

dossier

XIX Legislatura

6 luglio 2026

Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile

Atto del Governo n. 418

Ai sensi dell'articolo 24, commi 1, 2, lettera *h*), 3, 4 e 5, della legge 23 settembre 2025, n. 132



SERVIZIO STUDI

TEL. 06 6706-2451 - ✉ studi1@senato.it – ✕ [@SR_Studi](https://www.instagram.com/SR_Studi)

Dossier n. 728



SERVIZIO STUDI

Dipartimento Istituzioni

Tel. 06 6760-3855 - ✉ st_istituzioni@camera.it ✕ [@CD_istituzioni](https://www.instagram.com/CD_istituzioni)

Dipartimento Giustizia

Tel. 06 6760-9148 - ✉ st_giustizia@camera.it – ✕ [@CD_giustizia](https://www.instagram.com/CD_giustizia)

SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA

Tel. 066760-2145-✉ rue_segreteria@camera.it-✕ @CD_europa-
europa.camera.it

Atti del Governo n. 418

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

AC0507

INDICE

IL QUADRO EUROPEO DI RIFERIMENTO (A CURA DEL SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA)	5
---	----------

SCHEDE DI LETTURA

TITOLO I - UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE PER L'ATTIVITÀ DI POLIZIA	9
--	----------

CAPO I – DISPOSIZIONI GENERALI.....	9
--	----------

- *Articolo 1 (Oggetto e finalità).....*9
- *Articolo 2 (Definizioni)*13

CAPO II – DISPOSIZIONI IN MATERIA DI RICERCA, SVILUPPO, ADDESTRAMENTO, FORMAZIONE, SPERIMENTAZIONE E UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE NELLE ATTIVITÀ DI POLIZIA.....	18
---	-----------

- *Articolo 3 (Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività di polizia).....*18
- *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).....*24
- *Articolo 5 (Sviluppo, realizzazione e prova di determinati sistemi di IA per finalità di polizia negli spazi di sperimentazione normativa)*27
- *Articolo 6 (Formazione del personale di polizia)*32

CAPO III – SISTEMI DI INTELLIGENZA ARTIFICIALE UTILIZZATI NELLE 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	34
--	-----------

- *Articolo 7 (Etichettatura, filtraggio e categorizzazione di dati biometrici nell'attività di polizia).....*34
- *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)	37
▪ Articolo 9 (<i>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</i>).....	41
▪ Articolo 10 (<i>Disposizioni in materia di sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall'intelligenza artificiale, per il contrasto dei reati</i>).....	44
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	51
CAPO I – DISPOSIZIONI SANZIONATORIE E IN MATERIA DI PROCEDIMENTO PENALE	51
▪ Articolo 11 (<i>Definizioni</i>)	51
▪ Articolo 12 (<i>Modifiche al codice penale</i>).....	54
▪ Articolo 13 (<i>Modifiche al codice di procedura penale</i>).....	57
▪ Articolo 14 (<i>Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale</i>).....	62
▪ Articolo 15 (<i>Modifiche alla responsabilità amministrativa degli enti</i>).....	65
CAPO II – STRUMENTI PROCESSUALI CIVILI PER IL RISARCIMENTO DEI DANNI CAGIONATI DALL'UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE	69
▪ Articolo 16 (<i>Ambito di applicazione e foro del consumatore</i>).....	69
▪ Articolo 17 (<i>Accesso alle prove</i>)	75
▪ Articolo 18 (<i>Presunzione del nesso di causalità</i>).....	81
▪ Articolo 19 (<i>Rilevanza della conformità al regolamento (UE) 2024/1689</i>).....	82
▪ Articolo 20 (<i>Azione diretta nei confronti dell'impresa di assicurazione</i>).....	83
TITOLO III - DISPOSIZIONI FINALI.....	85
CAPO I – DISPOSIZIONI TRANSITORIE E FINANZIARIE.....	85
▪ Articolo 21 (<i>Disposizioni transitorie sull'utilizzo dei sistemi</i>	

<i>di intelligenza</i>	85
▪ Articolo 22 (<i>Clausola d'invarianza finanziaria</i>)	87

IL QUADRO EUROPEO DI RIFERIMENTO

(a cura del Servizio per i Rapporti con l'Unione europea)

Lo schema di decreto legislativo interviene in un settore interessato da una recente e significativa evoluzione del quadro normativo dell'Unione europea, rappresentata in particolare dal [regolamento \(UE\) 2024/1689](#) sull'intelligenza artificiale (*AI Act*).

Con riferimento alle disposizioni dello schema **relative all'utilizzo di sistemi di intelligenza artificiale nell'ambito delle attività di polizia**, il diritto dell'Unione presta specifica attenzione all'esigenza di coniugare efficacia dell'azione pubblica, sicurezza e tutela dei diritti fondamentali, anche alla luce della disciplina europea in materia di protezione dei dati personali, rappresentata dal [regolamento \(UE\) 2016/679](#) (GDPR) e dalla [direttiva \(UE\) 2016/680](#) relativa ai trattamenti effettuati a fini di prevenzione, accertamento e repressione dei reati.

In relazione alle disposizioni dello schema di decreto in esame, appare inoltre opportuno richiamare **i più recenti sviluppi del quadro normativo europeo**. Il 29 giugno 2026 il Consiglio dell'Unione europea ha infatti **ha definitivamente adottato** la [proposta](#) di regolamento volta a razionalizzare e semplificare alcune norme in materia di IA, parte del cosiddetto pacchetto *Digital Omnibus* (*Omnibus VII*).

Presso la **Camera**, la proposta è stata esaminata, ai fini della verifica di conformità al principio di sussidiarietà, dalla **Commissione Politiche dell'UE** che ha adottato, il 24 febbraio 2026, un [documento](#) recante una **valutazione conforme**.

Il regolamento introduce **alcune modifiche rilevanti** ai fini dell'attuazione dell'*AI Act*. In particolare, esso differisce al 2 dicembre 2027 l'applicazione degli obblighi previsti per determinate categorie di **sistemi di IA ad alto rischio**, disciplinati dal Capo III dell'*AI Act*, operanti in **settori particolarmente sensibili quali, tra gli altri, la biometria, la migrazione, l'asilo e la gestione delle frontiere**.

Il medesimo intervento normativo posticipa inoltre al **2 agosto 2027** il termine entro il quale gli Stati membri dovranno istituire gli spazi di sperimentazione normativa (*AI regulatory sandboxes*) previsti dall'*AI Act*. Viene altresì introdotta **una forma di coordinamento tra la valutazione d'impatto sui diritti fondamentali** richiesta dall'articolo 27 dell'*AI Act* per

i sistemi di IA ad alto rischio e gli adempimenti già previsti dalla normativa europea in materia di protezione dei dati personali, consentendo di fare riferimento, ove pertinente, alle valutazioni effettuate ai sensi del GDPR o della direttiva (UE) 2016/680.

Schede di lettura

TITOLO I - UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE PER L'ATTIVITÀ DI POLIZIA

CAPO I – DISPOSIZIONI GENERALI

Articolo 1 (Oggetto e finalità)

L'articolo 1 individua **oggetto e finalità** delle disposizioni in materia di **utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia**.

Preliminarmente, si evidenzia che il provvedimento in esame è adottato ai sensi dell'[articolo 24](#), commi 1, 2, lettera *h*), 3 e 5, della **legge n. 132 del 2025**, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, ai fini dell'adeguamento della normativa nazionale al [regolamento \(UE\) 2024/1689](#) (c.d. “AI Act” o “regolamento IA”) che stabilisce regole armonizzate sull'intelligenza artificiale.

Si rammenta che il regolamento (UE) 2024/1689 reca le definizioni di “autorità di contrasto” e di “attività di contrasto”, ossia le attività inerenti a prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. Il regolamento annovera tra i “sistemi ad alto rischio” quelli utilizzati per le suddette attività di contrasto. L'articolo 46 del regolamento prevede deroghe alla procedura di valutazione della conformità dei sistemi di IA ad alto rischio per l'utilizzo di tali sistemi da parte di autorità di contrasto o di protezione civile, salvo l'obbligo di autorizzazione durante o successivamente a tale utilizzo. Inoltre, l'articolo 5, paragrafo 1, lettera *h*), del medesimo regolamento prevede la possibilità di utilizzare sistemi di identificazione biometrica remota “in tempo reale”, altrimenti vietati, in spazi accessibili al pubblico a fini di attività di contrasto, a condizione che tale uso sia strettamente necessario per uno dei seguenti obiettivi:

- la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;
- la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;
- la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o

dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II¹, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Nello specifico, per attività di contrasto si intendono, ai sensi dell'articolo 3, numero 46), del regolamento IA, le attività svolte dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. Per ulteriori approfondimenti sul regolamento IA si rinvia al [dossier](#) relativo alla legge n. 132 del 2025.

In proposito, la legge n. 132 del 2025, all'articolo 24, comma 1, delega il Governo ad adottare, entro dodici mesi dalla data di entrata in vigore della stessa (10 ottobre 2025), uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento IA. Più nello specifico, il comma 2, lettera h), contempla, quale principio e criterio direttivo specifico cui il Governo è tenuto ad attenersi nell'esercizio della delega, in aggiunta ai principi e criteri direttivi generali di cui all'[articolo 32](#) della legge n. 234 del 2012, la previsione di un'apposita disciplina per l'**utilizzo di sistemi di intelligenza artificiale per l'attività di polizia**.

