RELAZIONE ILLUSTRATIVA

Il presente decreto è adottato ai sensi dell'articolo 24, comma 1, comma 2, lett. h), comma 3 e comma 5 della legge 23 settembre 2025, n. 132 ed è finalizzato all'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689, del Parlamento europeo e del Consiglio, del 13 giugno 2024 ("Regolamento IA" o "AI Act"), attraverso, in particolare, l'introduzione di una disciplina per l'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia, nonché l'introduzione di disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti di sistemi di intelligenza artificiale e di disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi.

Il decreto legislativo si compone di **22** articoli suddivisi in due titoli.

Il **titolo I**, dedicato all'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia, dà attuazione alla legge 23 settembre 2025, n. 132, in particolare all'articolo 24, comma 2, lettera *h*), che delega il Governo a prevedere un'apposita disciplina in materia di utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia. Si colloca nel quadro di adeguamento nazionale alla normativa europea sull'intelligenza artificiale, di cui al regolamento (UE) 2024/1689 (da qui, anche *AI Act*), con specifico riferimento all'impiego di sistemi di IA nelle attività e per le finalità di polizia, e persegue l'obiettivo di coniugare l'efficacia dell'azione di prevenzione e contrasto dei reati con la piena tutela dei diritti fondamentali e della protezione dei dati personali.

Nel suo complesso, si realizza una prima disciplina organica e settoriale dell'impiego di sistemi di intelligenza artificiale nelle attività di polizia, in attuazione della legge IA e in armonia con *l'AI Act*, ponendo particolare attenzione al bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali, alla regolazione dei casi operativi più sensibili, quali i trattamenti di dati biometrici, attraverso rigorose garanzie procedurali, tecniche e di controllo, alla promozione di un uso responsabile e consapevole dell'IA, anche mediante la formazione del personale di polizia e la partecipazione a "spazi di sperimentazione normativa", nonché al coordinamento con la normativa, di matrice euro-unitaria, in materia di protezione dei dati personali, con particolare riferimento al trattamento dei dati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

Il **titolo II**, relativo alle **disposizioni penali**, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiali e alle **disposizioni processuali civili** in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi, dà attuazione alle deleghe di cui all'articolo 24, commi 3, 4 e 5, della legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale". Il provvedimento si inserisce nel quadro normativo definito dal regolamento (UE) 2024/1689 (AI Act), che ha introdotto un sistema armonizzato di regole sull'intelligenza artificiale fondato su una classificazione dei sistemi in base al

livello di rischio e su un articolato corredo di obblighi a carico dei diversi operatori della catena del valore.

Coerentemente con la ratio antropocentrica che attraversa l'intera legge n. 132 del 2025 — la quale impone di calare l'uso dei sistemi di intelligenza artificiale entro un quadro di garanzie incentrato sulla tutela della persona — il decreto interviene su due versanti che, pur tecnicamente distinti, condividono la medesima finalità di protezione dell'individuo rispetto agli usi e agli effetti dei sistemi di intelligenza artificiale: la tutela penale contro la realizzazione e l'impiego illeciti di tali sistemi, da un lato, e la tutela civile risarcitoria del danneggiato, dall'altro.

Il **titolo II** si articola in due capi. Il **Capo I** reca disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti di sistemi di intelligenza artificiale, in attuazione dell'articolo 24, comma 3, della medesima legge nonché disposizioni in materia di utilizzo dell'intelligenza artificiale nel corso di indagini penali. Il **Capo II** introduce strumenti processuali civili a tutela del danneggiato per i danni cagionati dall'utilizzo di sistemi di intelligenza artificiale, in attuazione dell'articolo 24, comma 5, lettera d), della legge n. 132 del 2025.

Titolo I - Utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia

Il titolo I si articola in quattro capi, per un totale di undici articoli.

CAPO I – Disposizioni generali (articoli 1 e 2)

Il Capo I è il "quadro di riferimento" generale del decreto, definendone perimetro, finalità e definizioni, e assicurando il coordinamento con l'*AI Act* europeo, la legge n. 132 del 2025 e la normativa sulla protezione dei dati personali.

Articolo 1 (Oggetto e finalità)

L'articolo 1 individua l'oggetto del decreto e ne definisce le finalità generali.

La disposizione, al comma 1, chiarisce che il decreto disciplina l'utilizzo di sistemi di intelligenza artificiale da parte degli organi, uffici e comandi delle Forze di polizia, nell'esercizio delle attività e per le finalità di polizia, in attuazione dell'articolo 24, comma 2, lettera *h*), della legge n. 132 del 2025 e in coerenza con il regolamento (UE) 2024/1689.

Viene espressamente richiamato, al comma 2, il rispetto dei diritti e delle libertà fondamentali garantiti dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione europea dei diritti dell'uomo, nonché dei principi di proporzionalità, non discriminazione, sorveglianza umana effettiva e trasparenza già previsti dalla legge n. 132 del 2025.

Il comma 3 del primo articolo precisa, inoltre, che il decreto non introduce nuovi obblighi rispetto a quelli previsti dall'*AI Act* per i sistemi e i modelli di

IA utilizzati nelle attività e finalità di polizia, ma ne specifica e coordina l'applicazione nell'ordinamento interno, fatte salve le esclusioni espressamente previste dal regolamento medesimo

Articolo 2 (Definizioni)

L'articolo 2 reca il quadro definitorio necessario per l'applicazione del decreto, assicurando coerenza con la terminologia dell'*AI Act*, della legge nazionale n. 132 del 2025 e della normativa in materia di protezione dei dati personali.

Il comma 2 dell'articolo stabilisce che, per quanto non espressamente definito, trovano applicazione le definizioni contenute nella legge n. 132/2025 e nel Regolamento (UE) 2024/1689, assicurando così un rinvio dinamico al quadro europeo di riferimento.

CAPO II - Disposizioni in materia di ricerca, sviluppo, addestramento, formazione, sperimentazione e utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia (articoli 3–6)

Il Capo II rappresenta il motore "organizzativofunzionale" del decreto, disciplinando l'intero ciclo di vita dei sistemi di IA (ricerca, sviluppo, sperimentazione, uso), le collaborazioni esterne, le *sandbox* (ossia gli "spazi di sperimentazione normativa") e la formazione degli operatori di polizia.

Articolo 3 (Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività di polizia)

L'articolo 3 delinea il quadro generale di principi e regole applicabili a tutte le fasi del ciclo di vita dei sistemi di IA utilizzati dalle Forze di polizia: ricerca, sperimentazione, sviluppo, addestramento, adozione, applicazione, convalida e utilizzo operativo.

In tal modo, l'articolo racchiude la "filosofia generale" dell'uso dell'IA da parte delle Forze di polizia: centralità dell'uomo, logica "*riskbased*", ruolo sussidiario dell'IA, valorizzazione della responsabilità degli operatori, conformità alla normativa sull'IA e sulla *privacy*.

Il comma 1 afferma che l'impiego dell'IA nelle attività di polizia deve essere improntato a un approccio antropocentrico, proporzionato e fondato sulla valutazione del rischio, in coerenza con l'*AI Act*, tenendo conto della classificazione dei sistemi (con particolare riguardo a quelli ad alto rischio) e delle diverse categorie di interessati.

Il comma 2 è dedicato alle attività cd. di "pre-impiego", ossia di ricerca, sperimentazione, sviluppo e addestramento dei sistemi di IA, al fine di orientare le stesse al perseguimento della funzionalità e dell'affidabilità operativa dei sistemi e dei modelli di IA destinati a essere utilizzati dalle Forze di polizia, nella prospettiva di migliorare l'apporto tecnologico dell'intelligenza artificiale alle valutazioni e alle decisioni umane nella relativa attività.

Il comma 3 qualifica gli *output* dei sistemi di IA come strumenti di supporto all'attività e alle decisioni umane, che restano nella responsabilità degli operatori di polizia.

Al comma 4 è previsto formalmente, per l'utilizzo dei sistemi e dei modelli di IA, l'obbligo di "revisione umana qualificata" dei risultati delle elaborazioni automatizzate, prima che possano incidere sulla sfera giuridica delle persone interessate, con tracciabilità documentata e individuazione del personale competente.

Per i sistemi di IA "ad alto rischio", il comma 5 richiede che la sorveglianza umana sia effettiva, in linea con l'articolo 14 del regolamento UE sull'IA, e che il personale di polizia sia adeguatamente formato per minimizzare i rischi per la salute, la sicurezza e i diritti fondamentali.

Il comma 6 riconduce il trattamento di dati personali, comprese le categorie particolari, i dati operativi sensibili e i dati relativi a condanne penali e reati, nell'alveo del decreto legislativo n. 51 del 2018, attuativo della direttiva UE n. 680 del 2016, fatte salve le specifiche disposizioni del regolamento UE sui sistemi ad alto rischio e quelle del Capo III del presente decreto.

Il comma 7, infine, ribadisce che il decreto delegato non introduce nuovi od ulteriori obblighi rispetto a quelli previsti dall'*AI Act*.

Articolo 4 (Collaborazione nell'ambito della ricerca e sperimentazione scientifica finalizzata alla realizzazione di sistemi e modelli di intelligenza artificiale per l'attività di polizia)

L'articolo 4, comma 1, disciplina le forme di collaborazione che le Forze di polizia possono instaurare, nell'ambito di progetti di ricerca, sperimentazione, sviluppo, addestramento e convalida di sistemi, modelli o dispositivi di IA, con università, enti di ricerca e altri soggetti pubblici o privati, inclusi soggetti *in house* o a totale partecipazione pubblica, fermo restando il rispetto delle regole dell'Unione europea in materia di concorrenza e aiuti di Stato.

Per questa via, l'articolo apre all'innovazione tramite partenariati, ma pone dei limiti chiari su dati operativi sensibili e proprietà dei modelli, evitando esternalizzazioni incontrollate di *asset* critici.

Il comma 2, con specifico riguardo al trattamento dei dati personali, prevede che siano escluse la condivisione e la messa a disposizione di dati operativi sensibili a favore dei *partner*, e che sia vietato che gli stessi acquisiscano o utilizzino, anche indirettamente e per finalità commerciali o diverse da quelle di polizia, sistemi, risorse *hardware* o *software*, modelli o dispositivi addestrati con dati operativi sensibili.

Il comma 3 impone, inoltre, che gli accordi di collaborazione disciplinino espressamente la titolarità dei diritti di proprietà intellettuale e industriale sui risultati, sui modelli, sui dati di addestramento e sui software, nel rispetto del codice della proprietà industriale e della normativa di settore, garantendo in ogni caso alle Forze di polizia la titolarità dei modelli addestrati su dati operativi sensibili.

Articolo 5 (Sviluppo, realizzazione e prova di determinati sistemi di IA per finalità di polizia nello spazio di sperimentazione normativa)

L'articolo costituisce la base giuridica, ai sensi dell'articolo 59, paragrafo 2, dell'*AI Act* e del decreto legislativo n. 51 del 2018, per il trattamento di dati personali – incluse le categorie particolari e i dati relativi a reati – da parte delle Forze di polizia all'interno degli "spazi di sperimentazione normativa" (2*regulatory sandboxes* ") in materia di intelligenza artificiale.

La partecipazione delle Forze di polizia ai suddetti spazi è finalizzata, a mente del comma 2, allo sviluppo, alla realizzazione e alla prova di sistemi di IA, in particolare ad alto rischio, destinati alle attività e finalità di polizia, nel rispetto dei diritti fondamentali e della protezione dei dati personali, nonché delle condizioni previste dall'articolo 59, paragrafo 1, dello stesso regolamento UE sull'IA.

Il comma 3 prevede il raccordo con le Autorità nazionali per l'IA (AGID e ACN), ferma restando la titolarità e la responsabilità esclusiva delle Forze di polizia per il trattamento dei dati personali, ivi compresi quelli operativi sensibili.

Il comma 4 prevede che con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'Interno, sono definite le modalità di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e il trattamento di dati personali – incluse le categorie particolari e i dati relativi a reati – da parte delle Forze di polizia all'interno degli "spazi di sperimentazione normativa".

Articolo 6 (Formazione del personale di polizia)

L'articolo 6 introduce specifiche previsioni in materia di formazione del personale delle Forze di polizia, da realizzarsi presso gli istituti di istruzione e formazione competenti, entro il limite delle risorse disponibili a legislazione vigente.

Il comma 2 della disposizione in esame individua i risultati formativi minimi che devono essere assicurati, tra i quali:

- la comprensione dei principi di funzionamento, delle potenzialità e dei limiti dei sistemi di IA;
- la conoscenza dei possibili errori e bias, con particolare riguardo ai sistemi di riconoscimento biometrico e di analisi predittiva;
- la capacità di interpretazione critica degli output dei sistemi di IA e la consapevolezza del ruolo centrale della sorveglianza umana;
- la conoscenza delle implicazioni giuridiche, etiche e di responsabilità derivanti dall'uso dei sistemi di IA, con riferimento all'*AI Act*, alla legge n. 132 del 2025 e al decreto legislativo n. 51 del 2018;
- la consapevolezza dei rischi di cybersicurezza connessi all'impiego di tali sistemi, in linea con le indicazioni di ACN.

Per i sistemi di IA classificati "ad alto rischio" ai sensi del regolamento UE n. 1689 del 2024, il comma 3 prevede che taluni risultati formativi, in particolare

quelli relativi ai bias, all'interpretazione degli output e alla cybersicurezza, siano assicurati nell'ambito di corsi specificamente dedicati a tali sistemi.

CAPO III - Sistemi di intelligenza artificiale utilizzati nell'attività di polizia per l'etichettatura, il filtraggio e la categorizzazione di dati biometrici, per l'identificazione biometrica remota in tempo reale per finalità di prevenzione o di protezione e per il riconoscimento facciale a posteriori a fini di contrasto dei reati (articoli 7-10)

Il Capo III contiene il nucleo più operativo e sensibile del decreto, con la disciplina relativa ai sistemi di IA per la categorizzazione, l'etichettatura e il filtraggio di dati biometrici, l'identificazione biometrica remota in tempo reale in luoghi pubblici per finalità di polizia e il riconoscimento facciale a posteriori, integrato con componenti di IA nei sistemi di videosorveglianza, per il contrasto dei reati in luoghi o in occasione di eventi particolari, ove sussistono esigenze di ordine e sicurezza pubblica.

Articolo 7 (Etichettatura, filtraggio e categorizzazione di dati biometrici nell'attività di polizia)

L'articolo 7 disciplina l'utilizzo di sistemi di IA per l'etichettatura, il filtraggio e la categorizzazione di set di dati biometrici acquisiti lecitamente, ai sensi dell'articolo 5, paragrafo 1, lettera *g*), ultimo periodo, del regolamento UE n. 1689 del 2024, per finalità di polizia.

La disposizione, di natura ricognitiva delle attività di categorizzazione biometrica ammesse a fini di contrasto dal regolamento sull'IA fuori della pratica vietata di cui alla lett. *g*) sopra indicata, consente (al comma 1, lett. *a-d*)) tali "usi tecnici" esclusivamente quando:

- non sono finalizzati a inferire o dedurre le caratteristiche vietate dall'articolo 5, paragrafo 1, lettera g), primo periodo, dell'*AI Act* (quali, ad esempio, opinioni politiche, convinzioni religiose o filosofiche, orientamento sessuale);
- sono funzionali alla comparazione o alla ricerca, ovvero ad altre attività conformi alla normativa vigente, e sono effettuati unicamente per finalità di polizia;
- non costituiscono l'unico fondamento di decisioni che producano effetti giuridici negativi sulle persone interessate;
- il titolare del trattamento adotta misure idonee a prevenire il reimpiego dei dati e dei risultati per finalità incompatibili.

Il comma 2 prevede che il trattamento dei dati personali con i sistemi di cui al presente articolo è effettuato tenendo conto della classificazione dei sistemi di IA ai sensi dell'*AI Act*, avuto riguardo anche agli orientamenti della Commissione europea sull'attuazione pratica dello stesso regolamento europeo, e nel rispetto del decreto legislativo n. 51 del 2018.

