisce che l'azione della PA debba rispettare i principi di economicità, efficacia, imparzialità, pubblicità e trasparenza, ai quali neppure l'impiego dell'IA può derogare.

A questi principi si è progressivamente affiancata una disciplina specifica dell'automazione amministrativa. Un primo punto di svolta è rappresentato dalla sentenza del Consiglio di Stato n. 2270 del 2019, che ha ricondotto l'automazione amministrativa alle esigenze di conoscibilità, comprensibilità, non esclusività della decisione automatizzata e non discriminazione. Questa impostazione è stata recepita dall'art. 30 del d.lgs. 36/2023 in materia di contratti pubblici e, più recentemente, dalla legge n. 132/2025, la quale prevede che l'intelligenza artificiale operi nella pubblica amministrazione in

funzione strumentale e di supporto, ferma restando in capo alla persona l'autonomia decisionale e la responsabilità del procedimento e del provvedimento.

Ne discende un dato rilevante per i piccoli comuni: l'utilizzo dell'IA presuppone comunque un funzionario in grado di comprenderne e valutarne criticamente l'output. La presenza dell'uomo nel procedimento rischia, infatti, di trasformarsi in una garanzia soltanto formale quando chi è chiamato a controllare la macchina non dispone delle competenze necessarie per farlo.

Nella stessa direzione si muove l'AI Act, che per i sistemi ad alto rischio prevede specifiche forme di sorveglianza umana e include tra essi alcuni sistemi utilizzati per l'accesso a servizi e prestazioni pubbliche essenziali.⁴ Se tali garanzie rafforzano la tutela del cittadino, esse possono al tempo stesso gravare maggiormente proprio sugli enti privi di uffici legali, informatici o di competenze specialistiche.

3. La fragilità dei piccoli comuni e il paradosso della capacità

I dati confermano la gravità del problema di partenza. Secondo l'Associazione Nazionale dei Comuni Italiani, tra il 2013 e il 2024 i dipendenti a tempo indeterminato dei piccoli comuni sono diminuiti di oltre 8.500 unità, mentre nell'82% delle sedi di segreteria comunale sotto i tremila abitanti manca un segretario titolare.⁵

È proprio questa fragilità organizzativa a far emergere il «paradosso della capacità»: i comuni che potrebbero beneficiare maggiormente dell'IA, per la scarsità di personale, sono spesso quelli con minori competenze interne per selezionare le soluzioni, valutarne l'affidabilità, controllarne gli output e governarne i rischi.

L'IA può attenuare alcune conseguenze della debolezza organizzativa, ma non sostituisce le politiche di reclutamento e formazione. Un ente privo di personale capace di vagliarne criticamente gli output rischia infatti di trasformare la propria fragilità in dipendenza tecnologica. A ciò si aggiunge il rischio dell'*automation bias*⁶, ossia la tendenza dell'operatore umano ad attribuire eccessivo affidamento al risultato prodotto dal sistema automatizzato. La formazione del personale diventa quindi parte della stessa capacità amministrativa necessaria per un utilizzo consapevole dell'IA.

4. L'amministrazione aumentata e la governance condivisa

Da questa prospettiva nasce l'idea di «amministrazione aumentata»: non un'amministrazione automatizzata o sostitutiva del lavoro umano, ma un modello nel quale la tecnologia amplia le capacità operative e conoscitive del personale esistente: ricerca normativa, sintesi documentale, predisposizione di bozze, gestione della conoscenza interna, supporto istruttorio, informazione ai cittadini.

Alcune esperienze confermano la praticabilità di tali impieghi: il progetto FAST Piccoli Comuni ha sperimentato l'uso dell'IA a supporto della redazione degli atti amministrativi, mentre il rapporto IFEL-AIPACT documenta percorsi come quello di ottantacinque comuni toscani.⁷ L'obiettivo non è sostituire il funzionario, ma consentirgli di concentrarsi sulle attività che richiedono valutazione e responsabilità.

Nei piccoli comuni, tuttavia, l'amministrazione aumentata difficilmente può essere costruita facendo affidamento sulle sole risorse del singolo ente, poiché ai limiti organizzativi si aggiungono i costi dei sistemi e la carenza di competenze tecniche.