I principi e criteri direttivi indicati dal sopra citato articolo 32 sono, in estrema sintesi, i seguenti:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture, secondo il principio della massima semplificazione dei procedimenti;

b) ai fini di un migliore coordinamento con le discipline vigenti, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione della normativa;

c) gli atti di recepimento di direttive non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse (c.d. *gold plating*);

d) ove necessario, al fine di assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. In ogni caso le sanzioni penali sono previste "solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti";

¹ L'Allegato II indica i seguenti reati: terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei predetti reati.

e) al recepimento di direttive o di altri atti che modificano precedenti direttive o di atti già attuati con legge o con decreto legislativo si procede apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione;

f) nella redazione dei decreti legislativi si tiene conto delle eventuali modifiche delle direttive, intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano le procedure per salvaguardare l'unitarietà dei processi decisionali, l'efficacia e la trasparenza dell'azione amministrativa, nel rispetto dei principi di sussidiarietà e delle competenze delle regioni e degli enti territoriali;

h) le direttive che riguardano le stesse materie o che comportano modifiche degli stessi atti normativi vengono attuate con un unico decreto legislativo, compatibilmente con i diversi termini di recepimento;

i) è sempre assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.

L'articolo 24 reca, al comma 3, un'ulteriore delega al Governo, anch'essa esercitabile entro dodici mesi, per la definizione organica della disciplina dei casi di **realizzazione e di impiego illeciti di sistemi di intelligenza artificiale**, indicando, al comma 5, i seguenti principi e criteri direttivi:

a) previsione di strumenti, anche cautelari, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive;

b) introduzione di autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato;

c) precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente;

d) nei casi di responsabilità civile, previsione di 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 IA;

e) regolazione dell'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari, nel rispetto delle garanzie inerenti al diritto di difesa e

ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza;

f) modifica, a fini di coordinamento e di razionalizzazione del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle predette lettere.

Pertanto, con lo schema di decreto in esame si provvede a introdurre una specifica disciplina concernente l'utilizzo dei **sistemi di intelligenza artificiale** strumentale all'**attività di polizia** e, contestualmente, sia disposizioni penali – sostanziali e processuali – in materia di **realizzazione e impiego illeciti di sistemi IA**, sia disposizioni processuali civili relativamente al **risarcimento dei danni** derivanti dall'utilizzo di tali sistemi.

Ciò premesso, l'articolo in commento, al **comma 1**, definisce l'**ambito di applicazione** del Titolo I, specificando che le relative disposizioni concernono l'**utilizzo di sistemi di intelligenza artificiale** da parte degli organi, uffici e comandi delle **Forze di polizia**, con riferimento alle specifiche funzioni espletate, in conformità delle norme e dei principi del regolamento IA e della legge n. 132 del 2025.

Il **comma 2** richiede, nell'applicazione delle disposizioni di cui al Titolo I, il **rispetto dei diritti e delle libertà fondamentali** garantiti dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché dei **principi di proporzionalità, non discriminazione, sorveglianza umana e trasparenza**, già previsti dall'[articolo 3](#) della legge n. 132 del 2025.

Si segnala, in particolare, che l'articolo 3, al comma 1, prescrive che la ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengano nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

Il **comma 3** specifica, infine, che le disposizioni di cui al Titolo I **non determinano il sorgere di nuovi obblighi** rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi e i modelli di intelligenza artificiale utilizzati nelle attività e finalità di polizia.

Articolo 2 (Definizioni)

L'articolo 2 reca le **definizioni** necessarie all'applicazione del decreto in commento, rinviando, per quanto non espressamente previsto, alle definizioni indicate nella legge n. 132 del 2025 in materia di intelligenza artificiale e nel regolamento (UE) 2024/1689 (*AI Act*).

In particolare, al **comma 1**, sono elencate le seguenti definizioni:

- **regolamento IA:** si intende il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale;
- **legge IA:** si intende la legge n. 132 del 2025. recante disposizioni e deleghe al Governo in materia di intelligenza artificiale;
- **sistema di IA:** si intende un sistema di intelligenza artificiale automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali (articolo 3, punto 1), del regolamento IA);

Sul punto, si segnala che la Commissione europea, ai sensi dell'articolo 96, paragrafo 1, lettera f), del regolamento IA, ha elaborato, in data 29 luglio 2025, i propri [orientamenti sulla definizione di sistema di intelligenza artificiale](#) stabilita dal regolamento medesimo.

- **pratiche vietate:** consistono nelle pratiche di IA vietate a norma dell'articolo 5 del regolamento IA;

Ai sensi del sopra citato articolo 5, paragrafo 1, sono vietate le seguenti pratiche di IA:

a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;

b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o

economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo;

c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:

- un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

- un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

d) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa;

e) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;

f) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza;

g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto;

h) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

- la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

- la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

- la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Si evidenzia, inoltre, che la Commissione europea, sulla base di quanto disposto dall'articolo 96, paragrafo 1, lettera b), del regolamento IA ha elaborato, in data 29 luglio 2025, i propri [orientamenti in merito alle pratiche di intelligenza artificiale vietate](#) ai sensi del regolamento medesimo.

- **sistema di IA ad alto rischio:** è un sistema di IA classificato ad alto rischio, conformemente all'articolo 6 del regolamento IA in combinato disposto con il suo allegato III;

L'articolo 6 stabilisce che un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

- il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

- il prodotto, il cui componente di sicurezza di cui sopra è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.

Il medesimo articolo, al paragrafo 2, include tra i sistemi di IA ad alto rischio anche quelli indicati nell'[Allegato III](#). Nel rinviare a tale allegato per approfondimenti, si segnala che i settori in cui rientrano tali sistemi sono quelli riguardanti: la biometria; le infrastrutture critiche; l'istruzione e la formazione professionale; l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo; l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e la fruizione degli stessi; le attività di contrasto; la migrazione, l'asilo e la gestione del controllo delle frontiere; l'amministrazione della giustizia e i processi democratici.

- **categorie particolari di dati personali:** sono le categorie di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 3, punto 37), del regolamento IA);
- **dati relativi a condanne penali e reati:** sono i dati personali di cui all'articolo 10 del regolamento (UE) 2016/679;

A tale proposito si ricorda che il trattamento di tali dati deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

- **dati operativi sensibili:** rappresentano i dati relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali (articolo 3, punto 38), del regolamento IA);
- **output:** sono previsioni, contenuti, raccomandazioni o decisioni generate da un sistema di IA;
- **scraping non mirato:** consiste nell'estrazione e nella raccolta automatizzata e indiscriminata, su larga scala, mediante l'utilizzo di un sistema di intelligenza artificiale, di immagini facciali dalla rete *internet* o da filmati di telecamere a circuito chiuso, allo scopo di creare o ampliare banche dati di riconoscimento facciale;
- **Autorità nazionali per l'intelligenza artificiale:** sono l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN), ai sensi dell'articolo 20, comma 1, della legge n. 132 del 2025;
- **Garante:** è il Garante per la protezione dei dati personali, istituito dal decreto legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali);
- **Forze di polizia:** sono le Forze di polizia di cui all'articolo 16 della legge n. 121 del 1981 ("Nuovo ordinamento dell'Amministrazione della pubblica sicurezza"), ovvero l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza, il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica e, fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, il Corpo di polizia penitenziaria e il Corpo forestale dello Stato (questi ultimi possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica);

Con riferimento al Corpo forestale dello Stato, si ricorda che, per effetto del decreto legislativo n. 177 del 2016 ("Disposizioni in materia di razionalizzazione delle funzioni di polizia e assorbimento del Corpo forestale dello Stato, ai sensi dell'articolo 8, comma 1, lettera a), della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"), il Corpo è oggi confluito nell'Arma dei carabinieri.

- **attività di polizia:** consistono nelle attività di contrasto, ovvero quelle attività svolte, nell'esercizio delle rispettive attribuzioni e funzioni, dagli organi, uffici e comandi delle Forze di polizia a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni

penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse (articolo 3, punto 46), del regolamento IA);

- **finalità di polizia:** rappresentano gli obiettivi di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse e per i quali sono svolte le suddette attività di polizia (articolo 3, punti 45)² e 46), del regolamento IA).

Si segnala che la lettera *q*) dell'articolo 2, recante la definizione di “finalità di polizia”, opera un rinvio alle “attività di polizia di cui alla lettera *s*)” del medesimo articolo. Tuttavia, la definizione di “attività di polizia” non è contenuta nella lettera *s*), bensì nella lettera *p*) dell'articolo 2.

Si valuti l'opportunità di un coordinamento.

Il **comma 2** stabilisce che per le **definizioni non riportate** nel presente articolo si rinvia a quelle contenute nell'[articolo 2](#) della legge n. 132 del 2025 e nell'[articolo 3](#) del regolamento IA.

² Il punto 45) dell'articolo 3 del regolamento IA, riferendosi alle finalità richiamate nel testo, definisce come “**autorità di contrasto**” “qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse”

**CAPO II – DISPOSIZIONI IN MATERIA DI RICERCA, SVILUPPO,
ADDESTRAMENTO, FORMAZIONE, SPERIMENTAZIONE E UTILIZZO DEI
SISTEMI DI INTELLIGENZA ARTIFICIALE NELLE ATTIVITÀ 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 individua i **criteri generali per l'utilizzo di sistemi e modelli di intelligenza artificiale** nelle attività di polizia. Tra le altre cose, si prevede che l'utilizzo dei sistemi e dei modelli di intelligenza artificiale 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

Preliminarmente, per quanto concerne la definizione di “**Forze di polizia**” recata dal provvedimento in esame, si rinvia all'approfondimento contenuto nella scheda relativa all'articolo 2.

Più nel dettaglio, poi, il **comma 1** prevede che la **ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione, la convalida e l'utilizzo di sistemi e modelli di intelligenza artificiale (IA)** per le attività e le finalità delle forze di polizia avvengono:

- nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione;
- nel rispetto del diritto dell'Unione europea;
- nel rispetto dei principi di cui all'articolo 3 della legge n. 132 del 2025 in materia di intelligenza artificiale;

Il richiamato articolo 3 individua principi generali in materia di utilizzo dell'intelligenza artificiale; tra questi, merita richiamare i principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, non discriminazione, parità dei sessi e sostenibilità; inoltre lo sviluppo di sistemi e modelli di intelligenza artificiale deve avvenire su dati e tramite processi di cui devono essere garantite e vigilate correttezza, attendibilità, sicurezza e qualità e devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo; infine, l'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale

e politica e deve essere garantito alle persone con disabilità il pieno accesso ai sistemi di intelligenza artificiale, su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio.