Articolo 8 (Sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale per finalità di prevenzione, nonché di ricerca delle persone scomparse e delle vittime di specifici reati)

L'articolo costituisce uno degli elementi caratterizzanti il presente decreto, regolando in via innovativa, in linea con quanto ammesso dall'art. 5 del ripetuto regolamento UE n. 1689/2024, l'uso eccezionale di sistemi di IA per l'identificazione biometrica remota in tempo reale di persone fisiche in luoghi pubblici o aperti al pubblico, da parte delle Forze di polizia.

L'*incipit* del comma 1 mantiene fermo quanto previsto dal "nuovo" articolo 359-*ter* del codice di procedura penale, effettuando così un collegamento e un coordinamento inter-provvedimentale, ripetuto anche nell'art. 9 del presente decreto, tra l'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale per finalità di prevenzione di gravi minacce e di protezione (ricerca di persone scomparse e di vittime di specifici reati), a norma dell'art. 5, par. 2, lett. *h*), punti *i*) e *ii*), disciplinato dal presente articolo, e l'impiego dei medesimi sistemi biometrici nelle indagini preliminari per le finalità di cui al medesimo art. 5, par. 2, lett. *h*), punto *iii*), regolato nell'ambito della distinta delega prevista dallo stesso art. 24, commi 3 e 5, lett. *e*), della legge nazionale sull'intelligenza artificiale, la n. 132 del 2025.

Ciò premesso, l'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale, a mente dello stesso comma 1 della norma in commento, è ammesso esclusivamente per:

- la prevenzione di specifiche e gravi minacce gravi, ai sensi dell'articolo 5, paragrafo 1, lettera h), punto ii), dell'*AI Act*, relative ad un attacco terroristico ovvero alla vita o all'incolumità delle persone;
- la ricerca di persone scomparse o di vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale, ai sensi dell'articolo 5, paragrafo 1, lettera h), punto i), dell'*AI Act*.

L'impiego dei sistemi in parola, ai sensi del comma 2, deve essere limitato alla conferma dell'identità di persone specificamente interessate ovvero alla ricerca mirata e alla localizzazione, anche dinamica, di persone specificamente individuate o individuabili in relazione alla minaccia o alla ricerca in corso.

Il comma 3 prevede che il confronto biometrico può avvenire esclusivamente con una banca dati di riferimento adeguata allo scopo, alimentata da dati biometrici e informazioni identificative delle persone interessate, derivanti da banche dati già in uso alle Forze di polizia o da immagini, filmati e altri elementi biometrici acquisiti lecitamente nel corso dell'attività di polizia. Lo stesso comma pone il divieto espresso, in coerenza con le pratiche vietate dal Regolamento sull'IA, di utilizzare banche dati biometriche create tramite *scraping* non mirato o in violazione della normativa in materia di protezione dei dati personali.

L'utilizzo dei sistemi è subordinato a una procedura articolata, scandita dai commi 4, 5, 6 e 7:

- richiesta motivata del Questore, dei Comandanti provinciali dell'Arma dei carabinieri o della Guardia di finanza, o dei Responsabili di specifici servizi centrali, al Procuratore della Repubblica presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione o di ricerca;
- autorizzazione preventiva dell'Autorità giudiziaria, mediante decreto motivato che elichi, finalità, durata (non superiore a quindici giorni,

prorogabile per periodi di pari durata), area interessata e persone oggetto di ricerca.

In casi di urgenza, caratterizzati dal rischio di un grave e irreparabile pregiudizio, è prevista la possibilità di attivazione immediata dei sistemi su iniziativa delle Forze di polizia, previa comunicazione anche in forma orale al Procuratore della Repubblica e richiesta di autorizzazione da presentare senza ritardo e comunque entro ventiquattro ore dall'attivazione dei sistemi di IA per l'identificazione biometrica remota in tempo reale. L'Autorità giudiziaria provvede sulla richiesta entro le successive ventiquattro ore.

Ai sensi del comma 8, se non sono osservate le condizioni e i termini previsti dai citati commi da 4 a 7 o in mancanza di autorizzazione l'uso del sistema di IA per l'identificazione biometrica in tempo reale deve cessare, con obbligo di cancellazione dei dati, dei risultati e degli output, e con inutilizzabilità dei risultati acquisiti in violazione delle condizioni previste.

Il comma 9 dispone l'applicazione analogica dell'art. 226, comma 5, del decreto legislativo n. 271 del 1989 (disposizioni attuative del codice di procedura penale), per regolare lo speciale regime di utilizzabilità, in un procedimento penale, degli elementi acquisiti durante le attività preventive e mediante l'uso dei sistemi di IA biometrici di cui al presente articolo.

Articolo 9 (Valutazione d'impatto sui diritti fondamentali, conservazione delle registrazioni e notifica dell'utilizzo dei sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale)

L'articolo introduce ulteriori, necessarie garanzie procedurali e tecniche per l'utilizzo dei sistemi di IA di cui all'articolo 8 del presente decreto e all'articolo 359 *ter* del codice di procedura penale.

In particolare, il titolare del trattamento è tenuto a:

- effettuare, prima dell'uso dei sistemi biometrici in discorso, una valutazione di impatto sui diritti fondamentali, ai sensi dell'articolo 27 dell'*AI Act* (comma 1);
- registrare ogni utilizzo in file di log non modificabili, contenenti almeno le informazioni previste dall'articolo 12, paragrafo 3, dell'*AI Act*, da conservare per cinque anni e accessibili solo alle autorità competenti per la verifica della liceità dei trattamenti, per i controlli interni e per i procedimenti penali (comma 2);
- rispettare, in ogni caso, i termini di conservazione dei dati personali previsti, per le finalità di polizia, dall'articolo 10 del decreto del Presidente della Repubblica n. 15 del 2018 (comma 3).

A mente del comma 4, che richiama uno specifico obbligo imposto dall'art. 5, par. 4, del regolamento UE sull'IA, dopo l'utilizzo il titolare deve notificare l'attivazione dei sistemi di IA al Garante per la protezione dei dati personali. La notifica, che non può contenere dati operativi sensibili, è subordinata al nulla osta dell'autorità giudiziaria, la quale può differirla per un periodo massimo di tre mesi, rinnovabile una sola volta, per specifiche esigenze di segretezza; sono previste modalità di notifica periodica o cumulativa per più attivazioni omogenee.

Il comma 5 stabilisce che con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia e sentiti il Garante e le Autorità nazionali per l'IA, dovranno essere definiti, coerentemente con le norme del regolamento IA, i requisiti tecnici minimi di affidabilità e accuratezza dei sistemi di IA per l'identificazione biometrica in tempo reale, le modalità di monitoraggio delle prestazioni e dei bias dei medesimi sistemi, le misure di sicurezza, il contenuto informativo minimo delle richieste di autorizzazione e delle notifiche, nonché gli ulteriori adempimenti richiesti dall'*AI Act*.

Articolo 10 (Disposizioni in materia di sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall'intelligenza artificiale, per il contrasto dei reati)

L'articolo 10, comma 1, disciplina l'integrazione, ove ricorrano esigenze di ordine e sicurezza pubblica, nei sistemi di videosorveglianza la cui installazione sia già consentita da specifiche disposizioni di legge, di componenti di IA che consentano l'attivazione successiva di tecnologie di riconoscimento facciale, in modo da non configurare un'ipotesi di identificazione biometrica remota in tempo reale ai sensi dell'art. 5, par. 2, lett. *h*), dell'*AI Act*.

Sotto questo profilo, quindi, la disposizione in commento distingue nettamente l'uso "a posteriori" del riconoscimento facciale da quello in tempo reale, imponendo limiti temporali, di finalità e di responsabilità, nonché prevedendo una forte tracciabilità dei trattamenti, in linea con *l'AI Act* e, soprattutto, con la direttiva UE n. 680 del 2016, recepita nel nostro ordinamento dal d.lgs. n. 51 del 2018.

Il comma 2 stabilisce che l'utilizzo di tali tecnologie è ammesso, ai sensi dell'articolo 26, paragrafo 10, primo comma, dello stesso atto unionale, esclusivamente dopo la commissione di un reato, anche tentato, e al solo fine di identificare persone già indiziate sulla base di documentazione video-fotografica e di ulteriori elementi oggettivi e verificabili, sotto la responsabilità diretta ed esclusiva di un ufficiale di pubblica sicurezza designato dal Questore per la gestione dell'ordine e la sicurezza pubblica, ovvero, al di fuori della predetta ipotesi, di un ufficiale di polizia giudiziaria della Forza di polizia che procede in relazione al fatto di reato.

In contesti caratterizzati da particolari esigenze di ordine e sicurezza pubblica, il comma 3 prevede che l'installazione di tali sistemi può comportare il trattamento automatizzato dei dati biometrici delle persone che accedono ai luoghi o agli eventi, con memorizzazione locale in una base dati di riferimento, unitamente, senza far ricorso ad applicazioni biometriche di IA, ai corrispondenti dati anagrafici e, ove previsto, dell'identificativo del posto assegnato (ad esempio, per eventi con posti numerati). In caso di reato, l'attivazione delle tecnologie di riconoscimento facciale comporta il confronto biometrico a posteriori tra i dati delle persone da identificare (già indiziate) e quelli biometrici e anagrafici (e, se disponibili, ubicativi) presenti nella base dati di riferimento.

I commi da 4 a 8 si concentrano in particolare sul trattamento dei dati personali: il Dipartimento della pubblica sicurezza del Ministero dell'Interno è individuato quale titolare del trattamento, cui compete una valutazione di impatto e una consultazione preventiva del Garante ai sensi degli articoli 23 e

24 del decreto legislativo n. 51 del 2018, con possibilità di una valutazione unica valida per tutti i sistemi analoghi.

Le disposizioni richiamate stabiliscono che:

- i dati personali contenuti nella base dati di riferimento siano conservati per un periodo massimo di sette giorni dalla raccolta e cancellati automaticamente decorso tale termine;
- i log relativi agli accessi e alle operazioni effettuate sui sistemi siano conservati per cinque anni, non modificabili, e accessibili per le verifiche di liceità, per i controlli interni e per i procedimenti penali;
- restino in ogni caso fermi i termini di conservazione dei dati per finalità di polizia previsti dal decreto del Presidente della Repubblica n. 15 del 2018.

Il comma 9 pone il divieto, ripreso dall'analogo disposto dell'articolo 26, par.10, terzo comma, secondo periodo, del regolamento UE sull'IA, di basare decisioni che producano effetti giuridici negativi sulla persona unicamente sui risultati del riconoscimento facciale, mentre il comma 10 vieta di utilizzare sistemi di IA per finalità di identificazione biometrica generalizzata, non mirata e priva di collegamento con uno specifico reato o procedimento penale.

Il comma 11 prevede che con decreto del Ministro dell'interno, sentito il Garante, siano definite le modalità di trattamento e di memorizzazione dei dati biometrici nella base dati di riferimento, le misure tecniche e organizzative di sicurezza e gli ulteriori adempimenti in conformità all'*AI Act*.

All'installazione e alla manutenzione dei sistemi potranno provvedere, senza oneri per la finanza pubblica, i gestori dei luoghi o gli organizzatori o promotori degli eventi, ovvero chi ha la disponibilità delle strutture ove tali eventi si svolgono, con concessione in comodato gratuito delle apparecchiature alla Questura, che ne acquisisce la completa ed esclusiva disponibilità (comma 12).

Il comma 13 sigilla l'invarianza finanziaria complessiva della disposizione in commento.

Titolo II - Disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiali e disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi

Il titolo II si articola in due capi.

Il **capo I** attua la delega contenuta nell'art. 24, comma 3, della legge 23 settembre 2025, n. 132, secondo i principi e criteri direttivi enunciati al comma 5: introduzione di autonome fattispecie di reato incentrate sull'omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale (lett. b); regolazione dell'uso di tali sistemi nelle indagini preliminari (lett. e); strumenti, anche cautelari, di rimozione di contenuti illecitamente generati (lett. a, per il profilo del sequestro preventivo); disposizioni di coordinamento (lett. f).

Questo capo del decreto legislativo interviene per presidiare con la sanzione penale l'effettività delle prescrizioni regolamentari nei segmenti che mettono in gioco beni di rango primario: vita, incolumità pubblica e individuale,

sicurezza dello Stato. La ratio è coerente con la dimensione antropocentrica della legge delega (art. 1): la disciplina penale colpisce non il sistema, ma l'omissione umana nelle fasi del suo ciclo di vita.

Il **capo II** dà attuazione alla delega contenuta nell'articolo 24, commi 3 e 5, lettera d), della legge 23 settembre 2025, n. 132, che ha conferito al Governo il compito di adottare uno o più decreti legislativi recanti, nei casi di responsabilità civile per danni cagionati nell'utilizzo di sistemi di intelligenza artificiale, strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689.

L'intervento si colloca in un contesto eurounitario profondamente mutato rispetto al momento di presentazione, da parte della Commissione europea, della proposta di direttiva sulla responsabilità civile da intelligenza artificiale (COM(2022) 496). La Commissione, nel programma di lavoro per il 2025, ne ha infatti annunciato il ritiro, in coerenza con l'obiettivo di semplificazione del quadro normativo digitale. Resta nondimeno fermo il rilievo della direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi, che incide direttamente sulla disciplina del software e dei sistemi di intelligenza artificiale qualificabili come prodotti, e che dovrà essere recepita nell'ordinamento nazionale entro il 9 dicembre 2026.

In tale cornice, il capo II persegue tre finalità fondamentali:

a) garantire al danneggiato strumenti effettivi di accesso alla prova, in considerazione dell'opacità tecnologica che caratterizza i sistemi di intelligenza artificiale e della tipica asimmetria informativa tra utilizzatore e fornitore;

b) alleggerire l'onere probatorio sul nesso di causalità, attraverso una presunzione modulata in funzione della classificazione di rischio del sistema operata dal regolamento (UE) 2024/1689;

c) rafforzare la tutela del danneggiato persona fisica, mediante la previsione di un foro speciale del consumatore e di un'azione diretta nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile.

L'intervento è costruito secondo una logica di complementarità, e non di sostituzione, rispetto agli statuti speciali di responsabilità già operanti nell'ordinamento. Sono fatte espressamente salve le disposizioni dell'articolo 82 del regolamento (UE) 2016/679 e la normativa nazionale di recepimento della direttiva (UE) 2024/2853, in tal modo evitando ogni effetto di restrizione delle tutele esistenti negli ambiti specificamente regolati dal diritto eurounitario.

Articolo 11 (Definizioni)

L'articolo 11 opera un rinvio integrale alle definizioni contenute nell'articolo 3 del regolamento (UE) 2024/1689. La scelta del rinvio dinamico evita duplicazioni definitorie e garantisce piena uniformità terminologica con il quadro eurounitario, in coerenza con le indicazioni del § 3 della circolare PCM 2001 in tema di rapporti fra atti normativi. Per tale via, in particolare, le nozioni di "sistema di intelligenza artificiale", "fornitore", "deployer", "modello di IA per finalità generali" e "sistema ad alto rischio" assumono nel presente decreto il medesimo significato che rivestono nel regolamento.

Articolo 12 (Modifiche al codice penale)

L'articolo attua il criterio direttivo della lettera b) del comma 5, introducendo nel codice penale, dopo l'articolo 437, il nuovo articolo 437-bis (Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita degli stessi). La collocazione tra i delitti di comune pericolo mediante violenza (artt. 422-437 c.p.) riflette il bene giuridico tutelato e l'affinità strutturale con l'art. 437, che disciplina l'omessa collocazione di impianti destinati a prevenire infortuni sul lavoro.

Il primo comma descrive la condotta tipica: l'omessa predisposizione di misure tecniche o di sorveglianza umana idonee a prevenire alterazioni del funzionamento dei sistemi di intelligenza artificiale ad alto rischio. La condotta è imputata a chi opera in una delle fasi del ciclo di vita rilevanti (progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale): l'elenco è funzionale a coprire tutte le posizioni di garanzia individuate dal regolamento (UE) 2024/1689 — fornitore, importatore, distributore, deployer. La punibilità è subordinata al verificarsi di un pericolo concreto, in conformità del criterio di delega: la pena è graduata in funzione del bene giuridico esposto a pericolo (reclusione da uno a cinque anni per la vita o l'incolumità individuale; da due a otto anni per la pubblica incolumità o la sicurezza dello Stato).