Una possibile risposta risiede nelle forme di cooperazione sovracomunale, attraverso le quali condividere non soltanto i costi, ma soprattutto le competenze necessarie alla selezione, al controllo e alla gestione dei sistemi di IA. Unioni di comuni e altre forme associative potrebbero così divenire sedi comuni per il supporto tecnico, la formazione del personale e la valutazione delle soluzioni adottate.

La funzione amministrativa e la responsabilità della decisione resterebbero in capo al singolo ente, mentre la capacità tecnologica necessaria all'esercizio della funzione potrebbe essere organizzata a livello sovracomunale. In questa prospettiva, l'IA non conduce necessariamente a una centralizzazione delle funzioni, ma può favorire una nuova forma di cooperazione tra enti, capace di preservare la prossimità del comune e, al tempo stesso, di assicurare una scala organizzativa adeguata alla complessità tecnologica.

5. Conclusioni

L'IA può ampliare le capacità del personale dei piccoli comuni, ma il suo impiego richiede competenze adeguate a governarla. Il problema non è, dunque, soltanto adottare l'intelligenza artificiale, ma disporre della capacità amministrativa necessaria per

utilizzarla in modo consapevole. Il «paradosso della capacità» può essere superato attraverso modelli di governance sovracomunale capaci di condividere competenze e strumenti senza sottrarre al singolo ente la responsabilità della funzione esercitata. In questa prospettiva, l'amministrazione aumentata può diventare uno strumento di riequilibrio, anziché un ulteriore fattore di divario tra amministrazioni diversamente strutturate.

¹ Art. 1, c. 2, l. 6 ottobre 2017, n. 158; ISTAT, *Censimento e dinamica della popolazione. Anno 2024*, 2025.

² A. Sankin, D. Mehrotra, S. Mattu, A. Gilbertson, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, in *The Markup*, 2 dicembre 2021.

³ Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270; Consiglio di Stato, sez. VI, 13 dicembre 2019, nn. 8472, 8473 e 8474.

⁴ Artt. 6 e 14 e Allegato III, punto 5, lett. a), Reg. (UE) 2024/1689.

⁵ ANCI, *Il personale. Le proposte*, Stati generali dei piccoli Comuni, 2026, pp. 3 e 6.

⁶ R. Parasuraman, D.H. Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration*, in *Human Factors*, 2010, vol. 52, n. 3, pp. 381-410.

⁷ Fondazione IFEL, *Intelligenza artificiale nei Comuni italiani. Competenze, governance, territori*. La roadmap di IFEL nel progetto AIPACT, 2026.

Aggiornamenti al fascicolo n. 5

Il numero di settembre, chiuso il 25 agosto, aveva lasciato aperti tre profili, rinviandoli al presente numero. Se ne dà conto qui, distinguendo quelli che possono dirsi chiusi da quelli che restano aperti.

Profili chiusi

Decreti legislativi di adeguamento. Il decreto sull'utilizzo dei sistemi di IA nell'attività di polizia e sulla responsabilità civile e penale è il d.lgs. 9 settembre 2026, n. 160, pubblicato nella Gazzetta Ufficiale, Serie generale, n. 214 del 15 settembre 2026, e in vigore dal 30 settembre 2026. Le premesse confermano la deliberazione definitiva del Consiglio dei ministri del 4 agosto 2026, già indicata nel n. 5, e l'esame preliminare del 10 giugno 2026. Il decreto è commentato nei capitoli I-XII di questo numero.

Legge n. 132/2025: diritto d'autore. Le disposizioni in materia sono contenute negli artt. 25 e 26. L'art. 25, unico articolo del capo IV, modifica l'art. 1, primo comma, della legge n. 633/1941, riferendo la tutela alle opere dell'ingegno «umano», anche laddove create con l'ausilio di strumenti di intelligenza artificiale purché costituenti risultato del lavoro intellettuale dell'autore, e inserisce l'art. 70-septies, per il quale le riproduzioni e le estrazioni ai fini dell'estrazione di testo e di dati attraverso modelli e sistemi di IA, anche generativa, sono consentite in conformità agli artt. 70-ter e 70-quater. L'art. 26 reca, fra l'altro, il nuovo art. 612-quater c.p. sull'illecita diffusione di contenuti generati o alterati con sistemi di IA: la fattispecie che l'art. 25-vicies del d.lgs. n. 231/2001, introdotto dal d.lgs. n. 160/2026, include ora fra i reati presupposto della responsabilità degli enti (v. capitolo X). Il raccordo analitico di queste disposizioni con la direttiva (UE) 2019/790 e con il capitolo sul diritto d'autore del Codice di buone pratiche sarà oggetto di un numero dedicato.