- secondo un approccio antropocentrico, proporzionato e fondato sul rischio, che tenga conto della classificazione dei sistemi di IA e delle diverse categorie di interessati.

Il **comma 2** indica le **finalità** delle attività di ricerca, sperimentazione, sviluppo e addestramento dei sistemi di intelligenza artificiale. Queste infatti devono essere orientate al **perseguimento della funzionalità e dell'affidabilità operativa dei sistemi e dei modelli di IA** destinati ad essere utilizzati dalle forze di polizia. Ciò nella prospettiva di migliorare l'apporto tecnologico dell'intelligenza artificiale alle valutazioni e alle decisioni umane nella relativa attività.

Il **comma 3** si sofferma sulle **modalità di utilizzo** dei sistemi e dei modelli di intelligenza artificiale e dei relativi *output* da parte delle Forze di polizia. Questo dovrà avvenire in conformità con l'assetto istituzionale vigente e nell'ambito delle proprie competenze. L'utilizzo dovrà poi essere in funzione strumentale e di **supporto alle relative attività di polizia**, allo scopo di incrementarne l'efficacia e l'efficienza.

Il **comma 4** dispone che l'utilizzo dei sistemi e dei modelli di intelligenza artificiale 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, nel **rispetto dell'autonomia e delle sfere di competenza** dei procedimenti decisionali degli appartenenti alle Forze di polizia. La revisione è effettuata da personale individuato dalle procedure interne di ciascuna forza di polizia ed è documentata in modo da assicurarne la tracciabilità.

Ciò conformemente agli obblighi stabiliti dal regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale.

In base al **comma 5**, le Forze di polizia devono assicurare che per i **sistemi di IA ad alto rischio**:

- la **sorveglianza umana** sia effettiva e conforme a quanto previsto dall'articolo 14 del regolamento (UE) 2024/1689;

tale articolo fissa, tra le altre cose, proprio il principio generale che i sistemi di IA ad alto rischio siano progettati e sviluppati, anche con

strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso; ciò significa che le persone fisiche alle quali è affidata la sorveglianza umana devono avere la possibilità, ove opportuno e proporzionato, a) di comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) di essere consapevoli della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;

d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.

- il **personale** preposto possieda **formazione e necessarie competenze** per prevenire e **ridurre al minimo i rischi** per la salute, la sicurezza e i diritti fondamentali.

Si ricorda che l'articolo 6 del regolamento (UE) 2024/1689 prevede che un sistema di IA sia considerato ad **alto rischio** se utilizzato come componente di sicurezza di un prodotto, o se è esso stesso un prodotto utilizzato nei settori oggetto delle norme di armonizzazione tecnica UE richiamate nell'allegato I del regolamento (tra questi macchine, sicurezza dei giocattoli, imbarcazioni da diporto e moto d'acqua, ascensori, apparecchi potenzialmente esplosivi in atmosfera, apparecchiature radio, impianti a fune, dispositivi di protezione personale, dispositivi medico-diagnostici *in vitro*, sicurezza aviazione civile, omologazione veicoli a motore e veicoli agricoli, equipaggiamento marittimo e interoperabilità sistema ferroviario). Sono inoltre comunque considerati sistemi di IA ad alto rischio quelli inclusi nell'allegato III del regolamento e cioè, tra gli altri, quelli che operano nel settore della biometria (fatta eccezione per quelli la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere); quelli destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli e quelli

destinati a essere utilizzati per valutare i risultati dell'apprendimento; quelli destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche e per adottare decisioni riguardanti le condizioni dei rapporti di lavoro; quelli utilizzati per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria; quelli utilizzati per valutare l'affidabilità creditizia delle persone fisiche; quelli destinati a essere utilizzati per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge; quelli destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum (con esclusione dei sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico); quelli destinati ad essere utilizzati dalle competenti autorità per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro e per l'esame delle domande di asilo, di visto o di permesso di soggiorno.

Il **comma 6** disciplina il **trattamento dei dati personali** nelle attività di ricerca, sperimentazione, sviluppo, addestramento, adozione, applicazione, convalida e di utilizzo di sistemi e modelli di intelligenza artificiale per le attività e le finalità delle Forze di polizia. In primo luogo, si specifica che tali dati includono anche le **“categorie particolari di dati personali”**, i **“dati operativi sensibili”** e i **“dati relativi a condanne penali e reati”** nella disponibilità delle forze di polizia in forza di disposizioni legislative o regolamentari ovvero di atti amministrativi generali.

Si segnala che:

- le “categorie particolari di dati personali” sono definiti dall'articolo 3, paragrafo 1, numero 37 del regolamento (UE) 2024/1689 come le categorie di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (di cui all'articolo 9 del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10 del regolamento (UE) 2018/1725),
- i “dati operativi sensibili” sono definiti dall'articolo 3, paragrafo 1, numero 38, del regolamento (UE) 2024/1689 come i “dati operativi relativi ad attività di prevenzione, accertamento, indagine o

perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali”;

- gli atti amministrativi generali si collocano in una posizione intermedia nella tripartizione classica degli atti della pubblica amministrazione, tra gli atti normativi (i regolamenti) e i provvedimenti amministrativi in senso stretto. Tale tipologia di atti si connota per la generalità dei destinatari (non necessariamente determinati nell'atto stesso, ma determinabili *ex post*) e la loro inidoneità ad essere applicati a una serie ripetuta di casi, esaurendosi la loro portata con un'unica applicazione. Rientrano tradizionalmente in questa categoria i bandi di concorso e di gara, gli atti di approvazione di tariffe e prezzi, i piani, i programmi, le autorizzazioni generali, ecc. La categorizzazione degli atti amministrativi generali non è meramente teorica, poiché ne discende un regime giuridico differenziato. Tali atti, infatti, soggiacciono a un regime giuridico parzialmente in deroga a quello proprio dei provvedimenti amministrativi in senso stretto. In particolare, la legge n. 241 del 1990, infatti, esonera gli atti amministrativi generali dall'obbligo generale di motivazione (articolo 3, comma 2); li sottrae alle garanzie partecipative - comunicazione di avvio del procedimento, intervento degli interessati, presentazione di memorie e documenti – (articolo 13, comma 1); l'attività dell'amministrazione diretta alla loro emanazione è esclusa dal diritto di accesso (articolo 24, comma 1, lettera c)).

Ciò premesso, il trattamento dei dati personali deve avvenire nel rispetto della normativa contenuta nel decreto legislativo n. 51 del 2018 (che ha attuato l'ultima direttiva UE in materia, la 2016/680). Questo fermo restando:

- le specifiche disposizioni dettate dal Regolamento (UE) 2024/1689 per i sistemi ad alto rischio, già sopra richiamati;
- le prescrizioni contenute nel Capo III con riferimento ai 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 ai fini di contrasto dei reati (articoli da 7 a 10, per i quali si rinvia alle relative schede di lettura).

Il **comma 7**, infine, stabilisce che le attività di cui all'articolo in commento siano comunque svolte senza nuovi obblighi rispetto a quanto stabilito dal regolamento (UE) 2024/1689 e tenendo conto delle esclusioni previste dal medesimo regolamento.

Si ricorda che l'articolo 2 del regolamento esclude dall'ambito di applicazione, tra gli altri, i sistemi di IA per scopi militari, di difesa o di

sicurezza nazionale ovvero quelli messi in servizio al solo scopo di ricerca e sviluppo scientifico.

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 consente alle **Forze di polizia** di attivare **collaborazioni** con **università ed enti di ricerca** finalizzate alla realizzazione di **progetti di intelligenza artificiale** utilizzabili per le **attività di polizia**.

Il **comma 1**, prevede che le **Forze di polizia** possano instaurare forme di **collaborazione** con università, enti di ricerca e altri soggetti pubblici o privati, per la realizzazione di **progetti di ricerca e sperimentazione scientifica**, finalizzati alla creazione di **sistemi di intelligenza artificiale** o di dispositivi che utilizzano tecnologie di IA per le **attività di polizia**.

Per attività di polizia si intendono – come riportato dall'articolo 2, comma 1, lettera r), del provvedimento in esame - le attività di contrasto svolte, nell'esercizio delle rispettive attribuzioni e funzioni, dagli organi, uffici e comandi delle Forze di polizia. Le attività di contrasto sono le attività svolte a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse (articolo 3, punto 46), del regolamento (UE) 1689/2024).

Si evidenzia, in proposito, che la relazione illustrativa specifica che tra i suddetti progetti sono inclusi anche lo sviluppo, l'addestramento e la convalida di sistemi, modelli o dispositivi di intelligenza artificiale.

Tra i soggetti con cui possono essere attivate tali collaborazioni sono incluse le società **in house** o a **totale partecipazione pubblica**.

La relazione illustrativa osserva come la disposizione in esame favorisca l'innovazione attraverso partenariati, ponendo, tuttavia, dei limiti su dati operativi sensibili e proprietà dei modelli, evitando esternalizzazioni incontrollate di *asset* critici.