Il secondo comma prevede una fattispecie autonoma, fuori dai casi disciplinati dal comma 1. La disposizione consente di colpire la condotta di chi, non avendo il controllo lecito del sistema di intelligenza artificiale, altera il funzionamento del sistema. Si tratta di una previsione di chiusura, necessaria per evitare aree di impunità nei casi in cui il pericolo concreto derivi dalla manipolazione attiva, esterna, del sistema. La disposizione si raccorda alla matrice omissiva del primo comma, quale completamento dell'intervento e, quindi, razionalizzazione dello stesso, in quanto risulterebbe illogico non punire l'agente esterno che realizza la, più grave, condotta attiva di alterazione. Da ciò anche il più grave trattamento sanzionatorio. Qualora dal fatto derivi un pericolo concreto per la vita o l'incolumità individuale, è prevista la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo concreto per l'incolumità pubblica o per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni.

Il terzo comma prevede la forma colposa, espressamente consentita dalla delega. La selezione della colpa grave come elemento di tipicità — sul modello

dell'art. 590-sexies c.p. introdotto dalla legge n. 24 del 2017 — risponde a un'esigenza di proporzionalità: si circoscrive la punibilità alle macroscopiche violazioni delle regole di diligenza, evitando la criminalizzazione di ogni scostamento dallo standard tecnico in un dominio caratterizzato da rapida evoluzione e da una compresenza di standard tecnici nazionali, unionali e internazionali. In questi casi la pena è ridotta da un terzo a un sesto.

Articolo 13 (Modifiche al codice di procedura penale)

L'articolo attua il criterio direttivo della lettera e) del comma 5, introducendo nel codice di procedura penale, dopo l'articolo 359-bis, il nuovo articolo 359-ter. La collocazione, nel Titolo IV del Libro V dedicato alle attività del pubblico ministero, riflette la natura dello strumento quale mezzo di ricerca della prova nelle indagini preliminari.

La disposizione disciplina l'uso, per finalità investigative, di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale. La materia è regolata, sul piano del diritto dell'Unione, dall'art. 5, paragrafo 1, lettera h), del regolamento (UE) 2024/1689, che pone un divieto generale, derogabile soltanto in casi tassativi e con stringenti garanzie procedurali. La disciplina interna è chiamata a tracciare il perimetro di liceità sul piano del procedimento penale italiano.

I commi 1 e 2 individuano le tre ipotesi di impiego: conferma di identificazione e ricerca mirata di un indiziato; localizzazione di un sospetto non identificato; ricerca del latitante destinatario di misura cautelare o di ordine di esecuzione. Il rinvio alla commissione di uno dei delitti di cui all'allegato II del regolamento consente di mantenere coerenza con il perimetro di liceità del diritto dell'Unione, evitando duplicazione di cataloghi di reati, introducendo, tuttavia, nell'ordinamento interno, ai fini di una più puntuale delimitazione di tale perimetro, che i delitti in questione debbano essere puniti con la pena della reclusione non inferiore nel massimo a quattro anni. Il comma 3 individua le modalità con le quali può avvenire il confronto biometrico, ossia con banche dati di riferimento a seconda delle finalità di cui ai medesimi commi riferiti a ciascuna delle categorie di persone per cui è ammesso il confronto. Il comma 4 estende l'impiego alla ricerca di vittime di sottrazione, tratta o sfruttamento sessuale, in coerenza con l'art. 5, paragrafo 1, lettera h), punto i), del regolamento.

Il comma 5 subordina l'impiego alla richiesta del pubblico ministero al giudice per le indagini preliminari. La previsione di una riserva di giurisdizione, e non di un'autonoma autorizzazione del pubblico ministero, costituisce il presidio essenziale di garanzia in considerazione dell'elevata intrusività dello strumento, conformemente all'orientamento del giudice delle leggi in materia di mezzi di ricerca della prova che incidono sulla riservatezza e sui dati personali.

Il comma 6 definisce il contenuto dell'autorizzazione: motivazione, delimitazione dell'area geografica, indicazione delle persone ricercate, predeterminazione del tempo strettamente necessario (in ogni caso non superiore a quindici giorni, prorogabili con decreto motivato). Il richiamo alle

valutazioni di cui all'art. 5, paragrafo 2, del regolamento (UE) 2024/1689 incorpora, sul piano sostanziale, i requisiti di necessità e proporzionalità del diritto dell'Unione.

Il comma 7 regola le ipotesi di urgenza, con un meccanismo di doppia convalida modellato sull'art. 267, comma 2, c.p.p. in materia di intercettazioni. Si prevede l'attivazione anche da parte degli ufficiali di polizia giudiziaria, con tempi rigorosamente scanditi (dodici ore per la trasmissione della richiesta al pubblico ministero; ventiquattro ore per la richiesta di convalida al giudice; quarantotto ore per la decisione di convalida).

Il comma 8 sanziona con l'inutilizzabilità i risultati ottenuti dall'impiego del sistema al di fuori dei casi consentiti o in violazione delle disposizioni dei commi 6 e 7. La sanzione processuale, formulata secondo il paradigma dell'art. 191 c.p.p., garantisce l'effettività delle prescrizioni autorizzative e si configura come strumento di chiusura del sistema di garanzie In questi casi, tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato .

Articolo 14 (Modifiche alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale)

L'articolo attua parzialmente il criterio direttivo della lettera a) del comma 5, nella parte in cui prevede strumenti cautelari di rimozione di contenuti generati illecitamente con sistemi di intelligenza artificiale. La modifica incide sull'art. 104 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al d.lgs. 28 luglio 1989, n. 271, che disciplina le modalità di esecuzione del sequestro preventivo dei dati informatici.

La lettera a) dell'articolo opera la correzione del segno d'interpunzione al termine della lettera e) dell'art. 104, comma 1, in conformità della tecnica redazionale (sostituzione del punto fermo con il punto e virgola). La lettera b) modifica la lettera e-bis) del medesimo comma, ampliando l'ambito oggettivo dei contenuti suscettibili di sequestro mediante ordine ai prestatori di servizi intermediari: si include espressamente la categoria dei contenuti generati anche con sistemi di intelligenza artificiale. La disposizione di riferimento, sul piano del diritto dell'Unione, è il regolamento (UE) 2021/784 in materia di contrasto alla diffusione di contenuti terroristici e il regolamento (UE) 2022/2065 (Digital Services Act).

Articolo 15 (Modifiche al decreto legislativo 8 giugno 2001, n. 231)

L'articolo attua il criterio direttivo della lettera c) del comma 5 — precisazione dei criteri di imputazione della responsabilità amministrativa degli enti per gli illeciti inerenti ai sistemi di intelligenza artificiale — operando per integrazione del catalogo dei reati presupposto del d.lgs. n. 231 del 2001. Tale opzione preserva la coerenza sistematica della disciplina della responsabilità amministrativa degli enti, fondata sulla tipicità penale del fatto presupposto.

L'articolo introduce nel d.lgs. n. 231 del 2001 il nuovo art. 25-vicies (Reati commessi con l'uso di sistemi di intelligenza artificiale), che si colloca dopo

l'art. 25-undevicies, da ultimo introdotto dalla legge 6 giugno 2025, n. 82, in materia di delitti contro gli animali.

Il comma 1 prevede la sanzione pecuniaria da seicento a mille quote per il delitto di cui all'art. 437-bis c.p. introdotto dall'art. 1 dello schema. La forbice si colloca nella fascia alta del catalogo e riflette la gravità del bene giuridico tutelato; il parametro di riferimento è offerto dall'art. 25-septies del medesimo decreto legislativo, relativo ai delitti di omicidio colposo e lesioni colpose gravi commessi in violazione della disciplina sulla salute e sicurezza sul lavoro.

Il comma 2 prevede la sanzione pecuniaria da duecento a settecento quote per il delitto di cui all'art. 612-quater c.p. (deepfake), introdotto dall'art. 26 della legge n. 132 del 2025. La forbice si colloca su un livello mediano del catalogo, in coerenza con la fascia delle sanzioni applicate ai delitti contro la persona di analoga gravità.

Il comma 3 estende l'applicazione delle sanzioni interdittive previste dall'art. 9, comma 2, lettere b), c), d) ed e), del d.lgs. n. 231 del 2001 a entrambe le ipotesi di responsabilità. La selezione delle lettere b), c), d) ed e) — sospensione o revoca di autorizzazioni, divieto di contrattare con la pubblica amministrazione, esclusione da agevolazioni e divieto di pubblicità — esclude l'interdizione dall'esercizio dell'attività (lett. a)) in osservanza del principio di proporzionalità: si privilegiano le misure incidenti sull'operatività dell'ente nei settori connessi all'illecito, evitando la sanzione integralmente paralizzante dell'attività.

CAPO II
(Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale)

Articolo 16 (Ambito di applicazione e foro del consumatore)

L'articolo 16 delimita l'ambito di applicazione della disciplina e introduce una regola di competenza territoriale a tutela del danneggiato persona fisica.

Il comma 1 estende l'applicazione delle disposizioni sull'accesso alle prove di cui all'articolo 17 a tutte le azioni di risarcimento del danno, contrattuale ed extracontrattuale, cagionato nell'utilizzo di un sistema di intelligenza artificiale. La scelta di ricomprendere entrambe le forme di responsabilità risponde all'esigenza di assicurare al danneggiato un meccanismo di disclosure indipendente dal titolo, contrattuale o aquiliano, della pretesa risarcitoria.

Il comma 2 circoscrive invece l'ambito applicativo delle disposizioni sulla presunzione del nesso di causalità di cui all'articolo 18 e sulla rilevanza della conformità al regolamento di cui all'articolo 19 alle azioni in cui il danno deriva dalla violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689. L'asimmetria tra l'ambito dell'articolo 19 e quello degli articoli 20 e 21 è coerente con la natura delle due tutele: l'accesso alle prove rileva ogniqualvolta sia in discussione il funzionamento di un sistema di IA, mentre

la presunzione causale presuppone, nella sua giustificazione tecnico-giuridica, la violazione di un obbligo regolatorio puntuale.

Il comma 3 contiene una clausola di salvezza dei regimi speciali di derivazione eurounitaria che presentano un ambito di sovrapposizione potenziale con la disciplina in oggetto. Sono fatte salve, in particolare, le disposizioni dell'articolo 82 del regolamento generale sulla protezione dei dati, in materia di responsabilità del titolare e del responsabile del trattamento per danno da illecito trattamento, nonché la normativa nazionale di recepimento della direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi. La clausola assicura che, negli ambiti in cui operano già regimi armonizzati di responsabilità, il presente decreto non determini effetti di interferenza o di riduzione delle tutele.

Il comma 4 introduce un foro alternativo del consumatore, prevedendo che, quando il danneggiato è una persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, sia altresì competente il giudice del luogo in cui il danneggiato ha la residenza o il domicilio. La disposizione si ispira al modello del foro del consumatore di cui all'articolo 66-bis del codice del consumo, ma se ne distingue per la natura non esclusiva, configurandosi come foro aggiuntivo rispetto ai criteri ordinari di competenza. La scelta è coerente con la ratio protettiva della delega, posto che l'esigenza di prossimità del giudice rispetto al danneggiato risulta particolarmente avvertita in controversie tecnicamente complesse, nelle quali l'asimmetria di posizione tra utente individuale e fornitore del sistema raggiunge il suo massimo grado.

Articolo 17 (Accesso alle prove)

L'articolo 17 disciplina lo strumento centrale di superamento dell'asimmetria informativa tra danneggiato e soggetto cui è imputato il danno, modellato in larga parte sull'archetipo dell'ordine di esibizione previsto dalla disciplina antitrust di derivazione eurounitaria, nonché sulle indicazioni provenienti dalla proposta, ancorché ritirata, di direttiva sulla responsabilità da intelligenza artificiale.

Il comma 1 attribuisce al giudice il potere di ordinare, su istanza della parte che allega di avere subito il danno, all'altra parte o al terzo che ne dispone, l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema di intelligenza artificiale. L'ordine è subordinato alla presentazione, da parte dell'istante, di fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema e il danno lamentato. Lo standard probatorio prescelto è quello della verosimiglianza, coerente con la funzione strumentale dell'esibizione, che presuppone per definizione una situazione di asimmetria informativa non superabile con i mezzi ordinari di acquisizione probatoria.

Il comma 2 individua, con elencazione meramente esemplificativa, le tipologie documentali più ricorrenti nelle controversie aventi ad oggetto sistemi di intelligenza artificiale: i registri di cui all'articolo 12 del regolamento (UE)

2024/1689, la documentazione del sistema di gestione dei rischi di cui all'articolo 9, le informazioni pertinenti contenute nella documentazione tecnica di cui all'articolo 11 e le informazioni relative ai parametri e alle modalità di supervisione umana di cui all'articolo 14. La scelta di ancorare l'oggetto dell'esibizione alla documentazione prevista dal regolamento sull'intelligenza artificiale persegue una duplice finalità: assicurare la concreta accessibilità di documenti già obbligatoriamente predisposti dal fornitore o dal deployer e valorizzare la funzione probatoria degli obblighi di compliance imposti dal regolamento medesimo.

Il comma 3 codifica i principi di necessità e proporzionalità dell'ordine di esibizione, imponendo al giudice di tenere conto degli interessi di tutte le parti, con particolare riguardo alla tutela dei segreti commerciali e delle informazioni riservate.

Il comma 4 disciplina specificamente l'ipotesi in cui l'esecuzione dell'ordine comporti il rischio di divulgazione di segreti commerciali o di altre informazioni riservate, prevedendo che il giudice adotti le misure idonee a garantirne la tutela. Il rinvio all'articolo 121-ter del codice della proprietà industriale consente di mutuare integralmente lo strumentario procedurale già sperimentato in materia di tutela dei segreti commerciali, evitando duplicazioni normative.

Il comma 5 disciplina le conseguenze dell'inadempimento dell'ordine di esibizione da parte della controparte: il giudice può desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile, mentre, quando l'inadempimento riguarda la documentazione di cui al comma 2, opera una più incisiva sanzione probatoria, consistente nel ritenere come ammessi i fatti allegati dall'istante, previa valutazione di ogni altro elemento di prova. La graduazione delle conseguenze è funzionale a incentivare la conservazione e l'esibizione spontanea della documentazione regolatoria.

Il comma 6 prevede, quale corollario, una sanzione pecuniaria a carico del terzo inadempiente, nella misura da euro 1.500 a euro 10.000, in considerazione dell'impossibilità di applicare al terzo le sanzioni probatorie previste per la parte.

Articolo 18 (Presunzione del nesso di causalità)

L'articolo 18 rappresenta il fulcro dell'intervento sulla ripartizione dell'onere probatorio. La disposizione introduce una presunzione *iuris tantum* del nesso di causalità tra la violazione di un obbligo previsto dal regolamento (UE) 2024/1689 e il danno.

La disposizione prevede che il nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria. L'inversione dell'onere della prova sul nesso causale non si estende alla colpa né alla violazione dell'obbligo, che restano oggetto di prova a carico dell'attore.

Articolo 19 (Rilevanza della conformità al regolamento (UE) 2024/1689)

L'articolo 19 chiarisce che la conformità del sistema di intelligenza artificiale agli obblighi previsti dal regolamento (UE) 2024/1689, anche se attestata da certificazione rilasciata ai sensi del capo III, sezione 5, del medesimo regolamento, non esclude di per sé la responsabilità del convenuto. La disposizione mira a prevenire che il sistema di valutazione della conformità predisposto dal regolamento si traduca in un meccanismo di immunità sostanziale dalla responsabilità civile, distinguendo nettamente il piano regolatorio della compliance da quello aquiliano o contrattuale del risarcimento del danno. Resta naturalmente fermo il valore probatorio della conformità ai fini della valutazione complessiva del comportamento del convenuto.

Articolo 20 (Azione diretta nei confronti dell'impresa di assicurazione)

L'articolo 20 introduce nell'ordinamento un'azione diretta del danneggiato nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile per i danni cagionati nell'utilizzo di sistemi di intelligenza artificiale, sul modello già sperimentato per la responsabilità civile da circolazione di veicoli a motore (articolo 144 del codice delle assicurazioni private).