Profili che restano aperti

Alla data di chiusura del presente fascicolo non si riportano gli estremi di pubblicazione del secondo decreto legislativo approvato il 4 agosto 2026, relativo alle autorità nazionali, ai poteri di vigilanza e alla formazione: se ne darà conto alla pubblicazione, anche per il raccordo con la mappa delle competenze tracciata nel capitolo XI del n. 5. Resta aperto, altresì, il numero e la composizione aggiornata dell'elenco dei firmatari del Codice di buone pratiche per i modelli di IA per finalità generali.

SEGNALAZIONE — IMPERFEZIONI TESTUALI DEL D.LGS. N. 160/2026

Nell'art. 2 del decreto, la lettera q) rinvia a una lettera s) inesistente, anziché alla lettera p), e le lettere p) e q) citano il «regolamento (UE) 1689/2024» anziché il regolamento (UE) 2024/1689. Ne è dato conto al capitolo II. Qualora intervenga un avviso di rettifica, se ne riferirà in questa rubrica.

APPARATO

Riferimenti normativi e fonti

DIRITTO DELL'UNIONE EUROPEA

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in GUUE L, 2024/1689 del 12 luglio 2024. Disposizioni richiamate: artt. 3 (punti 1, 4, 37, 38, 45, 46), 4, 5 (par. 1, lett. e), g), h), e parr. 2, 4 e 5), 6, 9, 11, 12, 14, 26 (parr. 2, 6 e 10), 27, 57, 59, 96 e 99; capo III, sezione 5; allegati I, II e III.
- Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, recante modifica del regolamento (UE) 2024/1689, in GUUE del 24 luglio 2026, in vigore dal 27 luglio 2026.
- Regolamento (UE) 2016/679 del 27 aprile 2016, sulla protezione dei dati personali; in particolare artt. 10 e 82.
- Direttiva (UE) 2016/680 del 27 aprile 2016, sulla protezione dei dati personali trattati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
- Direttiva (UE) 2024/2853 del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi.
- Direttiva (UE) 2019/790 del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale.

DIRITTO INTERNO

- Decreto legislativo 9 settembre 2026, n. 160, «Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, 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», in Gazzetta Ufficiale, Serie generale, n. 214 del 15 settembre 2026, con le relative note.
- Legge 23 settembre 2025, n. 132, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», in Gazzetta Ufficiale n. 223 del 25 settembre 2025; in particolare artt. 2, 3, 14, 20, 24, 25 e 26.
- Costituzione, artt. 73, terzo comma, 76 e 87; disposizioni sulla legge in generale, art. 10.
- Codice penale, artt. 437, 437-bis e 612-quater; codice di procedura penale, artt. 57, 359-bis e 359-ter; norme di attuazione, di coordinamento e transitorie del codice di procedura penale (d.lgs. 28 luglio 1989, n. 271), artt. 104 e 226; codice di procedura civile, art. 116.
- Decreto legislativo 8 giugno 2001, n. 231, artt. 9, 10 e 25-vicies; decreto legislativo 18 maggio 2018, n. 51, artt. 8, 23 e 24; d.P.R. 15 gennaio 2018, n. 15, art. 10; decreto legislativo 10 febbraio 2005, n. 30, art. 121-ter; d.P.R. 11 luglio 1980, n. 382, art. 64.
- Legge 1° aprile 1981, n. 121, art. 16; decreto-legge 13 maggio 1991, n. 152, convertito dalla legge 12 luglio 1991, n. 203, art. 12; legge 23 agosto 1988, n. 400, art. 17; legge 24 dicembre 2012, n. 234; legge 22 aprile 1941, n. 633, artt. 1, 70-ter, 70-quater e 70-septies.

FONTI RICHIAMATE NEL CONTRIBUTO

- Le fonti del contributo di Luca Frescura sono indicate nelle note che lo corredano.

NUMERI PRECEDENTI DELLA RIVISTA RICHIAMATI

- N. 1, maggio 2026, *Il Digital Omnibus*; n. 2, giugno 2026, *L'amministrazione algoritmica*; n. 3, luglio 2026, *La trasparenza algoritmica*; n. 4, agosto 2026, *L'AI Act riscritto*; n. 5, settembre 2026, *L'AI Act applicato*.