Per quanto riguarda le società *in house*, si ricorda quanto previsto dall'art. 7 del Codice dei contratti (D.Lgs. 36/2023): «Le pubbliche amministrazioni organizzano autonomamente l'esecuzione di lavori o la prestazione di beni e servizi attraverso l'autoproduzione, l'esternalizzazione e la cooperazione nel rispetto della disciplina del codice e del diritto dell'Unione europea». Ai sensi del comma 2 della stessa disposizione «Le stazioni appaltanti e gli enti concedenti possono affidare direttamente a società *in house* lavori, servizi o forniture, nel rispetto dei principi di cui agli articoli 1, 2 e 3» sulla base di un provvedimento

motivato nei termini indicati dalla norma. Si richiama inoltre l'Allegato I.1, del D.Lgs. 36/2023 che, all'art. 3, comma 1, lett. *e*), definisce l'affidamento *in house* come «l'affidamento di un contratto di appalto o di concessione effettuato direttamente a una persona giuridica di diritto pubblico o di diritto privato definita dall'articolo 2, comma 1, lettera *o*), del testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo 19 agosto 2016, n. 175 e alle condizioni rispettivamente indicate dall'articolo 12, paragrafi 1, 2 e 3, della direttiva 24/2014/UE e dall'articolo 17, paragrafi 1, 2 e 3 della direttiva 23/2014/UE, nonché, per i settori speciali, dall'articolo 28, paragrafi 1, 2 e 3, della direttiva 24/2014/UE». (fonte: Autorità nazionale anticorruzione, [Parere funzione consultiva n. 3 del 24 marzo 2026](#)).

Viene specificato, inoltre, che devono essere rispettate le regole dell'Unione europea in materia di concorrenza e **aiuti di Stato**.

A tale proposito, si ricorda che l'articolo 107, paragrafo 1, del Trattato sul funzionamento dell'Unione europea - TFUE prevede che, salvo deroghe contemplate dai Trattati, siano incompatibili con il mercato interno, nella misura in cui incidono sugli scambi tra Stati membri, gli aiuti concessi sotto qualsiasi forma dagli Stati, ovvero mediante fondi pubblici, che, favorendo talune imprese o talune produzioni, falsino o minaccino di falsare la concorrenza. Si rinvia, per approfondimenti ulteriori, al dossier del Servizio Studi della Camera - [Parte generale](#) e [Parte speciale](#).

Al riguardo, si segnala che la Direzione centrale per la Polizia scientifica e la sicurezza cibernetica del Dipartimento della pubblica sicurezza e l'università di Bari hanno sottoscritto un [protocollo d'intesa](#) finalizzato a rafforzare la collaborazione istituzionale nei settori della sicurezza informatica, della prevenzione dei reati digitali e della ricerca scientifica avanzata. Il protocollo prevede, tra l'altro, lo sviluppo di progetti innovativi nei campi della cybersecurity, e dell'intelligenza artificiale.

Il **comma 2** impone il rispetto della normativa in materia di **protezione dei dati personali** nello svolgimento dell'attività di trattamento di dati nell'ambito dei suddetti progetti di ricerca e sperimentazione scientifica.

In particolare, gli accordi di collaborazione con università ed enti di ricerca devono contenere apposite clausole che **escludano la condivisione** di dati operativi sensibili e l'**acquisizione** o l'**utilizzo, anche indirette**, da parte dei soggetti con i quali sono attivate le collaborazioni, **per finalità commerciali o per altre finalità** non previste dalle predette collaborazioni, di sistemi di IA e delle relative risorse *hardware* e *software* o di dispositivi integrati con componenti di IA che siano stati addestrati per l'attività di polizia.

Il **comma 3** prescrive, inoltre, che i rapporti di collaborazione disciplinino espressamente la **titolarità dei diritti di proprietà intellettuale, industriale** e di **sfruttamento economico** dei risultati della ricerca, dei modelli derivati, dei dati di addestramento e del *software*. Tali accordi dovranno rispettare:

- il codice della proprietà industriale (decreto legislativo n. 30 del 2005);
- l'articolo 64 del decreto del Presidente della Repubblica n. 382 del 1980, che impone l'obbligo di trasmettere all'[Anagrafe nazionale delle ricerche](#) tutte le notizie relative alle ricerche comunque finanziate, in tutto o in parte, con fondi a carico del bilancio dello Stato o di bilanci di enti pubblici;
- la normativa di settore applicabile.

La disposizione richiede, infine, che sia, in ogni caso, garantita 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 negli spazi di sperimentazione normativa)

L'articolo 5 disciplina la partecipazione delle **Forze di polizia** agli **spazi di sperimentazione normativa per l'intelligenza artificiale**, individuando la base giuridica per il trattamento dei dati personali necessario per le **finalità di polizia**. Il trattamento può riguardare anche dati relativi a reati e categorie particolari di dati personali. La partecipazione a tali spazi è finalizzata allo **sviluppo**, alla **realizzazione** e alla **prova di sistemi di IA** destinati alle **attività di polizia**, in particolare se classificati ad **alto rischio**. La sperimentazione deve svolgersi nel rispetto della protezione dei dati personali nonché delle condizioni previste dalla normativa europea, prevedendo il **raccordo con le Autorità nazionali per l'intelligenza artificiale**. Si demanda a un **decreto del Presidente del Consiglio dei ministri** la definizione delle modalità di coordinamento con lo spazio di sperimentazione previsto dal regolamento IA.

Il **comma 1** individua l'articolo in esame quale **base giuridica per il trattamento di dati personali** effettuato dalle Forze di polizia nell'ambito di **spazi di sperimentazione normativa per l'intelligenza artificiale**, quando tale trattamento è necessario per **finalità di polizia**.

La disposizione precisa che in tale trattamento sono inclusi i dati relativi a reati e le categorie particolari di dati di cui all'articolo 3, punto 37), del regolamento (UE) 2024/1689 (cosiddetto **regolamento IA**).

Secondo quanto previsto all'articolo 3, punto 55, del regolamento IA, per "**spazio di sperimentazione normativa per l'IA**", si intende un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare. Il "**piano dello spazio di sperimentazione**" è invece "un documento concordato tra il fornitore partecipante e l'autorità competente in cui sono descritti gli obiettivi, le condizioni, il calendario, la metodologia e i requisiti relativamente alle attività svolte all'interno dello spazio di sperimentazione" (articolo 3, punto 54), del regolamento IA).

Con riferimento alla **base giuridica**, si ricorda che il regolamento IA, all'articolo 59, paragrafo 2, impone che – a fini di prevenzione, indagine,

accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità di contrasto – il trattamento dei dati personali negli spazi di sperimentazione normativa per l’IA si basa su una specifica disposizione di diritto nazionale o dell’Unione. L’articolo 5 in esame assolve, pertanto, proprio alla funzione di individuare tale base giuridica interna, in combinato disposto con l’articolo 5 del **decreto legislativo n. 51 del 2018**. Quest’ultima disposizione sancisce la liceità del trattamento dei dati quando esso è necessario per l’esecuzione di un compito di un’autorità competente per determinate finalità³ e si basa sul diritto dell’Unione europea o su disposizioni di legge o di regolamento o su atti amministrativi generali che individuano i dati personali e le finalità del trattamento.

Si ricorda che l’articolo 2, comma 1, lettera o), del presente provvedimento, intende per **Forze di polizia** quelle di cui all’articolo 16 della legge n. 121 del 1981 (si rinvia alla scheda dell’articolo 2 per approfondimenti).

Si rinvia alla scheda relativa all’articolo 2 anche per quanto riguarda le definizioni di **finalità di polizia**, di **dati relativi a reati** e di **categorie particolari di dati personali**.

Il **comma 2** specifica che la partecipazione delle Forze di polizia agli spazi di sperimentazione normativa per l’intelligenza artificiale è finalizzata allo **sviluppo, alla realizzazione e alla prova** di sistemi di intelligenza artificiale, **specialmente ad alto rischio**, destinati alle attività di polizia, nel rispetto della protezione dei dati personali e della **tutela dei diritti e delle libertà fondamentali**.

Per le definizioni di sistema di intelligenza artificiale, nonché di sistema di IA ad alto rischio, si rinvia alla scheda di approfondimento dell’articolo 2 del provvedimento in esame.

Il **comma 3** sancisce che, negli spazi di sperimentazione normativa per l’intelligenza artificiale, la sperimentazione avviene nel **rispetto cumulativo di determinate condizioni** (*ex* articolo 59, paragrafo 1, del regolamento IA).

Ai sensi della disposizione appena richiamata, tali condizioni prevedono quanto segue:

- i sistemi di IA sono sviluppati per salvaguardare un interesse pubblico rilevante da parte di un’autorità pubblica o di un’altra persona fisica o giuridica e in uno o più dei settori seguenti:

³ Si tratta delle finalità indicate al comma 2 dell’articolo 1 dello stesso decreto n. 51 del 2018, ossia: prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

- la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari;
 - un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la tutela della biodiversità, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi;
 - la sostenibilità energetica;
 - la sicurezza e la resilienza dei sistemi di trasporto e della mobilità, delle infrastrutture critiche e delle reti;
 - l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici;
- i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui alla sezione 2 del capo III del medesimo regolamento IA (relativo ai requisiti per i sistemi di IA ad alto rischio) qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali;
 - esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 (disposizioni in materia di valutazione d'impatto sulla protezione dei dati) durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento;
 - i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati;
 - i fornitori possono condividere ulteriormente i dati originariamente raccolti solo in conformità del diritto dell'Unione in materia di protezione dei dati; i dati personali creati nello spazio di sperimentazione non possono essere condivisi al di fuori dello spazio di sperimentazione;
 - il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati né incide sull'applicazione dei loro diritti sanciti dal diritto dell'Unione in materia di protezione dei dati personali;
 - i dati personali trattati nell'ambito dello spazio di sperimentazione sono protetti mediante adeguate misure tecniche e organizzative e cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali;
 - i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione, salvo diversa disposizione del diritto dell'Unione o nazionale;

- una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica indicata all'allegato IV del medesimo regolamento IA;
- una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito *web* delle autorità competenti; tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

La disposizione in esame, inoltre, impone che la sperimentazione sia oggetto di **collaborazione e raccordo** con le **Autorità nazionali per l'intelligenza artificiale**, fermo restando la tutela dei dati operativi sensibili e l'esclusiva titolarità e responsabilità del trattamento degli stessi da parte delle amministrazioni competenti.