Il comma 1 prevede la facoltà per il danneggiato di richiedere, prima dell'instaurazione del giudizio, alla parte che intende citare, l'esistenza di un contratto di assicurazione. Tale richiesta, come esplicitato in norma, non è una condizione di procedibilità; né interferisce con i procedimenti di mediazione, obbligatoria o facoltativa, che restano assoggettati alle discipline eventualmente previste con riferimento allo specifico criterio di imputazione della responsabilità di volta in volta azionato. Il soggetto cui è imputato il danno, ricevuta la richiesta di risarcimento, comunica al richiedente, entro trenta giorni, l'esistenza di un contratto di assicurazione della responsabilità civile relativo al danno dedotto, gli estremi del contratto e la denominazione dell'impresa di assicurazione. L'omessa o incompleta comunicazione è sanzionata sul piano probatorio, mediante la previsione che il giudice possa desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile.

Il comma 2 attribuisce al danneggiato l'azione diretta nei confronti dell'impresa di assicurazione, nei limiti delle somme per le quali è stipulato il contratto di assicurazione.

I commi 3, 4 e 5 disciplinano i profili tipici dell'azione diretta: l'opponibilità al danneggiato delle eccezioni derivanti dal contratto di assicurazione, purché anteriori al sinistro; il diritto di rivalsa dell'impresa di assicurazione verso l'assicurato, nella misura in cui essa avrebbe avuto titolo contrattuale per rifiutare o ridurre la propria prestazione; il litisconsorzio necessario, nel giudizio promosso dal danneggiato, del soggetto individuato quale responsabile del danno. Quest'ultima previsione assicura l'unitarietà dell'accertamento sul fatto generatore del danno e previene il rischio di giudicati contraddittori tra l'azione diretta e l'eventuale azione di rivalsa.

Il comma 6 allinea il termine di prescrizione dell'azione diretta a quello dell'azione nei confronti del soggetto individuato quale responsabile del danno, in coerenza con la natura accessoria della tutela.

Titolo III - Disposizioni finali
Capo I – Disposizioni transitorie e finanziarie

Articolo 21 (Disposizioni transitorie sull'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia)

L'articolo 21 reca disposizioni transitorie volte a disciplinare il passaggio al nuovo quadro normativo per i sistemi di IA che, alla data di entrata in vigore del decreto, risultino già oggetto di rapporti contrattuali ovvero in fase di sviluppo, sperimentazione o utilizzo per finalità di polizia (comma 1).

Lo stesso articolo, al comma 2, richiama l'osservanza dei termini di entrata in vigore e di compiuta attuazione del regolamento IA, anche con riferimento alla relativa disciplina transitoria (cfr. artt. 111 e 113), per le disposizioni del presente titolo la cui applicazione sia prevista direttamente ovvero dipenda dallo stesso regolamento unionale.

La norma transitoria in commento è finalizzata a garantire la continuità operativa delle Forze di polizia e, al contempo, l'adeguamento progressivo dei sistemi esistenti alle nuove prescrizioni derivanti dall'*AI Act*, dalla legge n. "132" e dal presente – e discendente - decreto.

Articolo 22 (Clausola di invarianza finanziaria)

L'articolo reca la clausola di neutralità finanziaria, in attuazione del comma 6 dell'art. 24 della legge delega.

RELAZIONE TECNICA

Il decreto legislativo è adottato ai sensi dell'articolo 24, comma 1, comma 2, lettera *h*), comma 3 e comma 5 della legge 23 settembre 2025, n. 132 ed è finalizzato all'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689, del Parlamento europeo e del Consiglio, del 13 giugno 2024 ("Regolamento IA" o "AI *Act*"), attraverso, in particolare, l'introduzione di una disciplina per l'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia, nonché l'introduzione di disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti di sistemi di intelligenza artificiale e di disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi.
L'**articolo 1** definisce l'oggetto e la finalità del provvedimento.

L'**articolo 2** reca le definizioni dei termini ricorrenti nel testo del provvedimento che si caratterizzano per una valenza tecnica specifica.

L'**articolo 3** verte in materia di attività di ricerca, sperimentazione, sviluppo, addestramento, adozione, applicazione, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività e delle Forze di polizia, collocandole nell'ambito della cornice dei principi costituzionali ed unionali e di quelli di cui all'articolo 3 della legge IA (comma 1), specificando che le suddette attività sono strumentali all'incremento della funzionalità e dell'affidabilità operativa dei citati sistemi e dei modelli di IA (comma 2) e ribadendo che le Forze di polizia utilizzano i predetti sistemi modelli in funzione strumentale e di supporto alle relative attività, allo scopo di incrementarne l'efficacia e l'efficienza (comma 3).
In particolare, il comma 3 chiarisce la "funzione strumentale e di supporto" dell'utilizzo dei sistemi e dei modelli di IA e dei relativi *output* alle attività di polizia.
Il comma 4 prevede che l'utilizzo dei sistemi e dei modelli di IA nell'attività di polizia, debba prevedere 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, effettuata da personale individuato dalle procedure interne di ciascuna Forza di polizia e documentata in modo da assicurarne la tracciabilità. Tale revisione è già "a sistema", perché nessun risultato fornito da un sistema automatizzato può essere - né viene - utilizzato acriticamente, senza il controllo attivo di un operatore di polizia "qualificato" (cioè esperto della materia o del settore e della tecnologia impiegata), in un atto o provvedimento incisivo sulla sfera giuridica altrui. La disposizione formalizza un principio consustanziale alle diverse forme di responsabilità che gravano sull'operatore di polizia quando si avvale di strumenti informatici o telematici, e tale formalizzazione è assicurata anche sul piano documentale, in modo da assicurare la trasparenza e la tracciabilità delle operazioni di *check-up* e verifica effettuate dal personale individuato dalle procedure interne di ciascuna Forza di polizia, come già avviene nella prassi.
L'attività di revisione dei risultati delle elaborazioni automatiche a supporto dei processi decisionali che caratterizzano l'attività di polizia rientra nelle ordinarie attività istituzionali espletate delle singole amministrazioni e pertanto alle stesse provvederà il personale all'uopo individuato nell'ambito dell'organizzazione interna di ciascuna Forza di polizia che già attualmente. risulta preventivamente selezionato per attitudini e competenze e adeguatamente formato con riferimento ai sistemi di intelligenza artificiale già in uso da parte delle singole Forze di polizia.
Il comma 5, con specifico riguardo ai sistemi ad "alto rischio", specifica che le Forze di Polizia assicurano che la sorveglianza umana sia effettiva e conforme a quanto previsto dall'articolo 14 del regolamento (UE) 2024/1689 e che il personale preposto possieda le necessarie competenze e formazione al fine di prevenire e ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali. Tale disposizione è di natura meramente ricognitiva di quanto previsto da una specifica

disposizione del regolamento UE n. 1689 del 2024 per i sistemi di IA "ad alto rischio"; pertanto, le "competenze" e la "formazione" del personale richiamate dalla norma saranno assicurate nell'ambito delle strutture formative, fisiche e non, già esistenti di ciascuna Forza di polizia e, conseguentemente, senza nuovi o maggiori oneri per la finanza pubblica.
Nello specifico, anche la formazione del suddetto personale già avviene con riguardo ai sistemi di IA nell'ambito dell'attività formativa ordinariamente programmata dalle singole Forze di polizia nei confronti dei propri dipendenti. Tale attività, sia in presenza che *online*, continuerà ad essere erogata, secondo moduli formativi già consolidati, sia attraverso seminari di formazione per formatori in servizio presso gli Istituti di Istruzione delle Forze di polizia e sia tramite moduli formativi online disponibili sulla piattaforma SISFOR, portale formativo accessibile dalla Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza e Polizia Locale, con le risorse disponibili a legislazione vigente sui pertinenti capitoli di bilancio, senza nuovi o maggiori oneri finanziari. In merito all'attività di formazione si rinvia, inoltre, a quanto indicato dalla presente relazione con riferimento all'articolo 6.
Il comma 6 reca disposizioni in materia di trattamento dei dati personali nelle attività di cui al comma 1 e il comma 7 disciplina il divieto di introduzione di nuovi o ulteriori obblighi rispetto a quanto disposto dal regolamento IA, ferme restando le esclusioni previste dallo stesso regolamento.

L'**articolo 4** consente alle Forze di polizia ad 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, nell'ambito di specifici progetti di ricerca e sperimentazione scientifica volti alla realizzazione di sistemi di intelligenza artificiale o di dispositivi che utilizzano tecnologie di intelligenza artificiale per l'attività di polizia. All'attuazione del presente articolo si provvederà senza nuovi o maggiori oneri per la finanza pubblica.

L'**articolo 5** disciplina la base giuridica per il trattamento di dati personali, effettuato dalle Forze di polizia nell'ambito di spazi di sperimentazione normativa per l'intelligenza artificiale - finalizzata allo sviluppo, alla realizzazione e alla prova di sistemi di IA, in particolare ad alto rischio, destinati alle attività di polizia - quando tale trattamento è necessario per finalità di polizia. Alla disposizione sarà data attuazione nei limiti delle risorse umane, strumentali e finanziarie previste a legislazione vigente e, comunque, senza nuovi o maggiori oneri per la finanza pubblica.

L'**articolo 6** prevede che le Forze di polizia provvedano ad attivare, presso i rispettivi istituti di formazione, specifici corsi in materia di intelligenza artificiale applicata all'attività di polizia, secondo modalità stabilite da ciascuna amministrazione nell'ambito delle risorse disponibili a legislazione vigente.
Fermo quanto indicato all'articolo 3, la disposizione ha portata ricognitiva di un'attività di formazione già in corso di svolgimento da parte delle singole Forze di polizia, con riferimento ai sistemi di AI già in uso. Gli Istituti formativi delle Forze di polizia programmano, avviano ed espletano ordinariamente appositi corsi di formazione, specializzazione e aggiornamento in materia di intelligenza artificiale, tanto nell'ambito dei corsi di base, quanto nell'ambito di quelli di secondo livello, di progressione in carriera e permanente.
Infatti, essendo già in uso taluni di sistemi di IA nell'attività di polizia, vengono già erogati specifici corsi per operatori di polizia addetti a servizi e uffici specialistici (quali, a titolo esemplificativo, la polizia scientifica e la polizia postale), mentre per i futuri sistemi di IA si provvederà a implementare e ad aggiornare le piattaforme di *e-learning* (tra cui il SISFOR) e gli specifici corsi svolti presso gli Istituti di formazione e di specializzazione delle Forze di polizia, anche a carattere interforze (come la Scuola di Perfezionamento per le Forze di polizia-SPIF).
La disposizione non comporta, pertanto, nuovi o maggiori oneri, atteso che l'attività formativa verrà espletata a valere sulle risorse disponibili sui pertinenti capitoli n. 2721 e n. 2555 iscritti nello stato di previsione del Ministero dell'interno.

L'**articolo 7** stabilisce le condizioni in base alle quali sono consentiti l'etichettatura, il filtraggio e la categorizzazione di dati biometrici nell'attività di polizia e detta disposizioni in materia di trattamento dei dati personali connesso alle suddette attività.

L'**articolo 8** disciplina le condizioni per l'utilizzo di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale in luoghi pubblici o aperti al pubblico da parte degli organi, uffici e comandi delle Forze di polizia, per finalità di prevenzione di specifiche minacce e per la ricerca di persone scomparse o vittime di determinati reati, in conformità all'articolo 5, paragrafo 1, lettera h), punti *i*) e *ii*), del regolamento (UE) 2024/1689.
In particolare, la disposizione:

a) limita l'uso dei sistemi biometrici "*real time*" a casi eccezionali e tassativi, prevedendo che essi siano impiegati esclusivamente per confermare l'identità di persone specificamente interessate ovvero per la ricerca mirata, anche dinamica e comprensiva della localizzazione, di persone specificamente individuate o individuabili in relazione alla minaccia da prevenire o alla ricerca da eseguire (comma 2);
b) stabilisce che il confronto biometrico avvenga esclusivamente con banche dati di riferimento adeguate, costituite da dati biometrici e relative informazioni identificative, derivanti da banche dati in uso alle Forze di polizia o ad altre amministrazioni pubbliche, ovvero da immagini, filmati o altri elementi biometrici acquisiti lecitamente, vietando in ogni caso l'utilizzo di banche dati costituite mediante *scraping* non mirato o in violazione della normativa in materia di protezione dei dati personali (comma 3);
c) subordina l'attivazione dei sistemi a una richiesta motivata del Questore, dei Comandanti provinciali dell'Arma dei Carabinieri e della Guardia di Finanza o dei responsabili di specifici Servizi centrali delle Forze di polizia al Procuratore della Repubblica competente, con indicazione di finalità, durata, area territoriale interessata, persone ricercate, banche dati e sistemi utilizzati (comma 4);
d) prevede una successiva autorizzazione preventiva, con decreto motivato che delimita temporalmente (massimo quindici giorni, prorogabili per periodi di pari durata), spazialmente e soggettivamente l'uso del sistema, previo svolgimento delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento sull'IA (comma 5);
e) introduce un regime di urgenza che consente, in presenza di fondato motivo di grave e irreparabile pregiudizio, l'avvio immediato dell'utilizzo su disposizione dei suddetti responsabili delle Forze di polizia, previa comunicazione al Procuratore della Repubblica, con successiva richiesta di autorizzazione e stringenti termini per la decisione dello stesso magistrato (commi 6 e 7);
f) stabilisce che, in mancanza di autorizzazione o in caso di inosservanza delle condizioni e dei termini previsti, l'uso debba essere immediatamente interrotto e tutti i dati, risultati e *output* acquisiti e prodotti debbano essere cancellati, con inutilizzabilità dei risultati ottenuti in violazione, salvo gli elementi acquisiti legittimamente su altra base giuridica (comma 8) e stabilisce l'applicabilità dei limiti di utilizzo di cui all'articolo 226, comma 5, del decreto legislativo 28 luglio 1989, n. 271 (comma 9).

La norma, pertanto, reca disposizioni di carattere procedurale definendo condizioni, limiti e presìdi giurisdizionali per l'impiego di sistemi di IA che dovranno comunque essere acquisiti o utilizzati nel rispetto della normativa vigente e delle dotazioni finanziarie e strumentali già disponibili.
Le attività di richiesta, autorizzazione, gestione operativa dei sistemi e controllo del rispetto delle condizioni d'uso rientrano nelle ordinarie funzioni istituzionali delle Forze di polizia e dell'Autorità giudiziaria e saranno svolte dal personale già in servizio, senza incrementi di organico o istituzione di nuove strutture.
Le attività procedurali richiamate sono del tutto assimilabili a quelle già ordinariamente svolte dalle Forze di polizia e dall'Autorità giudiziaria nell'ambito delle attività di "contrasto" (prevenzione dei reati, investigazione, esecuzione penale, tutela dell'ordine pubblico). Si tratta, infatti, di uno strumento tecnologico (il sistema di IA per l'identificazione biometrica in tempo reale) giuridicamente e

operativamente paragonabile ad altri dispositivi tecnici già in uso alla polizia giudiziaria o all'Autorità giudiziaria per prevenire reati, accertare notizie di reato e individuarne i responsabili, come le intercettazioni telefoniche/telematiche/ambientali o l'acquisizione dei tabulati del traffico telefonico e telematico, o ancora la geo-referenziazione personale o veicolare e il riconoscimento biometrico del presunto autore di un reato.
Per quanto precede, gli stessi servizi di polizia giudiziaria e i medesimi operatori che già impiegano i suddetti dispositivi e svolgono le connesse attività burocratiche e operative, provvederanno all'utilizzo del sistema di IA per l'identificazione biometrica ed espleteranno le correlate attività di polizia, senza necessità di incrementi d'organico o di istituzione di nuove strutture e di implementazioni di natura strumentale
In merito alle banche dati di riferimento utilizzate per il confronto biometrico, si segnala che tale attività viene già quotidianamente svolta, non in tempo reale ma a posteriori (cioè dopo la commissione di un reato), dalla polizia giudiziaria, e la differenza temporale nell'impiego del sistema biometrico, che rileva unicamente sulle condizioni di utilizzo del sistema, non incide sulle banche dati di riferimento (già in uso come l'AFIS o formata appositamente sulla base dei dati biometrici estratti da foto, video o altri elementi acquisiti nel corso dell'attività di polizia) e sulle attività tecnico-scientifiche svolte, che restano le stesse previste dalla normativa vigente, così come medesimi sono gli operatori di polizia scientifica deputati alle attività di ricerca e di comparazione biometrica, sia essa "in tempo reale" o "in differita".
L'eventuale utilizzo di sistemi di identificazione biometrica remota in tempo reale avverrà nell'ambito delle procedure di acquisizione, gestione e manutenzione delle dotazioni tecnologiche già previste a legislazione vigente e nel rispetto della clausola di invarianza finanziaria di cui all'articolo 22.

L'articolo 9 reca le disposizioni in materia di valutazione d'impatto sui diritti fondamentali, conservazione delle registrazioni e notifica dell'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale, per le finalità di cui all'articolo 8 del decreto o all'articolo 359-*ter* del codice di procedura penale.
Le attività di valutazione d'impatto sui diritti fondamentali, di tenuta dei *log* e di comunicazioni al Garante si collocano nell'ambito dei compiti già previsti dalla normativa europea e nazionale in materia di protezione dei dati personali, che le Amministrazioni sono comunque tenute ad adempiere in presenza di trattamenti di dati sensibili per finalità di polizia.
La realizzazione e gestione dei *file* di *log*, così come la redazione delle valutazioni d'impatto e delle notifiche, avverrà utilizzando le infrastrutture informatiche e le strutture organizzative già operanti, senza necessità di nuove assunzioni o di incrementi di spesa, in coerenza con quanto già affermato nella presente relazione in ordine alle attività di formazione e di sorveglianza umana sui sistemi di IA.
Il decreto ministeriale attuativo previsto al comma 5 ha natura regolatoria e tecnica.

L'articolo 10 detta disposizioni in materia di sistemi di videosorveglianza dotati di tecnologia di riconoscimento facciale a posteriori, integrata da componenti di intelligenza artificiale, per il contrasto dei reati.
La disposizione, in particolare:

a) consente, nei casi in cui la legge già prevede l'installazione di sistemi di videosorveglianza, l'integrazione degli stessi con componenti di IA che permettano, ove ricorrano esigenze di ordine e sicurezza pubblica, l'attivazione successiva di tecnologie di riconoscimento facciale, con un intervallo di tempo tale da non configurare un'identificazione biometrica remota in tempo reale ai sensi del regolamento IA (comma 1);
b) limita l'utilizzo delle tecnologie di riconoscimento facciale ai soli casi successivi alla commissione di un reato, anche tentato, e al solo fine di identificare persone già indiziate sulla base di documentazione video-fotografica e di elementi oggettivi e verificabili, sotto la diretta ed

esclusiva responsabilità di un ufficiale di pubblica sicurezza designato dal Questore per la gestione dell'ordine e della sicurezza pubblica, ovvero, al di fuori dalla predetta ipotesi, dell'ufficiale di polizia giudiziaria di cui all'articolo 57, comma 1, lettere *a*) e *b*), del codice di procedura penale che procede in relazione al fatto di reato (comma 2);

c) disciplina l'uso dei sistemi in contesti caratterizzati da esigenze di ordine e sicurezza pubblica, prevedendo la memorizzazione locale dei dati biometrici delle persone che accedono ai luoghi o eventi interessati e dei corrispondenti dati anagrafici e, ove esistente, dell'identificativo del posto assegnato, ai fini del confronto biometrico a posteriori in caso di commissione di un reato (comma 3);
d) individua nel Ministero dell'interno – Dipartimento della pubblica sicurezza il titolare del trattamento, cui compete la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva del Garante ai sensi degli articoli 23 e 24 del d.lgs. n. 51 del 2018, con possibilità di una valutazione unica per sistemi analoghi (commi 4 e 5);
e) stabilisce un termine massimo di sette giorni per la conservazione dei dati personali nella base dati di riferimento, con cancellazione automatica decorso tale termine, e di cinque anni per la conservazione dei *log* di accessi e operazioni, non modificabili e accessibili per verifiche di liceità, controlli interni e procedimenti penali, fermo restando il quadro regolatorio fissato dal d.P.R. n. 15 del 2018 (commi 6, 7 e 8);
f) vieta che decisioni con effetti giuridici negativi siano basate unicamente sui risultati del riconoscimento facciale e che i sistemi siano utilizzati per identificazione biometrica generalizzata, non mirata e priva di collegamento con un reato o procedimento penale (commi 9 e 10);
g) demanda a un decreto del Ministro dell'interno, sentito il Garante, la definizione delle modalità di trattamento e memorizzazione dei dati biometrici, delle misure tecniche e organizzative di sicurezza e degli ulteriori adempimenti in conformità al regolamento IA (comma 11);
h) prevede espressamente che all'installazione e alla manutenzione dei sistemi possano provvedere, senza nuovi o maggiori oneri per la finanza pubblica, i gestori dei luoghi, gli organizzatori o promotori degli eventi o i soggetti che hanno la disponibilità delle strutture, con concessione in comodato gratuito dei sistemi alla Questura, che ne acquisisce la completa ed esclusiva disponibilità (comma 12);
i) contiene la clausola di invarianza finanziaria volta a prevedere che dall'attuazione delle disposizioni dell'articolo non dovranno derivare nuovi o maggiori oneri per la finanza pubblica (comma 13).

L'articolo non introduce obblighi di nuova installazione di sistemi di videosorveglianza, ma si limita a consentire l'integrazione con componenti di IA ove già prevista dalla legge l'installazione dei predetti sistemi, subordinando peraltro la copertura degli oneri di installazione e manutenzione ai soggetti gestori dei luoghi od organizzatori degli eventi, escludendo espressamente nuovi oneri per la finanza pubblica.

Le attività di polizia connesse all'eventuale implementazione delle tecnologie di IA nei sistemi di video-sorveglianza, inoltre, saranno svolte nell'ambito delle ordinarie funzioni istituzionali dell'Amministrazione della pubblica sicurezza, con particolare riferimento alla tutela dell'ordine e della sicurezza pubblica e all'accertamento dei reati e della responsabilità penale dei relativi autori.

Il medesimo articolo 10 affida, inoltre, alle Amministrazioni competenti e all'Autorità Garante per la protezione dei dati personali una serie di attività (valutazioni d'impatto, consultazioni, definizione di misure tecniche) che rientrano nelle competenze istituzionali già esercitate in materia di trattamenti di dati personali per finalità di polizia e non comportano incrementi di organico o l'organizzazione di nuovi uffici.

L'articolo 11 sancisce che, ai fini della determinazione del significato delle nozioni contenute nel presente schema di decreto legislativo, si applicano le definizioni di cui all'articolo 3 del Regolamento UE 2024/1689 del Parlamento Europeo e del Consiglio, del 13 giungo 2024.
La disposizione, operando un rinvio integrale alle definizioni contenute nel Regolamento 2024/1689, ha il fine di garantire la piena uniformità terminologica del provvedimento con il quadro eurounitario.

L'articolo 12 prevede l'inserimento nel codice penale del nuovo articolo 437-bis, rubricato "*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi".*
La disposizione prevede la pena della reclusione da uno a cinque anni, per chiunque ometta di predisporre le necessarie misure tecniche, adeguate a prevenire alterazioni del funzionamento dei sistemi di IA ad alto rischio, durante le fasi di progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale. La pena è maggiorata, da due a otto anni di reclusione, qualora il fatto determini un pericolo per l'incolumità pubblica o per la sicurezza dello Stato.
Si configura più grave reato se l'alterazione illecita dei sistemi IA ad alto rischio è compiuta da soggetti estranei alle attività previste al primo comma, con pene più elevate: da due a sei anni di reclusione in caso di pericolo per l'incolumità individuale e da 3 a 10 anni nei casi in cui sia messa in pericolo l'incolumità pubblica o di sicurezza dello Stato.
La disposizione non determina nuovi o maggiori oneri per la finanza pubblica, considerato che gli adempimenti giudiziari, di natura istituzionale, potranno essere espletati avvalendosi delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

L'articolo 13 prevede l'inserimento nel codice di procedura penale del nuovo articolo 359-*ter* rubricato "*Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale".* Il comma 1 dispone l'uso di sistemi di IA per l'immediata identificazione biometrica da remoto, nonché la loro localizzazione, a fini investigativi, per soggetti indiziati secondo quanto previsto dal regolamento unionale 2024/1689.
Il comma 2 prevede che quando occorre procedere alla ricerca di un latitante ai fini dell'esecuzione di un'ordinanza che dispone una misura cautelare coercitiva per uno dei delitti indicati al comma 1 o di un ordine di esecuzione non sospeso che dispone la carcerazione per i medesimi delitti, può essere autorizzata la localizzazione della persona ricercata tramite identificazione biometrica remota in tempo reale con l'uso di sistemi di intelligenza artificiale, procedendo al confronto dei suoi dati biometrici con quelli di individui memorizzati in una banca dati di riferimento.
Il comma 3 dispone che nei casi di cui ai commi precedenti, il confronto biometrico debba avvenire esclusivamente con una banca dati di riferimento adeguata a ciascuna delle finalità di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate, di cui ai commi anzidetti.
Il comma 4 prevede l'autorizzazione, nell'ambito di un procedimento penale e con le medesime modalità già stabilite per i casi precedenti, l'impiego di sistemi di identificazione biometrica remota in tempo reale finalizzati alla ricerca mirata di specifiche vittime di reati particolarmente gravi, quali la sottrazione di persona, la tratta di esseri umani e lo sfruttamento sessuale.
Il comma 5 stabilisce che, nei casi previsti dai commi da 1 a 4, l'impiego dei sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale è subordinato a una richiesta del pubblico ministero rivolta al giudice per le indagini preliminari.
Il comma 6 dispone che il giudice per le indagini preliminari autorizzi l'impiego dei sistemi di identificazione biometrica remota in tempo reale mediante decreto motivato, nel quale devono essere puntualmente definiti i limiti e le condizioni di utilizzo. In particolare, il provvedimento deve

delimitare l'area geografica di applicazione, individuare le persone specificamente ricercate, stabilire la durata dell'attività, limitata al tempo strettamente necessario e comunque non superiore a quindici giorni, eventualmente prorogabili, su richiesta del pubblico ministero, per periodi successivi di pari durata, qualora persistano i presupposti. L'autorizzazione è inoltre subordinata alla previa effettuazione delle valutazioni previste dall'articolo 5, paragrafo 2, del regolamento (UE) 2024/1689, a garanzia del rispetto dei requisiti di liceità, necessità e proporzionalità.
Il comma 7 prevede che in caso di urgenza, consentendo l'impiego immediato dei sistemi di identificazione biometrica remota in tempo reale quando il ritardo possa arrecare un pregiudizio grave e irreparabile alle finalità investigative o di tutela previste, il pubblico ministero può disporre direttamente l'utilizzo del sistema con decreto motivato, purché sussistano i requisiti sostanziali già indicati al comma 6. Il provvedimento deve essere trasmesso al giudice per le indagini preliminari entro 24 ore, il quale provvede alla convalida entro le successive 48 ore, autorizzando la prosecuzione dell'attività. Nei casi di ulteriore urgenza, in cui non sia possibile attendere il provvedimento del pubblico ministero gli ufficiali di polizia giudiziaria possono attivare direttamente il sistema, trasmettendo la richiesta al pubblico ministero entro 12 ore. Il pubblico ministero, se sussistono i presupposti, richiede la convalida al giudice entro 24 ore dall'avvio. Il giudice provvede entro le successive 48 ore, autorizzando l'eventuale prosecuzione nel rispetto dei limiti previsti.
Il comma 8 stabilisce un espresso divieto di utilizzabilità dei risultati ottenuti mediante sistemi di intelligenza artificiale qualora il loro impiego sia avvenuto al di fuori dei casi consentiti dalla legge, oppure in violazione delle procedure e garanzie previste dai commi 6 e 7 e dispone che, in tali casi, tutti i dati personali, i risultati e gli *output* acquisiti e prodotti siano cancellati, salvo che costituiscano corpo del reato.
Le disposizioni non determinano nuovi o maggiori oneri per la finanza pubblica, considerato che gli adempimenti giudiziari, di natura istituzionale, potranno essere espletati avvalendosi delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

L'articolo 14 introduce modifiche all'articolo 104, comma 1, delle norme di attuazione del codice di procedura penale, per adattare gli strumenti giudiziari alla tutela di contenuti on line che sono sottoposti agli interventi dell'intelligenza artificiale. Pertanto, la modifica all'articolo dispone riguardo al sequestro preventivo di tali contenuti, qualsiasi essi siano, non solo riferiti al profilo personale dell'utente, attraverso l'ordine da parte dell'autorità giudiziaria ai fornitori di servizi Internet e ai gestori delle piattaforme (*social network*, siti *web*) di inibire l'accesso al contenuto. Tale misura può anche avvenire tramite l'oscuramento dell'URL e, nei casi più gravi, al sequestro del profilo *social* che ha diffuso l'opera generata dall'IA.
Considerate le modalità in cui è resa esecutiva la suddetta misura cautelare, si tratta di un mero aggiornamento e coordinamento della disciplina privo di effetti a carico della finanza pubblica.

L'articolo 15 interviene sulla disciplina della responsabilità amministrativa delle persone giuridiche di cui al decreto legislativo 8 giungo 2001 n. 231, aggiungendo il nuovo articolo 25-*vicies*, rubricato *Reati commessi con l'uso di sistemi di intelligenza artificiale.*
Il comma 1 del nuovo articolo prevede la sanzione pecuniaria da seicento a mille quote per introducendo delitto di cui all'articolo 437-*bis* c.p.

Il comma 2 prevede la sanzione pecuniaria da duecento a settecento quote per il delitto di cui all'articolo 612-*quater* cp (c.d. *deepfake*), quest'ultimo introdotto dall'articolo 26 della legge n. 132 del 2025.
Infine, il comma 3 estende l'applicazione delle sanzioni interdittive previste dall'articolo 9, comma 2, lettere b), c), d) ed e) del suddetto decreto legislativo ad entrambe le ipotesi di responsabilità previste nei precedenti due commi.
Dal punto di vista finanziario, si evidenzia che dall'attuazione della disposizione potrebbero derivare effetti positivi di gettito, allo stato eventuali e pertanto prudenzialmente non quantificati.

L'**articolo 16** delimita l'ambito di applicazione della disciplina e introduce una regola di competenza territoriale a tutela del danneggiato persona fisica.
Le previsioni sono sono dirette a delimitare l'ambito applicativo della disciplina del presente provvedimento evitando sovrapposizioni o riduzioni dei mezzi di tutela del danneggiato. Inoltre, la configurazione di un foro aggiuntivo, rispetto quelli già previsti dalla disciplina processuale-civilistica, è volto a tutelare maggiormente il soggetto consumatore in controversie tecnicamente complesse, nelle quali vi è una forte asimmetria di posizione tra utente e fornitore. Dal punto di vista finanziario, la norma non determina nuovi o maggiori oneri a carico della finanza pubblica, poiché tale previsione non istituisce un nuovo e autonomo organo giudicante, né duplica le giurisdizioni vigenti limitandosi a rimodulare la competenza territoriale, operando una differente ripartizione interna tra gli uffici giudiziari ordinari già esistenti. La definizione delle potenziali controversie derivanti dall'utilizzo dei sistemi di IA avverrà a valere sulle risorse umane già in servizio presso i Tribunali competenti, nei limiti delle rispettive dotazioni organiche e senza necessità di nuove assunzioni.

L'articolo 17 disciplina i mezzi probatori nella suddetta materia, prendendo a riferimento lo strumento dell'ordine di esibizione, previsto dalla normativa Antitrust di derivazione eurounitaria.
Dal punto di vista finanziario, la norma non determina nuovi o maggiori oneri per la finanza pubblica, in quanto limitata a disciplinare gli adempimenti a carico delle parti. Si evidenzia, inoltre, che dall'attuazione della disposizione potrebbero derivare effetti positivi di gettito, allo stato eventuali e pertanto prudenzialmente non quantificati.

L'articolo 18 prevede che, nelle ipotesi di violazione di uno o più obblighi previsti dal Regolamento (UE) 2024/1689, il nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria.
La disposizione rappresenta il fulcro dell'intervento sulla ripartizione dell'onere probatorio, in quanto introduce una presunzione iuris tantum del nesso di causalità tra la violazione di uno o più obblighi previsti dal regolamento UE 2024/1689 e il danno. Le modifiche intervenendo su ambiti processuali attinenti alla ripartizione dell'onere probatorio, non determinano nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 19 disciplina la responsabilità civile derivante dall'utilizzo di sistemi di intelligenza artificiale, prevenendo possibili esoneri da responsabilità nei casi specifici in cui sia stata rilasciata la certificazione di conformità ai sensi del Regolamento UE 2024/1689.