L'articolo 2, comma 1, lettera *m*), del presente provvedimento, nel rinviare all'articolo 20, comma 1, della legge n. 132 del 2025, definisce quali "**Autorità nazionali per l'intelligenza artificiale**", l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN). La lettera *h*) del medesimo comma indica come **dati operativi sensibili**, per effetto di un rinvio normativo all'articolo 3, punto 38), del regolamento IA, i dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali.

Il **comma 4** demanda a un **regolamento** dell'esecutivo la definizione delle **modalità di coordinamento** tra lo spazio di sperimentazione normativa per l'IA ex articolo 57 del regolamento IA e la sperimentazione di sistemi di IA per le finalità di polizia di cui all'articolo in commento.

La disposizione, richiamando anche l'articolo 17, comma 3, della legge n. 400 del 1988 in materia di regolamenti ministeriali (che impone che tali regolamenti siano adottati solo allorché la legge conferisca il relativo potere e che gli stessi non possano dettare norme contrarie a quelle contenute nei regolamenti del Governo), prevede che il regolamento sia adottato con **decreto del Presidente del Consiglio dei ministri, su proposta delle Autorità nazionali per l'intelligenza artificiale (AgID e ACN), di concerto con il Ministro dell'interno**.

Infine, si ricorda che la disciplina dei regolamenti di cui all'articolo 17, comma 3, della legge n. 400 del 1988, richiamata dalla norma in commento, prevede, secondo quanto precisato dal comma 4 del medesimo articolo, che essi:

- rechino la denominazione "regolamento";

- siano adottati previo parere del Consiglio di Stato;
- siano sottoposti al visto ed alla registrazione della Corte dei conti;
- siano pubblicati nella Gazzetta Ufficiale.

• *Sviluppo, modifica, test e convalida di strumenti algoritmici, sistemi e modelli di IA nell'ambito della nuova proposta di regolamento Europol*

Lo **sviluppo** e l'**impiego di strumenti di IA** nell'azione di contrasto alla criminalità, specialmente organizzata e transfrontaliera, costituisce uno dei **punti qualificanti** della nuova [proposta](#) di regolamento relativa ad **Europol**, l'Agenzia dell'UE per la cooperazione nell'attività di contrasto. La proposta – che interviene a breve distanza dall'adozione del [regolamento](#) UE 2025/2611 di riforma del quadro giuridico di Europol – punta a rafforzare ulteriormente il mandato dell'Agenzia, potenziandone l'azione quale polo **informativo, operativo** nonché come **centro tecnologico** e dell'**innovazione**, affinché vengano messe a disposizione degli Stati membri **capacità avanzate, competenze specialistiche e strumenti operativi**.

In quest'ottica l'**art. 61** della proposta disciplina, in particolare, l'**utilizzo** da parte di Europol di un **ambiente di sviluppo e sperimentazione**, che deve essere conforme ai requisiti della “*sandbox* regolatorie” ex art. 57 dell'AI Act. Stando alla nuova proposta, Europol potrebbe quindi servirsi di un ambiente tecnico separato, isolato e protetto per **sviluppare, modificare sostanzialmente, testare, convalidare e addestrare**, tra l'altro, **sistemi e modelli di IA** e altre tecnologie avanzate.

A completamento del quadro, l'art. 64 prevede che Europol **sostenga** gli Stati membri sia nel **rafforzamento delle competenze specialistiche** sia nell'**impiego** efficace delle **capacità avanzate condivise**, sviluppate sia sul versante delle **tecnologie emergenti** – compresa l'intelligenza artificiale, le indagini digitali, l'*intelligence open-source* e la decrittazione e il trattamento dei dati – sia su quello delle **metodologie operative** rilevanti per la **cooperazione transfrontaliera** delle autorità di contrasto, compresi i metodi di prevenzione della criminalità e le procedure investigative.

Articolo 6 (Formazione del personale di polizia)

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.

La disposizione enumera i "risultati formativi minimi" che i corsi debbono assicurare.

L'**articolo 6, comma 1**, stabilisce che le Forze di Polizia attivino specifici **corsi in materia di intelligenza artificiale applicata all'attività di polizia**.

Lo svolgimento dei corsi avviene secondo modalità stabilite dagli istituti di istruzione e formazione.

Dal punto di vista finanziario, per l'espletamento dei corsi formativi si ricorre alle **risorse disponibili a legislazione vigente** senza maggiori oneri per la finanza pubblica.

Il successivo **comma 2** dispone che tali corsi assicurino alle Forze di polizia il raggiungimento di **risultati formativi minimi**, nel rispetto dell'articolo 4 del [regolamento IA](#).

L'articolo 4 del Regolamento europeo n. 1689/2024 (cd. *AI Act*) mira a garantire un adeguato livello di alfabetizzazione in materia di Intelligenza Artificiale in favore di tutti coloro che, a vario titolo e per diversi fini, utilizzino i sistemi di IA.

La disposizione stila l'elenco degli obiettivi da raggiungere e delle conoscenze da acquisire per coloro che frequentino i corsi di formazione.

Gli agenti sono istruiti sul **funzionamento**, sulle **potenzialità**, sui **limiti**, sugli **errori** dei sistemi dell'intelligenza artificiale (**lettere a e b**). Particolare attenzione è riservata ai sistemi di **riconoscimento biometrico** e di **analisi predittiva**, ai fini delle attività poliziesche.

Altre finalità dei corsi attengono all'**interpretazione critica** degli *output* (**lettera c**) e alla conoscenza delle **implicazioni giuridiche, etiche e di responsabilità** connesse all'utilizzo dei sistemi di IA ai fini di polizia (**lettera d**).

Relativamente a quest'ultimo tema, la disposizione fa specifico riferimento al regolamento IA, al [regolamento europeo n. 679/2016](#) e al [decreto legislativo n. 51/2018](#).

Il Regolamento europeo n. 679/2016, meglio noto come *GDPR (General Data Protection Regulation)*, è stato adottato al fine di garantire la protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati in tutta l'Unione europea. Il presente regolamento ha profondamente modificato il [decreto legislativo n. 196/2003](#) (cd. Codice della Privacy), ovvero la normativa nazionale in materia di *privacy* e protezione dei dati personali.

Il Decreto legislativo n. 51/2018 recepisce nell'ordinamento italiano la [direttiva europea n. 680/2016](#) che disciplina la protezione dei dati personali trattati da autorità giudiziarie, di polizia e penitenziarie.

Un ulteriore obiettivo formativo che si intende perseguire, attraverso la partecipazione ai corsi di formazione, concerne la consapevolezza dei **rischi di cybersicurezza** connessi ai sistemi di intelligenza artificiale.

Per fronteggiare tali situazioni aleatorie, si seguono anche le indicazioni fornite dall'Agenzia per la cybersicurezza nazionale (ACN) (**lettera e**).

Il **comma 3** precisa che taluni risultati formativi, relativi agli errori dei sistemi di IA, all'interpretazione degli *output* e ai rischi di cybersicurezza, debbano essere garantiti nell'ambito di **corsi specifici circa i sistemi di IA**, classificati **ad alto rischio** dall'articolo 6 del regolamento IA, in uso nelle attività di polizia.

L'articolo 6 del regolamento IA prevede che un sistema di IA sia da considerarsi ad alto rischio nel caso in cui soddisfi, contemporaneamente, le seguenti condizioni:

- il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;
- il prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto, ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.

**CAPO III – SISTEMI DI INTELLIGENZA ARTIFICIALE UTILIZZATI
NELLE 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**

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 per **finalità di polizia**.

Preliminarmente, si ricorda che l’**articolo 5, paragrafo 1, lettera g)**, del regolamento (UE) 2024/1689 include tra le **pratiche di IA vietate** l’immissione sul mercato, la messa in servizio per tale finalità specifica o l’uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro **dati biometrici** al fine di trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale. Tale divieto non comprende l’**etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente**, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto.

Si ricorda, in proposito, che per dati biometrici si intendono - secondo la definizione recata dall’articolo 4, n. 14, del regolamento (UE) 2016/679, nonché dall’articolo 3, n. 13, della direttiva (UE) 2016/680 - i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici.

Ciò premesso, il **comma 1** dell’articolo in commento, in conformità a quanto disposto dal sopra citato articolo 5, paragrafo 1, lettera g), consente, nello svolgimento dell’**attività di polizia, l’etichettatura, il filtraggio o la categorizzazione** di set di dati biometrici acquisiti in conformità alla normativa vigente, purché:

- **non siano finalizzati** a trarre inferenze o deduzioni in merito a **razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale** delle persone fisiche;
- siano **strumentali ad attività di comparazione o ricerca**, ovvero ad altre attività comunque espletate nel rispetto delle norme vigenti ed esclusivamente per **finalità di polizia**;
- **non rappresentino l'unico fondamento** di decisioni che determinano effetti giuridici nei confronti di persone fisiche;
- il titolare del trattamento adotti **misure idonee a prevenire il reimpiego dei dati e dei risultati** per finalità incompatibili con quelle per cui sono stati raccolti.

Il **comma 2** stabilisce che il **trattamento dei dati personali** tramite le attività di etichettatura, filtraggio e categorizzazione di dati biometrici per finalità di polizia deve considerare, ai fini dell'adempimento degli obblighi determinati dal regolamento IA, la **classificazione dei sistemi di IA**, anche con riferimento agli orientamenti della Commissione europea sull'attuazione pratica del medesimo regolamento. La disposizione richiede, inoltre, che il predetto trattamento sia svolto in conformità del [decreto legislativo n. 51 del 2018](#).