L'articolo 20 reca norme di carattere procedurale, introducendo nell'ordinamento un'azione diretta del danneggiato nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile per i danni cagionati nell'utilizzo dei sistemi di intelligenza artificiale, così come

già sperimentato sul modello della responsabilità derivante da circolazione di veicoli a motore (articolo 144 del codice delle assicurazioni private).
In particolare, il comma 1 stabilisce che chiunque intenda promuovere l'azione di cui al precedente articolo 16 può chiedere preventivamente al soggetto cui ritiene sia imputabile il danno se è assistito da specifica copertura assicurativa, anche se tale richiesta non costituisce condizione di procedibilità. Il soggetto, ricevuta la richiesta, comunica al richiedente, entro trenta gironi, l'esistenza del contratto di assicurazione, gli estremi e la denominazione dell'impresa di assicurazione. Si specifica altresì, che l'omessa o incompleta comunicazione è sanzionata sul piano probatorio, mediante il riconoscimento in capo dal giudice della facoltà di poter desumere argomenti di prova ai sensi dell'articolo 116 c.p.c.
Il comma 2 attribuisce al danneggiato l'azione diretta nei confronti dell'impresa di assicurazione, nei limiti delle somme per le quali è stipulato il contratto di assicurazione.
I commi 3, 4 e 5, disciplinano i profili tipici dell'azione diretta: l'opponibilità al danneggiato delle eccezioni derivanti dal contratto di assicurazione; il diritto di rivalsa; il litisconsorzio necessario.
Infine, il comma 6 uniforma il termine di prescrizione dell'azione diretta a quello dell'azione nei confronti del soggetto individuato quale responsabile del danno.

L'articolo 21, privo di effetti finanziari, reca una norma transitoria volta a disciplinare il graduale passaggio al nuovo quadro normativo per i sistemi di IA che, alla data di entrata in vigore del decreto, risultino già oggetto di rapporti contrattuali ovvero in fase di sviluppo, sperimentazione o utilizzo per finalità di polizia.

L'articolo 22 reca la clausola di invarianza finanziaria.

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

VERIFICA DELLA RELAZIONE TECNICA

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito Positivo.

Il Ragioniere Generale dello Stato

Firmato digitalmente

ANALISI TECNICO-NORMATIVA (ATN)

Titolo: Schema di decreto legislativo, recante "*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*".

Amministrazione proponente: Presidenza del Consiglio dei ministri e Ministri per gli affari europei, il PNRR e le politiche di coesione, dell'interno e della **giustizia**, di concerto con i Ministri degli affari esteri, della difesa, dell'economia e delle finanze.

Referente ATN: Uffici legislativi dei dicasteri della giustizia e dell'interno.

PARTE I – ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1. Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di Governo.

Il provvedimento in esame, adottato in attuazione dell'articolo 24 della legge 23 settembre 2025, n. 132, si inscrive nel più ampio processo di adeguamento dell'ordinamento nazionale al regolamento (UE) 2024/1689, che ha introdotto, a livello eurounitario, un quadro armonizzato in materia di intelligenza artificiale. In tale contesto, l'intervento è diretto a definire una cornice normativa organica per l'utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia e per la disciplina dei profili di responsabilità civile e penale connessi al loro impiego.

L'intervento si rende necessario al fine di colmare, nei limiti consentiti dalla legge di delegazione, il divario tra la disciplina eurounitaria e il diritto interno, assicurando un assetto regolatorio coerente per l'impiego di sistemi di intelligenza artificiale in ambiti caratterizzati da particolare delicatezza istituzionale e costituzionale, quali la sicurezza pubblica, l'attività investigativa, la tutela dei diritti fondamentali, la repressione degli impieghi illeciti dei sistemi di IA e la protezione del danneggiato nei giudizi di responsabilità civile. Sotto tale profilo, il decreto risponde all'esigenza di governare l'innovazione tecnologica mediante regole idonee a coniugare efficacia dell'azione pubblica, certezza del diritto e garanzie sostanziali e procedurali a tutela delle situazioni soggettive coinvolte.

Quanto agli obiettivi, il provvedimento persegue, in termini coordinati, la finalità di definire una cornice giuridica certa per l'utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia, di assicurare che il ricorso a tecnologie ad elevato impatto sui diritti sia assistito da adeguati presìdi di legalità, proporzionalità, trasparenza e controllo umano, di rafforzare il sistema di prevenzione e repressione degli impieghi illeciti o pericolosi dell'intelligenza artificiale, nonché di introdurre strumenti processuali idonei a riequilibrare l'asimmetria informativa e probatoria nei giudizi di responsabilità civile connessi all'uso dei medesimi sistemi. In questa prospettiva, l'intervento si colloca altresì in rapporto di coerenza sistemica con le linee di modernizzazione amministrativa e di trasformazione digitale perseguite a livello nazionale, in particolare con gli indirizzi del PNRR in materia di digitalizzazione, innovazione e sicurezza della pubblica amministrazione, nella misura in

cui valorizza l'esigenza di coniugare innovazione tecnologica, affidabilità delle infrastrutture e rafforzamento delle capacità amministrative.

Il provvedimento appare, altresì, coerente con il programma di Governo nella parte in cui questo valorizza l'innovazione tecnologica quale leva di modernizzazione dell'azione pubblica, subordinandone tuttavia l'impiego al rispetto dei diritti fondamentali, alla sicurezza dei cittadini, all'affidabilità dei processi decisionali pubblici e alla predisposizione di strumenti idonei di garanzia, responsabilizzazione e tutela. Tale coerenza risulta ulteriormente confermata dal rilievo che, nell'ambito delle politiche pubbliche in materia di trasformazione digitale, il Governo ha più volte ricondotto l'innovazione tecnologica, la sicurezza dei sistemi informativi e il rafforzamento della capacità amministrativa a una strategia unitaria di modernizzazione del Paese e della pubblica amministrazione. In questa chiave il decreto presenta evidenti profili di contatto con la spinta alla digitalizzazione promossa dalla Missione 1, Componente 1, del Piano, là dove questa mira al rafforzamento delle infrastrutture digitali della PA, alla sicurezza cibernetica, alla digitalizzazione delle grandi amministrazioni centrali e alla crescita delle competenze necessarie a governare processi innovativi ad elevato contenuto tecnologico.

2. Analisi del quadro normativo nazionale.

L'intervento normativo si inserisce in un quadro ordinamentale composito, nel quale si intrecciano fonti di diritto europeo, disposizioni nazionali di delegazione, disciplina penale e processuale penale, disciplina civilistica e normativa settoriale in materia di protezione dei dati personali e di organizzazione delle Forze di polizia.

Costituisce fondamento dell'intervento, in primo luogo, la **legge 23 settembre 2025, n. 132,** recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, e in particolare l'articolo 24, che conferisce la delega per l'adozione di decreti legislativi diretti a disciplinare l'utilizzo dell'IA nell'attività di polizia, a introdurre disposizioni penali e processuali connesse all'impiego illecito di sistemi di IA e a definire strumenti di tutela del danneggiato nei casi di responsabilità civile per danni cagionati nell'utilizzo dei medesimi sistemi.

Sul piano eurounitario, il riferimento centrale è rappresentato dal **regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024,** che stabilisce regole armonizzate sull'intelligenza artificiale e introduce un sistema di classificazione dei sistemi di IA in base al livello di rischio, prevedendo divieti, obblighi di conformità, misure di sorveglianza umana, regole documentali, obblighi di registrazione, sistemi di valutazione della conformità e specifiche prescrizioni per i sistemi ad alto rischio.

Per quanto attiene ai profili di trattamento dei dati personali, rilevano il **regolamento (UE) 2016/679**, la **direttiva (UE) 2016/680**, il **decreto legislativo 30 giugno 2003, n. 196**, recante Codice in materia di protezione dei dati personali e il **decreto legislativo 18 maggio 2018, n. 51**, nonché il **decreto del Presidente della Repubblica 15 gennaio 2018, n. 15**, concernente le modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente ai trattamenti effettuati, per finalità di polizia, da organi, uffici e comandi di polizia.

Per i profili penalistici e processuali assumono rilievo:

- il **regio decreto 19 ottobre 1930, n. 1398**, recante approvazione del testo definitivo del codice penale,
- il **decreto del Presidente della Repubblica 22 settembre 1988, n. 447**, recante approvazione del codice di procedura penale,

- il **decreto legislativo 28 luglio 1989, n. 271**, recante norme di attuazione, di coordinamento e transitorie del codice di procedura penale, nonché
- il **decreto legislativo 8 giugno 2001, n. 231**, recante disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.

Sul versante civilistico rilevano, altresì:

- il **regio decreto 16 marzo 1942, n. 262**, recante approvazione del testo del codice civile,
- il **regio decreto 28 ottobre 1940, n. 1443**, recante approvazione del codice di procedura civile, nonché
- la normativa nazionale ed eurounitaria in materia di responsabilità per danno da prodotti difettosi, con particolare riguardo alla **direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024**.

Completano il quadro di riferimento, con riguardo ai profili organizzativi e di competenza nonché agli aspetti connessi alla titolarità dei risultati della ricerca e alla tutela dei segreti commerciali:

- la **legge 1° aprile 1981, n. 121**, recante nuovo ordinamento dell'Amministrazione della pubblica sicurezza,
- il **decreto legislativo 19 agosto 2016, n. 177**, recante disposizioni in materia di razionalizzazione delle funzioni di polizia e assorbimento del Corpo forestale dello Stato,
- il **decreto legislativo 15 marzo 2010, n. 66**, recante codice dell'ordinamento militare,
- la **legge 23 aprile 1959, n. 189**, recante ordinamento del Corpo della Guardia di finanza,
- il **decreto del Presidente della Repubblica 29 gennaio 1999, n. 34**, recante regolamento per la determinazione della struttura ordinativa del Corpo della Guardia di finanza,
- il **decreto legislativo 19 marzo 2001, n. 68**, recante adeguamento dei compiti del Corpo della Guardia di finanza,
- il **decreto legislativo 10 febbraio 2005, n. 30**, recante *Codice della proprietà industriale*, rilevante sia ai fini della disciplina della titolarità dei diritti sui risultati della ricerca, sui modelli, sui dati di addestramento e sul software, sia ai fini della tutela dei segreti commerciali, espressamente richiamata dallo schema in relazione all'accesso alle prove, nonché
- il **decreto del Presidente della Repubblica 11 luglio 1980, n. 382**, limitatamente all'articolo 64, richiamato dallo schema con riguardo alla disciplina dei diritti sui risultati della ricerca nell'ambito delle collaborazioni con università ed enti di ricerca.

Nel complesso, il provvedimento si colloca quale atto di adeguamento e completamento del sistema, destinato a integrare il diritto interno rispetto agli obblighi e alle facoltà previsti dal regolamento europeo, preservando il necessario coordinamento con le discipline vigenti in materia di sicurezza pubblica, procedimento penale, responsabilità civile e protezione dei dati personali.

3. Incidenza delle norme proposte sulle leggi e sui regolamenti vigenti.

L'intervento normativo incide su una pluralità di testi normativi vigenti, sia mediante l'introduzione di disposizioni nuove, sia attraverso modifiche puntuali a corpi normativi esistenti, al fine di assicurare la coerenza complessiva del sistema rispetto all'impiego dei sistemi di intelligenza artificiale.

Sotto un primo profilo, il titolo I del decreto introduce una disciplina autonoma, speciale e di completamento relativa all'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia.

Tale disciplina non opera, di regola, mediante novella diretta delle fonti di settore già vigenti, ma si pone in rapporto di integrazione funzionale e specializzazione rispetto ad esse, in particolare rispetto ai seguenti testi:

- **legge 1° aprile 1981, n. 121**,
- **decreto legislativo 19 marzo 2001, n. 68,**
- **decreto legislativo 15 marzo 2010, n. 66, in particolare il Libro primo, Titolo IV, Capo V,**
- **decreto legislativo 19 agosto 2016, n. 177**,
- **decreto legislativo 18 maggio 2018, n. 51**,
- **decreto del Presidente della Repubblica 15 gennaio 2018, n. 15** e alle ulteriori disposizioni che regolano l'attività di polizia e il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento dei reati.

In tale ambito, il decreto precisa presupposti, limiti, garanzie e modalità di impiego dei sistemi di IA, dando specificazione interna, tra l'altro, agli obblighi e alle facoltà rilevanti desumibili dagli articoli 5, 14, 27, 57 e 59 del **regolamento (UE) 2024/1689**, nonché coordinandosi con l'articolo 4 del medesimo regolamento per i profili concernenti la formazione del personale.

In questo senso, la relativa incidenza sull'ordinamento si realizza attraverso un corpo normativo autonomo che completa e specifica la disciplina previgente, senza sostituirsi ad essa.

Sotto un secondo profilo, il titolo II, capo I, incide direttamente sul sistema penalistico e processuale mediante tecnica di novella legislativa. In tale ambito, il decreto interviene sui seguenti testi normativi vigenti con le seguenti modalità:

- inserisce nel corpo del codice penale (**r.d. 19 ottobre 1930, n. 1398**), il nuovo articolo 437-bis;
- inserisce nel codice di procedura penale (**d.P.R. 22 settembre 1988, n. 447**) il nuovo articolo 359-ter;
- modifica l'articolo 104 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale (**d.lgs. 28 luglio 1989, n. 271**);
- introduce nel **d.lgs. 8 giugno 2001, n. 231** il nuovo articolo 25-vicies.

Tali interventi si raccordano, sul piano sistematico, ai criteri direttivi fissati dall'articolo 24, comma 5, della **legge 23 settembre 2025, n. 132** e si coordinano con il perimetro di liceità e con i presupposti di impiego dei sistemi biometrici remoti delineati dall'articolo 5, paragrafo 1, lettera h), del **regolamento (UE) 2024/1689**.

Con specifico riguardo alla modifica dell'articolo 104 del **decreto legislativo 28 luglio 1989, n. 271**, non si può omettere un riferimento agli ambiti interessati dal **regolamento (UE) 2021/784** relativo al contrasto della diffusione di contenuti terroristici online e del **regolamento (UE) 2022/2065** (Digital Services Act), rispetto ai quali assume rilievo il

tema della rimozione e del sequestro di contenuti digitali generati anche mediante sistemi di intelligenza artificiale.

In questa parte, pertanto, l'incidenza sulle fonti vigenti si realizza in forma diretta, attraverso interventi puntuali su testi normativi già esistenti, secondo una tecnica redazionale pienamente coerente con la natura codicistica e sistematica delle disposizioni interessate.

Sotto un terzo profilo, il titolo II, capo II, introduce una disciplina processuale civile speciale, applicabile alle azioni risarcitorie relative ai danni cagionati dall'utilizzo di sistemi di intelligenza artificiale.

Anche in questo ambito il decreto non si sostituisce ai regimi generali della responsabilità civile né al sistema processuale ordinario, ma vi si innesta con funzione integrativa e specializzante. Esso si coordina, in particolare, con il **regio decreto 16 marzo 1942, n. 262**, recante approvazione del testo del codice civile, con il **regio decreto 28 ottobre 1940, n. 1443**, recante approvazione del codice di procedura civile, con il **decreto legislativo 10 febbraio 2005, n. 30**, recante Codice della proprietà industriale, per i profili concernenti la tutela dei segreti commerciali, con l'articolo 82 del **regolamento (UE) 2016/679** e con la disciplina nazionale, ancora in fase di recepimento, della **direttiva (UE) 2024/2853** in materia di responsabilità per danno da prodotti difettosi.

In tale cornice, le disposizioni in esame introducono regole speciali in materia di accesso alle prove, riequilibrio dell'asimmetria informativa e probatoria, presunzione del nesso causale, rilevanza della conformità al regolamento europeo e azione diretta nei confronti dell'impresa di assicurazione, valorizzando, ai fini probatori, anche obblighi documentali e organizzativi già previsti dagli articoli 9, 11, 12 e 14 del **regolamento (UE) 2024/1689**.

L'incidenza sulle fonti vigenti si configura, pertanto, come introduzione di una disciplina speciale coordinata con il diritto civile e processuale comune, giustificata dalla peculiare opacità tecnica dei sistemi di IA e dalla conseguente esigenza di rafforzare la tutela del danneggiato.

Nel complesso, l'intervento si colloca in un rapporto di stretta complementarità rispetto alla normativa europea e nazionale già vigente: esso non determina effetti sostitutivi rispetto alle discipline generali in materia di protezione dei dati personali, responsabilità civile, procedimento penale o responsabilità amministrativa degli enti, ma introduce disposizioni di integrazione, coordinamento e specializzazione, dirette a governare le peculiarità derivanti dall'impiego dei sistemi di intelligenza artificiale.

Sotto il profilo tecnico-normativo, il decreto si caratterizza per l'impiego combinato di differenti tecniche di produzione normativa — disciplina autonoma, novella legislativa e rinvio dinamico al diritto eurounitario — utilizzate in modo coerente con la struttura materiale dei diversi ambiti regolati. Ne deriva un aggiornamento del quadro ordinamentale che, senza alterarne l'impianto di fondo, ne rafforza la capacità di governo dei processi innovativi connessi all'evoluzione tecnologica. Restano, infine, ferme le clausole di invarianza finanziaria recate dai titoli I e II, in coerenza con il principio di neutralità della spesa pubblica.

4. Analisi della compatibilità dell'intervento con i principi costituzionali.

L'intervento normativo appare, nel suo complesso, compatibile con i principi costituzionali, in quanto orientato a disciplinare l'impiego dell'intelligenza artificiale in settori particolarmente sensibili mediante un assetto volto a preservare la centralità della persona, la legalità dell'azione amministrativa e giudiziaria, la tutela dei diritti fondamentali e l'effettività della giurisdizione.

Con riguardo all'attività di polizia, il provvedimento si muove nel perimetro tracciato dagli articoli 2, 3, 13, 14, 15, 24, 25, 27, 97 e 111 della Costituzione, imponendo che l'utilizzo dei sistemi di IA avvenga nel rispetto dei diritti fondamentali, dei principi di proporzionalità, non discriminazione, trasparenza e sorveglianza umana effettiva, come espressamente chiarito dagli articoli 1, 3, 5, 7, 8, 9 e 10, nonché mediante procedure autorizzative e presìdi di controllo per le forme di impiego più intrusive, quali l'identificazione biometrica remota in tempo reale disciplinata dagli articoli 8, 9 e 15.

I principi richiamati dai suddetti articoli del provvedimento in esame permeano l'intero impianto dello stesso, e ne sostengono, in coerenza con il nuovo quadro europeo sull'intelligenza artificiale, l'obiettivo di coniugare innovazione tecnologica, efficacia dell'azione di polizia e massima tutela dei diritti dei cittadini in uno Stato di diritto, in coerenza con le direttive costituzionali sopra tracciate.

Sotto il profilo penalistico e processuale, il decreto appare coerente con i principi di legalità, determinatezza, offensività e proporzionalità della risposta sanzionatoria, nonché con le garanzie del giusto processo e della riserva di giurisdizione, in particolare per quanto riguarda la disciplina introdotta dagli articoli 14, 15, 16 e 17, con speciale riferimento all'impiego investigativo dei sistemi di identificazione biometrica remota in tempo reale di cui all'articolo 15, sottoposto a rigorose condizioni sostanziali e procedurali e al controllo del giudice per le indagini preliminari.

Quanto ai profili civilistici, le disposizioni di cui agli articoli 18, 19, 20, 21 e 22, concernenti rispettivamente l'ambito di applicazione, l'accesso alle prove, la presunzione del nesso causale, la rilevanza della conformità al regolamento europeo e l'azione diretta nei confronti dell'impresa di assicurazione, risultano coerenti con gli articoli 3, 24 e 111 della Costituzione, in quanto finalizzate a riequilibrare l'asimmetria informativa e probatoria che caratterizza il contenzioso relativo ai sistemi di IA, senza comprimere irragionevolmente le prerogative difensive della controparte.

Il provvedimento risulta, altresì, coerente con l'articolo 97 della Costituzione, nella misura in cui persegue l'obiettivo di assicurare che l'adozione di tecnologie avanzate da parte delle amministrazioni di pubblica sicurezza avvenga secondo criteri di affidabilità, responsabilità, tracciabilità e buon andamento, evitando impieghi opachi o non controllabili.

Ulteriore profilo di compatibilità con i principi costituzionali è ravvisabile con riguardo all'art. 117, primo della Costituzione, atteso che la potestà legislativa statale è stata esercitata nel rispetto – oltreché della Costituzione - dei vincoli derivanti dall'ordinamento comunitario, essendo l'intervento normativo, in attuazione delle deleghe contenute nell'art. 24 della legge 23 settembre 2025, n. 132, volto ad adeguare l'ordinamento interno alla normativa unionale sull'intelligenza artificiale, di cui al regolamento (UE) 2024/1689.

Nel complesso, la disciplina si presenta idonea a realizzare un bilanciamento ragionevole tra esigenze di sicurezza, efficienza investigativa, innovazione tecnologica e tutela dei diritti fondamentali, senza introdurre deroghe incompatibili con i principi costituzionali.

5. Analisi della compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Le disposizioni in esame attengono a materie riconducibili, in via prevalente, all'ordinamento penale, processuale, civile e all'organizzazione della sicurezza pubblica, rientranti nella competenza legislativa esclusiva dello Stato ai sensi dell'articolo 117, secondo comma, lettere l) e h), della Costituzione. Non si ravvisano, pertanto, interferenze

con competenze legislative o amministrative attribuite alle Regioni ordinarie, alle Regioni a statuto speciale o agli enti locali.

6. Verifica della compatibilità con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Non si rilevano profili di incompatibilità con i principi di sussidiarietà, differenziazione e adeguatezza di cui all'articolo 118, primo comma, della Costituzione, atteso che il provvedimento non attribuisce funzioni amministrative agli enti territoriali né introduce adempimenti a loro carico.

7. Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

Il decreto non introduce rilegificazioni. L'intervento, infatti, si colloca nel corretto livello della fonte legislativa delegata, in conformità alla legge di delegazione, e fa ampio uso di tecniche di coordinamento e rinvio dinamico al regolamento (UE) 2024/1689 e alle altre fonti vigenti, evitando duplicazioni superflue. La disciplina appare altresì coerente con l'obiettivo di semplificazione normativa, nella misura in cui concentra in un unico testo l'attuazione di una pluralità di criteri direttivi relativi all'impiego dell'intelligenza artificiale in settori tra loro connessi.

8. Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Allo stato, non risultano all'esame del Parlamento progetti di legge aventi oggetto identico o tale da sovrapporsi integralmente alla disciplina recata dal presente schema, il quale si pone in attuazione diretta della delega conferita con la legge n. 132 del 2025.

9. Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non si segnalano, allo stato, giudizi di legittimità costituzionale pendenti aventi ad oggetto disposizioni del tutto analoghe a quelle recate dallo schema. Con specifico riguardo al diritto interno, l'intervento appare coerente con le linee generali della giurisprudenza nazionale in materia di garanzie sostanziali e procedurali nei settori penale e civile, là dove questa richiede che l'impiego di strumenti tecnologici incidenti su posizioni soggettive rilevanti sia assistito da una base legale sufficientemente determinata, da regole di utilizzabilità e controllabilità dell'attività tecnica e da presìdi idonei a evitare automatismi decisionali incompatibili con la responsabilità dell'autorità procedente o giudicante.

Sul versante processuale-penale, le disposizioni dello schema si collocano in linea con i principi affermati dalla giurisprudenza di legittimità in materia di legalità processuale, rigorosa delimitazione dei presupposti di impiego dei mezzi tecnici di ricerca della prova, controllo giurisdizionale e inutilizzabilità degli esiti acquisiti in violazione delle garanzie di legge.

In tale cornice, la disciplina dell'identificazione biometrica remota in tempo reale e quella relativa all'inutilizzabilità dei risultati ottenuti fuori dai casi consentiti si inseriscono in un assetto ordinamentale che, nei procedimenti incidenti sulla libertà personale, sulla riservatezza e sul diritto di difesa, esige che l'uso della tecnologia resti integralmente assoggettato ai principi di legalità, proporzionalità e controllo del giudice.

Sul versante civile, le disposizioni introdotte in materia di accesso alle prove, presunzione del nesso causale e azione diretta nei confronti dell'impresa di assicurazione appaiono

coerenti con i principi generali della giurisprudenza nazionale in tema di effettività della tutela giurisdizionale e di ragionevole distribuzione degli oneri probatori, specialmente nei contesti connotati da asimmetria informativa o da particolare complessità tecnica.
In questa prospettiva può richiamarsi, in termini di conferma del rilievo che l'ordinamento attribuisce alla piena tutela delle posizioni soggettive incise da condotte o assetti organizzativi lesivi, la Corte di cassazione, Sezioni Unite civili, sentenza 25 settembre 2025, n. 26080, che ha valorizzato il diritto soggettivo del privato all'autodeterminazione nelle scelte che comportano impiego di risorse e la necessità che il sistema appresti rimedi effettivi nei confronti di lesioni giuridicamente rilevanti. In questo senso, la disciplina speciale delineata dallo schema non altera irragionevolmente il quadro dei rimedi civilistici vigenti, ma ne rafforza la capacità di offrire una tutela effettiva al danneggiato, calibrando gli strumenti processuali sulla peculiare opacità tecnica dei sistemi di intelligenza artificiale.
Non emergono, pertanto, linee giurisprudenziali interne ostative all'intervento; al contrario, le acquisizioni prevalenti in materia penale, processuale e civile convergono nel richiedere una base normativa chiara, la delimitazione dei presupposti di impiego degli strumenti tecnici, la controllabilità dei relativi esiti e l'effettività della tutela giurisdizionale.

PARTE II – CONTESTO NORMATIVO DELL'UNIONE EUROPEA E INTERNAZIONALE

10. Analisi della compatibilità dell'intervento con l'ordinamento dell'Unione europea.

Il provvedimento è direttamente connesso al diritto dell'Unione europea, in quanto costituisce attuazione della legge di delegazione adottata ai fini dell'adeguamento dell'ordinamento nazionale al regolamento (UE) 2024/1689.

La sua finalità primaria è, pertanto, assicurare la coerenza del diritto interno con il quadro eurounitario in materia di intelligenza artificiale.

La disciplina proposta appare compatibile con l'ordinamento dell'Unione europea in quanto si conforma all'impianto dell'AI Act, ne recepisce i principi fondamentali e ne specifica l'applicazione in ambiti che il medesimo regolamento rimette, nei limiti consentiti, alla disciplina nazionale, in particolare per quanto riguarda l'uso dei sistemi biometrici da parte delle autorità competenti per finalità di polizia e l'introduzione di strumenti di tutela e responsabilità nel diritto interno.

Il decreto risulta, inoltre, coerente con la Carta dei diritti fondamentali dell'Unione europea, in particolare con gli articoli 7, 8, 20, 21, 47, 48 e 52, nonché con la normativa eurounitaria in materia di protezione dei dati personali, di tutela giurisdizionale effettiva e di responsabilità per danno da prodotti difettosi.

11. Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Non risultano, allo stato, procedure di infrazione avviate dalla Commissione europea nei confronti della Repubblica italiana sul medesimo oggetto specifico. Il provvedimento si inserisce anzi in un'ottica di prevenzione di possibili disallineamenti rispetto agli obblighi derivanti dal regolamento (UE) 2024/1689.

12. Analisi della compatibilità dell'intervento con gli obblighi internazionali.

L'intervento appare compatibile con gli obblighi internazionali assunti dalla Repubblica italiana, e in particolare con la Convenzione europea dei diritti dell'uomo. Le garanzie

introdotte in tema di sorveglianza umana, controllo giurisdizionale, proporzionalità delle misure, tutela della riservatezza e accesso alla prova risultano coerenti con gli standard convenzionali elaborati dalla Corte europea dei diritti dell'uomo in materia di giusto processo, diritto alla vita privata, non discriminazione e tutela giurisdizionale effettiva.

13. Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non risultano, allo stato, giudizi pendenti innanzi alla Corte di giustizia dell'Unione europea aventi ad oggetto specificamente il presente schema. Tuttavia, la giurisprudenza della Corte in materia di protezione dei dati personali, trasparenza algoritmica e tutela giurisdizionale effettiva costituisce un parametro interpretativo di rilievo, cui il provvedimento appare sostanzialmente conforme.

In particolare, la Corte di giustizia, Prima Sezione, sentenza 7 dicembre 2023, causa C-634/21, SCHUFA Holding (Scoring) ha chiarito che i trattamenti automatizzati suscettibili di incidere in modo determinante sulla posizione dell'interessato ricadono nel perimetro delle garanzie di cui all'articolo 22 del regolamento (UE) 2016/679.

Successivamente, la Corte di giustizia, Prima Sezione, sentenza 27 febbraio 2025, causa C-203/22, Dun & Bradstreet Austria, ha ulteriormente precisato che l'interessato deve essere posto in condizione di comprendere i criteri essenziali della decisione automatizzata e di contestarne utilmente gli effetti. Tali principi appaiono coerenti con l'impianto del presente schema, che esclude la decisività automatica dell'output e valorizza il controllo umano, la tracciabilità e la verificabilità dei presupposti di impiego dei sistemi di IA.

14. Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non risultano pendenti innanzi alla Corte europea dei diritti dell'uomo giudizi aventi ad oggetto identico a quello disciplinato dal provvedimento. Le linee prevalenti della giurisprudenza della Corte confermano, tuttavia, che l'utilizzo di tecnologie invasive o automatizzate da parte delle autorità pubbliche deve essere sorretto da una base normativa chiara, garanzie adeguate contro l'arbitrarietà e rimedi effettivi.

In particolare, la Corte europea dei diritti dell'uomo, Grande Camera, sentenza 4 dicembre 2008, *S. and Marper v. the United Kingdom*, ricc. nn. 30562/04 e 30566/04, ha affermato, in materia di dati biometrici, che la conservazione di impronte digitali, campioni biologici e profili genetici di persone non condannate integra un'ingerenza nel diritto al rispetto della vita privata ai sensi dell'articolo 8 CEDU e richiede, pertanto, un rigoroso scrutinio di proporzionalità. La Corte ha in particolare censurato il carattere «general and indiscriminate» del meccanismo di conservazione e ha ribadito che, in una società democratica, la legittimità di tali misure presuppone una disciplina sufficientemente circoscritta quanto ai presupposti soggettivi e oggettivi di applicazione, alla durata della conservazione, alle finalità perseguite e all'esistenza di garanzie effettive contro arbitrii e usi impropri del materiale raccolto.

Più di recente, la Corte europea dei diritti dell'uomo, Grande Camera, sentenza 25 maggio 2021, *Big Brother Watch and Others v. the United Kingdom*, ricc. nn. 58170/13, 62322/14 e 24960/15, ha affermato che i regimi di sorveglianza segreta e di intercettazione massiva, pur non essendo in sé incompatibili con l'articolo 8 CEDU, richiedono una disciplina chiara e presìdi effettivi lungo l'intero ciclo del trattamento.

Anche sotto tale profilo, l'impostazione del decreto — fondata su delimitazione dei presupposti, autorizzazione, controlli e tracciabilità — appare in linea con i principali standard convenzionali.

Difatti, non soltanto le disposizioni della parte più generale del titolo I (in particolare, gli artt. 3, 4 e 5) contengono puntuali interventi e richiami in materia di protezione dei dati personali, con particolare riguardo a quelli "sensibili" (come i dati biometrici), ma la disciplina degli articoli 7-10, il cui fulcro è costituito, pur nella diversità delle ipotesi, proprio dal trattamento di dati biometrici per finalità di polizia, è dedicata in modo preponderante alla tutela degli stessi, con la previsione di obblighi, requisiti, procedure e garanzie stringenti e tassative.

Le disposizioni sull'etichettatura e il filtraggio di set di dati biometrici (art. 7) e sull'identificazione biometrica remota in tempo reale (art. 8-9 e 14), in particolare, sono state elaborate in conformità all'art. 5, par. 1, lett. *g*) e *h*), del regolamento (UE) 2024/1689, nonché in linea con gli orientamenti della Commissione europea sulle pratiche di IA vietate ai sensi del predetto articolo 5, pubblicate – a norma dello stesso regolamento – il 29 luglio del 2025 (C-2025 5052 final).

15. Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Non si hanno indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto all'interno degli Stati membri dell'Unione europea.

PARTE III – ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO

1. Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

Lo schema introduce, all'articolo 2, un insieme di definizioni normative necessarie a delimitare con precisione il perimetro applicativo del titolo I, adottando una tecnica mista che combina definizioni espressamente formulate nel testo, rinvii all'articolo 2 della legge n. 132 del 2025 e rinvii al regolamento (UE) 2024/1689.

Tale impostazione risponde all'esigenza di assicurare uniformità terminologica con il diritto eurounitario, evitando duplicazioni non necessarie, ma al tempo stesso consente di adattare il lessico normativo europeo alle specificità del contesto nazionale dell'attività di polizia.

Sotto questo profilo, assumono rilievo, anzitutto, le definizioni di "regolamento IA" e di "legge IA", introdotte dall'articolo 2, lettere a) e b), che assolvono a una funzione di semplificazione redazionale e di chiarezza sistematica, consentendo di richiamare in modo univoco, nel prosieguo del testo, rispettivamente il regolamento (UE) 2024/1689 e la legge 23 settembre 2025, n. 132.

Parimenti funzionali alla chiarezza applicativa risultano le definizioni di "sistema di IA", "pratiche vietate", "sistema di IA ad alto rischio", "categorie particolari di dati personali", "dati relativi a condanne penali e reati", "profilazione" e "output", recate dall'articolo 2, lettere c), d), e), f), g) h) e j), le quali rinviano a nozioni già presenti, direttamente o indirettamente, negli articoli 3, 5, 6 del regolamento (UE) 2024/1689 oltre che nell'articolo 10 del regolamento (UE) 2016/679 e ne assicurano il coerente innesto nel diritto interno.

Particolare rilievo assumono, inoltre, le definizioni che svolgono una funzione di adattamento e specificazione del quadro eurounitario rispetto al contesto nazionale.

In tale categoria rientrano, in primo luogo, la nozione di "dati operativi sensibili", introdotta dall'articolo 2, lettera i), che consente di circoscrivere l'ambito dei dati trattati o detenuti dalle Forze di polizia cui si riferiscono le speciali cautele del decreto, e quella di "scraping non mirato" (recata dall'articolo 2, lettera k) del testo), la cui espressa definizione appare particolarmente opportuna in ragione della centralità che tale nozione assume ai fini del divieto di utilizzare banche dati biometriche costituite mediante raccolte massive e indiscriminate di immagini.

Nella medesima prospettiva si collocano altresì le definizioni di "direttiva n. 680/2016", di "decreto legislativo n. 51 del 2018", di "d.P.R. n. 15 del 2018" e di "Garante", contenute nell'articolo 2, lettere l), m), o) e p), che, pur avendo carattere prevalentemente ricognitivo, risultano necessarie per evitare incertezze interpretative in una materia fortemente intrecciata con la disciplina del trattamento dei dati personali per finalità di polizia.

Rivestono poi uno specifico rilievo sistematico le definizioni che individuano gli attori istituzionali e l'ambito materiale di operatività del titolo I.

In particolare, la definizione di "Autorità nazionali per l'intelligenza artificiale", di cui all'articolo 2, lettera n), consente di coordinare il decreto con l'assetto nazionale di governance dell'IA; quella di "Forze di polizia", recata dall'articolo 2, lettera q), collega espressamente il testo all'articolo 16 della legge 1° aprile 1981, n. 121; le definizioni di "attività di polizia" e di "finalità di polizia", contenute nell'articolo 2, lettere r) e s), precisano l'ambito oggettivo e funzionale entro il quale il ricorso ai sistemi di IA è consentito, evitando incertezze circa l'estensione applicativa della disciplina. Si tratta, in questo caso, di definizioni particolarmente rilevanti, poiché da esse dipendono la corretta delimitazione del perimetro di liceità delle attività disciplinate e il coordinamento con la normativa europea e nazionale in materia di sicurezza pubblica e protezione dei dati.

Nel complesso, il nuovo apparato definitorio appare necessario, coerente e proporzionato. Esso non introduce innovazioni terminologiche arbitrarie, ma seleziona e organizza, in funzione del presente decreto, le definizioni indispensabili a garantire un'applicazione uniforme della disciplina, riservando al rinvio alla legge n. 132 del 2025 e al regolamento (UE) 2024/1689 la funzione di chiusura del sistema definitorio per quanto non espressamente previsto.

Sotto tale profilo, la tecnica utilizzata risulta conforme ai criteri di buona normazione, poiché consente di evitare duplicazioni, ridurre il rischio di divergenze semantiche e assicurare la piena coerenza con il lessico normativo già in uso a livello nazionale ed eurounitario.

2. Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi.

I riferimenti normativi contenuti nello schema risultano, in linea generale, corretti e coerenti con il quadro vigente, con puntuale richiamo agli atti normativi nazionali ed eurounitari rilevanti. La struttura dei rinvii appare idonea a garantire il coordinamento con le successive modificazioni e integrazioni delle fonti richiamate, in particolare mediante il rinvio dinamico al regolamento (UE) 2024/1689.

3. Ricorso alla tecnica della novella legislativa per introdurre modificazioni e integrazioni a disposizioni vigenti.

L'intervento normativo fa uso combinato di diverse tecniche redazionali: introduce un autonomo corpo di disposizioni per i profili concernenti l'attività di polizia; impiega la tecnica della novella codicistica per le modifiche al codice penale, al codice di procedura penale, alle norme di attuazione e al decreto legislativo n. 231 del 2001; introduce infine disposizioni processuali civili speciali in forma autonoma ma sistematicamente coordinate con il codice di procedura civile e con il diritto civile sostanziale.
La tecnica prescelta appare appropriata alla natura e alla complessità della materia, consentendo di preservare la leggibilità del testo e la chiarezza dei punti di incidenza sulle fonti vigenti, nonché di mantenere un adeguato coordinamento sistematico con i corpi normativi interessati.
Il ricorso alla tecnica della novella legislativa risulta quindi pienamente giustificato nei segmenti dell'intervento che richiedono l'inserimento o l'adeguamento di disposizioni all'interno di testi normativi vigenti, mentre la scelta di un'articolazione autonoma per la disciplina dell'attività di polizia e degli strumenti processuali civili appare coerente con la specificità e l'autonomia funzionale delle relative materie.

4. Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.

Lo schema non sembra produrre effetti abrogativi impliciti ulteriori rispetto a quelli espressamente voluti dal legislatore delegato mediante l'introduzione di nuove disposizioni speciali o la modifica puntuale di norme vigenti.

L'impianto normativo è costruito in termini di integrazione e coordinamento, con clausole di salvezza e di rinvio che riducono il rischio di abrogazioni tacite o di antinomie non governate.

5. Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

Il decreto non contiene disposizioni aventi efficacia retroattiva, né norme di interpretazione autentica o di reviviscenza di disposizioni precedentemente abrogate.

Le eventuali disposizioni derogatorie rispetto al diritto comune risultano circoscritte agli specifici ambiti regolati e appaiono giustificate dalla peculiarità tecnica e giuridica dell'oggetto disciplinato.

Inoltre, rispetto alla normativa vigente, il provvedimento non introduce deroghe in senso tecnico al quadro normativo unionale e nazionale di riferimento, ma reca una disciplina speciale di attuazione e specificazione degli istituti, degli strumenti e delle eccezioni previste dal regolamento (UE) 2024/1689.

Il riferimento, in particolare, è agli articoli 5, 7, 8, 9, 10 e 11 del Titolo I.

L'articolo 5 costituisce la base giuridica, richiesta dall'art. 59, par. 2, del regolamento (UE) 2024/1689, per il trattamento dei dati personali, inclusi i dati operativi sensibili, negli spazi di sperimentazione normativa (cd. "*sandbox*") previsti dagli artt. 57 e ss. dello stesso regolamento unionale, con specifico riferimento ai sistemi di IA ad alto rischio destinati all'utilizzo nelle attività di polizia. La disposizione non ha effetto retroattivo, trattandosi di spazi che devono essere ancora istituiti, né di reviviscenza di norme già abrogate o di interpretazione autentica, ovvero derogatorio rispetto alla normativa vigente.

L'articolo 7 declina l'eccezione prevista dall'articolo 5, paragrafo 1, lettera g), del regolamento (UE) 2024/1689, in materia di etichettatura, filtraggio e categorizzazione di dati biometrici nell'attività di polizia, senza generare effetti retroattivi (posta

l'obbligatorietà e la diretta applicabilità dell'atto unionale in questione), di interpretazione autentica (che non compete alla legislazione nazionale) o derogatori.

Gli articoli 8 e 9, invece, implementano e dettagliano sul piano interno l'eccezione prevista dall'articolo 5, paragrafo 1, lettera h), del regolamento (UE) 2024/1689, in materia di identificazione biometrica remota in tempo reale per finalità di prevenzione e di ricerca di persone scomparse o di specifiche vittime di reato.

Tali disposizioni non hanno effetto retroattivo, perché all'opposto disciplinano per la prima volta la possibilità di utilizzare, in via eccezionale, sistemi di IA per identificare o localizzare persone "*in tempo reale*"; per la stessa ragione, le stesse non determinano la reviviscenza di norme precedentemente abrogate, essendo le prime di questa tipologia, non forniscono interpretazione autentica (in assenza di una disposizione previgente sull'identificazione biometrica remota *in tempo reale*) né derogano ad alcuna norma vigente, innovando piuttosto l'ordinamento interno con riferimento alla tecnologia biometrica di che trattasi.

L'articolo 10 introduce, a sua volta, una disciplina speciale di settore in materia di riconoscimento facciale a posteriori, nel rispetto dell'articolo 26, paragrafo 10, del regolamento (UE) 2024/1689, e della disciplina generale sul trattamento dei dati personali per finalità di polizia di cui alla direttiva (UE) 2016/680 e al decreto legislativo 18 maggio 2018, n. 51.

Anche questa disposizione non ha effetto retroattivo, prevedendo la possibilità pro futuro di integrare sistemi di videosorveglianza installati sulla base di specifiche disposizioni di legge con componenti di intelligenza artificiale dotati della funzione di riconoscimento facciale a posteriori del presunto autore di un reato, non determina la reviviscenza di norme precedentemente abrogate né configura un'interpretazione autentica di norme vigenti.

La stessa, inoltre, risulta coerente con la previsione di cui all'articolo 9, comma 12, del decreto-legge n. 139 del 2021, che esclude, dalla moratoria prevista – fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2027 – dal comma 9 dello stesso articolo sull'installazione e sull'utilizzo di impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, le tecnologie biometriche impiegate dalle Autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali, di cui al decreto legislativo n. 51 del 2018, in presenza di parere favorevole del Garante per la protezione dei dati personali: a tal riguardo, si segnala che nell'art. 10 del provvedimento in esame la predetta *Authority* deve essere consultata preventivamente dal titolare del trattamento ai sensi del comma 5, nonché sentita nell'ambito del procedimento di adozione del decreto di cui al comma 11).

L'articolo 11 reca, infine, una disposizione transitoria priva di efficacia retroattiva.

6. Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.

Non risultano deleghe legislative aperte sul medesimo oggetto tali da interferire con il presente schema, al di fuori della medesima delega di cui all'articolo 24 della legge n. 132 del 2025, della quale il provvedimento costituisce attuazione. Non emergono, allo stato, profili di sovrapposizione con ulteriori deleghe integrative o correttive specificamente riferite alla medesima materia.

7. Indicazione degli eventuali atti successivi attuativi e dei motivi per i quali non è possibile esaurire la disciplina con la normativa proposta e si rende necessario il rinvio a successivi provvedimenti attuativi; verifica della congruità dei termini previsti per la loro adozione.

Il testo prevede alcuni atti successivi attuativi.

In particolare:

- l'articolo 5 demanda a un regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'interno, la definizione delle modalità di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e le attività sperimentali di sistemi di IA per finalità di polizia disciplinate dal medesimo articolo;
- l'articolo 9, comma 5, demanda a un decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, sentiti il Garante e le Autorità nazionali per l'intelligenza artificiale, l'individuazione dei requisiti tecnici minimi, delle misure di monitoraggio, sicurezza e notifica relativi ai sistemi di identificazione biometrica remota in tempo reale per finalità di prevenzione, di ricerca di persone scomparse o di vittime di specifici reati (art. 8), nonché nell'ambito delle indagini preliminari per i gravi delitti indicati nell'allegato II del regolamento sull'IA (art. 14, che innesta l'art. 359-*ter* nel codice di procedura penale);
- l'articolo 10, comma 11, invece, demanda a un decreto del Ministro dell'interno, sentito il Garante, la definizione delle modalità di trattamento e memorizzazione dei dati biometrici e delle misure di sicurezza relative alle tecnologie di intelligenza artificiale per il riconoscimento facciale *a posteriori* rispetto alla commissione di un fatto di reato (*post delictum*), integrabili, ove ricorrano esigenze di ordine e sicurezza pubblica, nei sistemi di videosorveglianza installati a norma di legge.

Tali rinvii appaiono giustificati dalla necessità di demandare a fonti secondarie o ad atti tecnico-amministrativi la disciplina di profili ad elevato contenuto specialistico e suscettibili di rapido aggiornamento. I termini previsti per la loro adozione risultano, in linea generale, congrui rispetto alla complessità degli adempimenti richiesti.

Circa la congruità dei termini previsti per l'adozione degli atti successivi attuativi sopra indicati, gli artt. 5, comma 4, e 9, comma 5, non prevedono un termine precipuo per la loro adozione, e tale scelta risulta coerente con la necessità di coordinare gli adempimenti tecnici e organizzativi necessari per la loro attuazione con quelli previsti dal regolamento (UE) 2024/1689 - rispetto ai quali, peraltro, sono in fase avanzata proposte normative (nel quadro del cd. pacchetto legislativo "*Digital Omnibus VII*") volte a rinviare alcuni obblighi dell'*AI Act,* offrendo alla pubblica amministrazione e alle imprese un margine temporale aggiuntivo - ovvero spettanti ad altre Autorità o Amministrazioni nazionali, oltreché motivata dall'assoluta innovatività e notevole complessità delle fattispecie che ne formano oggetto, come gli spazi di sperimentazione normativa/*sandbox* e l'identificazione biometrica remota in tempo reale per finalità di prevenzione, di ricerca o di indagine.

L'art. 10, comma 11, invece, prevede un termine di tre mesi, dalla data di entrata in vigore del provvedimento in esame, per l'adozione del decreto del Ministro dell'interno, sentito il Garante per la protezione dei dati personali, con cui dovranno essere individuate *inter alia* le modalità del trattamento automatizzato dei dati biometrici ai sensi della medesima disposizione e le misure tecniche e organizzative necessarie a garantire la sicurezza del trattamento stesso.

In questo caso, trattandosi di sistemi, quelli di videosorveglianza "tradizionali", già installati e utilizzati a norma di legge, e di una tecnologia, quella del riconoscimento facciale *a posteriori* rispetto alla commissione di un fatto di reato (*post delictum*), già sperimentata in alcuni ambiti specifici (come gli impianti sportivi in occasione di partite di calcio) ovvero impiegata dalla polizia giudiziaria nel quadro di un'attività di indagine penale, il termine di tre mesi per l'adozione del decreto appare congruo per l'individuazione "giuridica", con mirato riferimento a determinati luoghi od eventi, delle modalità, delle misure e degli adempimenti previsti dal suddetto comma 11, ferme restando le diverse – non predeterminate né predeterminabili in astratto – tempistiche delle successive, eventuali fasi di allestimento tecnico e di impiego operativo dei sistemi di videoripresa integrati dalle tecnologie biometriche in parola, e l'esigenza di coordinamento con i profili disciplinati dalle pertinenti disposizioni del regolamento (UE) n. 1689/2024 sui sistemi ad alto rischio, in particolare biometrici.

8. Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche.

Le relazioni di accompagnamento al provvedimento valorizzano elementi descrittivi e valutativi relativi agli impatti ordinamentali e finanziari dell'intervento. Non emerge, allo stato, la necessità di acquisire specifiche elaborazioni statistiche dell'Istituto nazionale di statistica, potendo gli eventuali dati di monitoraggio essere raccolti nell'ambito delle attività istituzionali delle amministrazioni competenti, anche in relazione all'attuazione pratica dei sistemi di IA e delle garanzie previste dal decreto.