Si ricorda, in proposito, che, ai sensi del combinato disposto degli articoli 6, paragrafo 5, e 96 del regolamento (UE) 2024/1689 la Commissione europea ha elaborato, in data 19 maggio 2026, un [progetto di orientamenti](#) sulla classificazione dei sistemi di IA ad alto rischio, avvalendosi dei riscontri ottenuti attraverso una consultazione pubblica con diversi portatori di interessi e dei contributi forniti dagli Stati membri attraverso il comitato per l'IA. Tale progetto è prodromico agli orientamenti definitivi della Commissione che mirano a sostenere i fornitori e gli operatori di sistemi di IA, nonché le autorità di vigilanza del mercato competenti, nel valutare se un sistema di IA debba essere classificato come ad alto rischio, facilitando in tal modo l'applicazione uniforme e l'effettiva applicazione dell'articolo 6 del regolamento IA.

Si segnala, inoltre, che il citato decreto legislativo n. 51 del 2018 reca disposizioni volte all'attuazione della [direttiva \(UE\) 2016/680](#), relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Esso si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti 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. In particolare, l'articolo 15 del decreto prevede che il titolare del trattamento, tenuto

conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate al fine di garantire che il trattamento sia effettuato in conformità alle disposizioni del decreto medesimo. Tali misure, ove necessario, sono oggetto di riesame e aggiornamento e, se risulta proporzionato rispetto all'attività di trattamento, includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

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 8 individua i casi e le condizioni in cui le **Forze di polizia** possono utilizzare **sistemi di intelligenza artificiale per l'identificazione biometrica remota «in tempo reale»** in spazi pubblici o aperti al pubblico.

La disposizione attua la delega contenuta nell'articolo 24, comma 2, lettera *h*) della legge 23 settembre 2025, n. 132 (legge sull'intelligenza artificiale), che demanda al Governo la previsione di «un'apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia».

Il **comma 1** definisce l'ambito oggettivo dell'impiego, riservandolo agli organi, uffici e comandi delle **Forze di polizia**. L'utilizzo è ammesso per le **finalità di prevenzione** di cui all'articolo 5, paragrafo 1, lettera *h*), punto ii), del regolamento IA, vale a dire la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone, ovvero di una minaccia, reale e attuale o reale e prevedibile, di attacco terroristico; nonché, altresì, per la **ricerca** di una persona scomparsa o di vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale, ai sensi del punto i) della medesima lettera *h*)⁴.

La disposizione fa salvo quanto previsto dall'articolo 359-ter del codice di procedura penale, così distinguendo l'uso a fini di prevenzione, qui disciplinato, dall'uso a fini di accertamento del reato in sede di indagine.

Il nuovo articolo 359-ter del codice di procedura penale, introdotto dallo schema di decreto in esame (v. scheda di lettura art. 13, *infra*) rimette l'autorizzazione sull'utilizzo di sistemi di intelligenza artificiale a fini di accertamento del reato in sede di indagine al giudice per le indagini preliminari su richiesta del pubblico ministero.

⁴ L'articolo 5, paragrafo 1, lettera *h*), del regolamento (UE) 2024/1689 vieta, in via di principio, l'identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, ammettendola in tre soli casi: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone, o di una minaccia, reale e attuale o reale e prevedibile, di attacco terroristico; iii) la localizzazione o l'identificazione di un indiziato, a fini di indagine o azione penale o di esecuzione della pena, per i reati elencati nell'allegato II e puniti con pena o misura privativa della libertà di durata massima non inferiore a quattro anni. L'articolo in commento recepisce i punti i) e ii).

Il **comma 2** circoscrive l'uso alla sola **conferma dell'identità** delle persone specificamente interessate, ovvero alla **ricerca mirata**, anche in modo dinamico e comprensiva della localizzazione, di **persone specificamente individuate** o individuabili in relazione alla minaccia da prevenire o alla ricerca da eseguire.

Il **comma 3** disciplina la **banca dati di riferimento**: il confronto biometrico avviene esclusivamente con un archivio adeguato a ciascuna finalità, derivabile da banche dati già in uso alle Forze di polizia o ad esse accessibili, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'attività di polizia.

È in ogni caso **vietato l'uso di banche dati alimentate**, in tutto o in parte, **mediante tecniche di scraping non mirato** (sulla definizione si *scraping* non mirato si veda la scheda di lettura dell'art. 2, *supra*), ovvero costituite in violazione della disciplina vigente in materia di protezione dei dati personali.

Il **comma 4** individua il **procedimento autorizzatorio**. La richiesta è formulata dal questore o dal comandante provinciale dell'Arma dei carabinieri o della Guardia di finanza, ovvero dai responsabili dei Servizi centrali di cui all'articolo 12 del decreto-legge n. 152 del 1991, ed è rivolta al **procuratore della Repubblica presso il tribunale del capoluogo del distretto** nel quale sono emerse le esigenze di prevenzione o di ricerca.

La richiesta indica:

- la finalità perseguita;
- la durata prevista;
- l'area territoriale;
- le persone interessate e ricercate;
- le banche dati di riferimento utilizzate;
- i sistemi e le tecnologie impiegati.

Sul punto, si rammenta che la direttiva (UE) 2016/680, recepita con il decreto legislativo n. 51 del 2018, indica le condizioni per la limitazione del diritto alla protezione dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento dei reati. Al riguardo, la Corte di giustizia dell'Unione europea, con [sentenza del 4 ottobre 2024](#) (causa C-548/21, *Bezirkshauptmannschaft Landeck*), ha sancito che tali limitazioni devono essere interpretate conformemente all'[articolo 52, paragrafo 1](#), della Carta dei diritti fondamentali dell'Unione europea, il quale impone il rispetto del principio di proporzionalità. In forza di tale principio, come afferma la Corte di giustizia, “qualora l'accesso ai dati personali da parte delle autorità nazionali competenti comporti il rischio di un'ingerenza grave [...] nei diritti fondamentali dell'interessato, è essenziale che

tale accesso sia subordinato a un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente”. Infatti, prosegue la Corte, “un controllo successivo non consentirebbe di [...] impedire che sia autorizzato un accesso ai dati di cui trattasi che ecceda i limiti dello stretto necessario”. Ne consegue che l’accesso delle autorità a questi dati deve essere subordinato al controllo preventivo di un giudice o di un organo amministrativo indipendente, salvi i “casi di urgenza debitamente comprovati”.

Il **comma 5** definisce contenuto e limiti dell’autorizzazione, che deve riferirsi a uno specifico evento o al tempo strettamente necessario, comunque **non superiore a quindici giorni, prorogabili** dal pubblico ministero con decreto motivato per ulteriori periodi di quindici giorni, al permanere delle condizioni e deve recare la delimitazione dell’area territoriale e l’indicazione delle persone interessate e ricercate.

L’autorizzazione può essere concessa soltanto previa effettuazione delle valutazioni di cui all’articolo 5, paragrafo 2, del regolamento IA, relative alla natura e gravità della situazione e alle conseguenze dell’uso sui diritti e sulle libertà delle persone.

L’articolo 5, paragrafo 2, del regolamento IA impone di tenere conto, per ciascun uso: a) della natura della situazione (in particolare gravità, probabilità ed entità del danno in assenza dell’uso del sistema); b) delle conseguenze dell’uso sui diritti e sulle libertà delle persone interessate. La valutazione si coordina con gli ulteriori presidi previsti dallo stesso articolo 5 (autorizzazione preventiva e registrazione) e con la valutazione d’impatto sui diritti fondamentali di cui all’articolo 27 del regolamento.

Si segnala che l’utilizzo di tali sistemi è assistito dalle ulteriori garanzie procedurali e tecniche dettate dal successivo articolo 9 (v. *infra*).

I **commi 6 e 7** regolano i **casi d’urgenza**. Quando vi è fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave e irreparabile per le finalità indicate, l’impiego può essere avviato, su disposizione del questore, dei comandanti o dei responsabili indicati al comma 4, dall’organo di polizia procedente, **previa comunicazione anche orale al pubblico ministero** e nei limiti dello stretto necessario, con delimitazione dell’area e indicazione delle persone ricercate. La richiesta di autorizzazione è **trasmessa** al pubblico ministero **senza ritardo e comunque entro ventiquattro ore** dall’inizio delle operazioni; il pubblico ministero, ove ne ravvisi le condizioni, provvede **nelle successive ventiquattro ore**.

Il **comma 8** disciplina le **conseguenze delle violazioni**. In caso di inosservanza delle condizioni e dei termini previsti dai commi 4, 5, 6 e 7, ovvero di mancata autorizzazione, **l’uso del sistema è immediatamente interrotto e tutti i dati personali**, i risultati e gli *output* acquisiti e prodotti

sono cancellati, salvi gli elementi legittimamente acquisiti sotto altra base giuridica; i risultati ottenuti in violazione della disposizione non possono in ogni caso essere utilizzati.

Infine, il **comma 9** prevede l'applicazione delle disposizioni di cui all'articolo 226, comma 5, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale.

Il comma 5 dell'articolo 226 delle disposizioni di attuazione del codice di procedura penale prevede che gli elementi acquisiti mediante intercettazioni preventive non siano utilizzabili nel procedimento penale, fatti salvi i fini investigativi. La disposizione stabilisce, inoltre, il divieto di menzionare tali attività e le notizie da esse acquisite negli atti di indagine, nonché di farne oggetto di deposizione o di altra forma di divulgazione.

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 9 detta le **garanzie procedurali** che accompagnano l'utilizzo dei sistemi di intelligenza artificiale per l'identificazione biometrica remota «in tempo reale».

La disposizione completa il quadro di garanzie introdotto dall'articolo 8, recependo sul piano interno i presidi di *accountability* che il regolamento (UE) 2024/1689 (regolamento IA) pone a condizione dell'uso dell'identificazione biometrica remota «in tempo reale».

Il **comma 1** impone al **titolare del trattamento**, in conformità a quanto previsto dall'articolo 5, paragrafo 2, e all'articolo 27 del regolamento IA, di completare, in via preventiva, una **valutazione d'impatto sui diritti fondamentali** prima di utilizzare i sistemi per le finalità di cui all'articolo 8 dello schema di decreto (identificazione biometrica remota «in tempo reale», v. *supra*) o all'articolo 359-ter c.p.p. (che prevede ipotesi di identificazione e localizzazione mediante sistemi di intelligenza artificiale, v. *infra*).

Sul punto si ricorda che l'articolo 5, paragrafo 2, del regolamento IA circoscrive l'uso dei **sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico** ai fini di attività di contrasto solo per confermare l'identità della persona specificamente interessata e presuppone la ponderazione, da un lato, della natura della situazione (gravità, probabilità ed entità del danno derivante dal mancato uso) e, dall'altro, delle conseguenze sui diritti e sulle libertà di tutte le persone coinvolte (gravità, probabilità ed entità delle stesse). L'impiego deve inoltre rispettare le tutele e le condizioni necessarie e proporzionate previste dal diritto nazionale che lo autorizza, in particolare i limiti temporali, geografici e personali, ed è subordinato al previo completamento della valutazione d'impatto sui diritti fondamentali (articolo 27) e alla registrazione del sistema nella banca dati UE (articolo 49); nelle situazioni di urgenza debitamente giustificate l'uso può essere avviato prima della registrazione, purché questa sia completata senza indebito ritardo.

L'articolo 27 del medesimo regolamento, come detto, disciplina la **valutazione d'impatto sui diritti fondamentali** (*Fundamental Rights Impact Assessment*), che il *deployer* deve effettuare prima dell'uso di determinati sistemi ad alto rischio. Essa comprende, in sintesi: la descrizione dei processi in cui il sistema sarà utilizzato; il periodo e la frequenza d'uso; le categorie di persone e di gruppi

interessati; i rischi specifici di pregiudizio per tali categorie; le misure di sorveglianza umana; le misure da adottare in caso di concretizzazione dei rischi. Ove gli obblighi siano già assolti tramite la valutazione d'impatto sulla protezione dei dati (articolo 35 del regolamento UE 2016/679 o articolo 27 della direttiva UE 2016/680), la valutazione sui diritti fondamentali la integra.

Il **comma 2** prescrive la **registrazione automatica** di ogni utilizzo in appositi **file di log non modificabili**, contenenti i dati indicati dall'articolo 12, paragrafo 3, del regolamento IA⁵. I *file di log* sono conservati per **cinque anni** dall'accesso e dall'operazione e resi accessibili esclusivamente alle autorità competenti per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale.

Al riguardo, si rappresenta che i “log” sono indicati, all'articolo 12, paragrafo 1, del regolamento IA come gli eventi la cui registrazione automatica è consentita dai sistemi di IA ad alto rischio lungo l'intero ciclo di vita del sistema.

Più in generale, i *file log* sono solitamente usati da programmi o sistemi operativi per tenere traccia di determinati eventi. Tali *file* sono usati per registrare tutto ciò che un sistema operativo o un programma ritiene necessario segnalare.

Il **comma 3** fa salvi i termini di conservazione dei dati personali stabiliti, per finalità di polizia, dall'articolo 10 del decreto del Presidente della Repubblica 15 gennaio 2018, n. 15. La conservazione quinquennale dei *log* di cui al comma 2 resta dunque distinta dai termini di conservazione dei dati trattati, che continuano a seguire la disciplina di settore.

L'articolo 10 del d.P.R. 15 gennaio 2018, n. 15 — regolamento sul trattamento dei dati personali per finalità di polizia, attuativo del codice in materia di protezione dei dati personali — fissa i termini massimi di conservazione dei dati trattati a tali fini, stabilendo (comma 1) che essi non eccedano il tempo necessario al conseguimento delle finalità di polizia e individuando (comma 3) termini differenziati per categoria di dati.

Il **comma 4** disciplina la **notifica al Garante** per la protezione dei dati personali, da effettuare dopo l'utilizzo, in conformità all'articolo 5, paragrafo 4, del regolamento IA⁶. La notifica è subordinata al **nulla osta**

⁵ L'articolo 12, paragrafo 3, del regolamento IA prescrive, per i sistemi di identificazione biometrica remota (allegato III, punto 1, lettera a), la registrazione di almeno: il periodo di ciascun utilizzo (data e ora di inizio e di fine); la banca dati di riferimento utilizzata per verificare i dati di input; i dati di input per i quali la ricerca ha prodotto una corrispondenza; l'identificativo delle persone fisiche che partecipano alla verifica dei risultati (articolo 14, paragrafo 5).

⁶ L'articolo 5, paragrafo 4, del regolamento IA prevede che ogni uso del sistema di identificazione biometrica remota «in tempo reale» sia notificato alla competente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati; la notifica contiene almeno le

preventivo dell'autorità giudiziaria competente, che può differirlo, in presenza di specifiche esigenze di segretezza, per un periodo non superiore a tre mesi, rinnovabile una sola volta. Essa contiene le informazioni essenziali sull'autorizzazione rilasciata e sul risultato conseguito e non include dati operativi sensibili. In caso di **più attivazioni nello stesso contesto operativo** o di **utilizzi omogenei**, la notifica può essere effettuata in forma periodica e cumulativa, secondo i termini fissati dal decreto di cui al comma 5, ferma restando la necessità del nulla osta preventivo.

Il **comma 5** rinvia a un **decreto del Ministro dell'interno**, di concerto con il Ministro della giustizia, sentiti il Garante e le Autorità nazionali per l'intelligenza artificiale⁷, l'individuazione, in relazione all'uso dei sistemi per le finalità dell'articolo 8 dello schema di decreto o dell'articolo 359-ter c.p.p.: dei requisiti tecnici minimi di affidabilità e accuratezza, comprese le soglie operative (lettera *a*); delle modalità di monitoraggio periodico delle prestazioni, con particolare riguardo alla rilevazione e mitigazione di *bias* o effetti discriminatori (lettera *b*); delle misure tecniche e organizzative per garantire la sicurezza del trattamento (lettera *c*) e per impedire accessi illeciti ai dati (lettera *d*); delle informazioni che il titolare è tenuto ad allegare alla richiesta di autorizzazione circa le caratteristiche tecniche del sistema, i risultati delle verifiche di accuratezza e i meccanismi di gestione degli errori (lettera *e*); delle modalità di esecuzione della notifica di cui al comma 4 (lettera *f*); nonché degli ulteriori adempimenti conformi al regolamento IA (lettera *g*).

informazioni di cui al paragrafo 6 e non include dati operativi sensibili. Tali autorità presentano alla Commissione relazioni annuali sull'uso notificato (paragrafo 6).

⁷ Le Autorità nazionali per l'intelligenza artificiale sono individuate dall'articolo 20 della legge n. 132 del 2025 nell'Agenzia per l'Italia digitale (AgID) e nell'Agenzia per la cybersicurezza nazionale (ACN).

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** disciplina l'integrazione dei **sistemi di videosorveglianza con tecnologie di riconoscimento facciale "a posteriori"** basate su IA per ragioni di **ordine e sicurezza pubblica**, in coerenza con il regolamento (UE) 2024/1689.

In particolare, l'attivazione del riconoscimento facciale è ammessa **solo dopo la commissione di un reato**, anche tentato, ai fini dell'**identificazione di soggetti indiziati**, sotto la responsabilità dell'ufficiale di pubblica sicurezza o di polizia giudiziaria competente, con esclusione dell'identificazione biometrica in tempo reale e di usi generalizzati o non collegati a un reato.

Infine, sul piano della protezione dei dati personali, l'articolo individua il **titolare del trattamento** nel **Dipartimento della pubblica sicurezza** e demandata a un **decreto del Ministro dell'interno** la definizione delle **modalità di trattamento e di memorizzazione** dei dati biometrici nella base dati di riferimenti, delle misure tecniche e organizzative di sicurezza e degli ulteriori adempimenti in conformità del regolamento IA.

Il **comma 1** prevede la possibilità di integrare, laddove sussistano **esigenze di ordine e sicurezza pubblica**, i **sistemi di videosorveglianza con componenti di intelligenza artificiale**, i quali consentono, ricorrendone i presupposti previsti dal successivo comma 2, l'**attivazione successiva di tecnologie di riconoscimento facciale**, con un intervallo di tempo tale da non configurare una identificazione biometrica remota in tempo reale ai sensi del regolamento (UE) 2024/1689.

Si ricorda, in proposito, che l'articolo 5, paragrafo 1, lettera *h*), include tra le pratiche di IA vietate l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno dei seguenti obiettivi:

- la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;
- la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

- la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'Allegato II⁸, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Al riguardo, la relazione illustrativa osserva come la disposizione in commento garantisca, in tal modo, la distinzione tra l'utilizzo "a posteriori" del riconoscimento facciale e quello "in tempo reale", prescrivendo limiti temporali, di finalità e di responsabilità, nonché prevedendo una forte tracciabilità dei trattamenti, in conformità del regolamento AI e, in particolare, della direttiva (UE) 2016/680, recepita dal decreto legislativo n. 51 del 2018.

La medesima disposizione specifica, inoltre, che la suddetta integrazione è ammessa nei casi in cui l'installazione di sistemi di videosorveglianza è consentita da specifiche disposizioni di legge e deve essere effettuata in conformità alla normativa in materia di trattamento dei dati personali e al regolamento (UE) 2024/1689.

Si ricorda, al riguardo, che le disposizioni concernenti il trattamento dei dati personali sono contenute, a livello unionale, nel regolamento (UE) 2016/679 e, a livello nazionale, nel decreto legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali), come modificato dal decreto legislativo n. 101 del 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Si rammenta, inoltre, che l'articolo 9, comma 9, del decreto-legge n. 139 del 2021 ha disposto la sospensione della installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte di autorità pubbliche o soggetti privati, con esclusione dei trattamenti effettuati dalle autorità competenti a fini della prevenzione e della repressione dei reati o dell'esecuzione di sanzioni penali (di cui al già citato decreto legislativo n. 51 del 2018), in presenza di parere preventivo favorevole del Garante per la protezione dei dati personali. Tale sospensione è stata disposta inizialmente fino all'entrata in vigore di una disciplina legislativa della materia, e comunque non oltre il 31 dicembre 2023. Tale termine è stato successivamente prorogato di un biennio dall'articolo

⁸ Si ricorda che l'Allegato II indica i seguenti reati: terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei predetti reati.

8-ter del decreto-legge n. 51 del 2023 e, da ultimo, al 31 dicembre 2027 dall'articolo 2, comma 6-*quater*, del decreto-legge n. 200 del 2025.

Il **comma 2** prevede che l'**utilizzo delle suddette tecnologie** è ammesso, in base a quanto disposto dall'articolo 26, paragrafo 10, primo comma, del regolamento (UE) 2024/1689, esclusivamente **dopo la commissione di un fatto di reato**, anche tentato, al solo fine della **identificazione delle persone già indiziate** della commissione del reato sulla base di documentazione video-fotografica e di elementi oggettivi e verificabili, sotto la diretta ed esclusiva **responsabilità dell'ufficiale di pubblica sicurezza** designato dal questore per la gestione dell'ordine e della sicurezza pubblica, ovvero, al di fuori di tale ipotesi, dell'**ufficiale di polizia giudiziaria della Forza di polizia** che procede in relazione al reato.

A tal riguardo, si rammenta che, ai sensi del citato articolo 26, paragrafo 10, primo comma, del regolamento IA, fatta salva la direttiva (UE) 2016/680, nell'ambito di un'indagine finalizzata alla ricerca mirata di una persona sospettata o condannata per la commissione di un reato, il *deployer* - ovvero una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità - di un sistema di IA ad alto rischio per l'**identificazione biometrica remota "a posteriori"** è tenuto a **richiedere**, per l'uso di tale sistema, un'**autorizzazione**, *ex ante* o senza indebito ritardo ed entro 48 ore, a un'**autorità giudiziaria o amministrativa**, la cui **decisione è vincolante e soggetta a controllo giurisdizionale**, ad eccezione dell'ipotesi in cui tale sistema è **utilizzato** per l'identificazione iniziale di un potenziale sospetto sulla base di **fatti oggettivi e verificabili** direttamente connessi al reato.

Si ricorda, altresì, che gli ufficiali di polizia giudiziaria, ai sensi dell'articolo 57, comma 1, lettere *a)* e *b)*, del codice di procedura penale, sono:

- i dirigenti, i commissari, gli ispettori, i sovrintendenti e gli altri appartenenti alla Polizia di Stato, ai quali l'ordinamento dell'amministrazione della pubblica sicurezza riconosce tale qualità;

- gli ufficiali superiori e inferiori e i sottufficiali dei Carabinieri, della Guardia di finanza, degli agenti di custodia e del Corpo forestale dello Stato, nonché gli altri appartenenti alle predette forze di polizia ai quali l'ordinamento delle rispettive amministrazioni riconosce tale qualità.

Il **comma 3** stabilisce che l'utilizzo dei sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall'intelligenza artificiale, per l'**accesso a luoghi o a eventi connotati da esigenze di ordine e sicurezza pubblica**, implica il **trattamento automatizzato dei dati biometrici** rilevati dalle immagini del volto delle persone che accedono a tali luoghi o eventi, con memorizzazione locale nella base di dati di riferimento per il confronto biometrico a posteriori,

unitamente, senza l'impiego di tali tecnologie di IA, ai corrispondenti dati anagrafici e, in caso di posto assegnato, il relativo identificativo, ottenuti mediante la scansione elettronica dei titoli di accesso. La medesima disposizione stabilisce che, in caso di **commissione di un fatto di reato**, l'utilizzo dei predetti sistemi di videosorveglianza con l'attivazione delle tecnologie di riconoscimento facciale determina il **trattamento automatizzato dei dati biometrici** estratti dalle immagini del volto delle persone da identificare in quanto indiziate di aver commesso il reato, ai fini del **confronto biometrico a posteriori** con i dati biometrici e anagrafici presenti nella suddetta base di dati di riferimento.

I **commi da 4 a 8** vertono specificamente sul **trattamento dei dati personali**.

In particolare, il **titolare del trattamento dei dati personali**, effettuato con l'utilizzo dei sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall'intelligenza artificiale, è individuato nel **Ministero dell'interno – Dipartimento della pubblica sicurezza** (comma 4), il quale, in relazione a tali tipologie di trattamento, è tenuto a eseguire preventivamente la **valutazione d'impatto sulla protezione dei dati** - con facoltà di effettuarne una sola, valida per tutti i sistemi analoghi - e a **consultare il Garante per la protezione dei dati personali** (comma 5).

Si ricorda, al riguardo, che, ai sensi dell'articolo 23 del decreto legislativo n. 51 del 2018, qualora il trattamento, in ragione dell'uso di nuove tecnologie e della sua natura, dell'ambito di applicazione, del contesto e delle finalità, si connoti per un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali, la quale presenta il seguente contenuto:

- una descrizione generale dei trattamenti previsti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare tali rischi;
- le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del decreto legislativo n. 51 del 2018.

Inoltre, ai sensi dell'articolo 24 del decreto medesimo, il titolare o il responsabile del trattamento, ad eccezione dei trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero, consulta il Garante prima del trattamento di dati personali che risulteranno in un nuovo archivio di prossima creazione nelle seguenti circostanze:

- la suddetta valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

- il tipo di trattamento presenta un rischio elevato per i diritti e le libertà degli interessati anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici.

Pertanto, il titolare del trattamento è tenuto a trasmettere al Garante la valutazione d'impatto sulla protezione dei dati e, ove richiesta, ogni altra informazione, al fine di consentire a tale autorità di effettuare una valutazione della conformità del trattamento, dei rischi per la protezione dei dati personali dell'interessato e delle relative garanzie.

Si prevede, inoltre, che i dati personali trattati mediante i predetti sistemi siano **conservati**, nella base di dati di riferimento per il confronto biometrico a posteriori, **per sette giorni** a decorrere dalla raccolta, e siano **automaticamente cancellati** alla scadenza di tale termine (comma 6).

La norma richiede, altresì, che gli **accessi** e le **operazioni di trattamento** sui citati sistemi siano effettuati **esclusivamente dalle persone autorizzate** e siano **automaticamente registrati** in appositi *file* di *log* non modificabili, in conformità a quanto previsto dall'articolo 12, paragrafo 3, del regolamento IA.

In merito, si evidenzia che, ai sensi del citato articolo 12, paragrafo 3, per i sistemi di identificazione biometrica remota le capacità di registrazione comprendono almeno i dati seguenti:

- la registrazione del periodo di ciascun utilizzo del sistema (data e ora di inizio e di fine di ciascun utilizzo);
- la banca dati di riferimento utilizzata dal sistema per verificare i dati di *input*;
- i dati di *input* per i quali la ricerca ha portato a una corrispondenza;
- l'identificativo delle persone fisiche che partecipano alla verifica dei risultati di cui all'[articolo 14, paragrafo 5](#), del regolamento IA.

Tali *file* sono **conservati per cinque anni** dall'accesso e dall'operazione e sono resi **accessibili per finalità di verifica** della liceità del trattamento, di controllo interno, nonché nell'ambito di un procedimento penale (comma 7), fermi restando i **termini di conservazione dei dati personali per finalità di polizia** previsti dall'[articolo 10](#) del decreto del Presidente della Repubblica n. 15 del 2018 (comma 8).

Si ricorda, in proposito, che l'articolo 10 sopra citato stabilisce, al comma 1, il principio generale in forza del quale i dati personali oggetto di trattamento possono essere conservati solo per il periodo di tempo non superiore a quello necessario al conseguimento delle finalità di polizia, ovvero quelle correlate ai compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati. Il comma 2 del medesimo articolo prevede che i dati personali soggetti a trattamento automatizzato, trascorsa la metà del tempo massimo di conservazione, se uguale o superiore a

quindici anni, siano accessibili ai soli operatori a ciò abilitati e designati, incaricati del trattamento secondo profili di autorizzazione predefiniti in base alle indicazioni del capo dell'ufficio o del comandante del reparto e in relazione a specifiche attività informative, di sicurezza o di indagine di polizia giudiziaria. I termini massimi di conservazione dei dati personali per finalità di polizia sono indicati al successivo comma 3, il quale li differenzia per categoria di dato, facendoli decorrere da eventi diversi a seconda della tipologia considerata. Si rinvia all'[articolo 10](#) per la consultazione degli stessi.

Il **comma 9**, conformemente a quanto disposto dall'articolo 26, paragrafo 10, terzo comma, del regolamento IA, stabilisce il **divieto di fondare esclusivamente** sui risultati forniti dall'applicazione di riconoscimento facciale una **decisione con effetti giuridici negativi** sulla persona cui si riferiscono i dati oggetto del trattamento

Il **comma 10 vieta l'utilizzo** dei sistemi di videosorveglianza con l'attivazione delle tecnologie di riconoscimento facciale per finalità di **controllo e di identificazione biometrica generalizzati o indiscriminati** di persone, non mirata e priva di collegamento con un reato o con un procedimento penale.

Il **comma 11** demanda ad apposito **decreto del Ministro dell'interno**, sentito il Garante, da adottare entro tre mesi dalla data di entrata in vigore del presente provvedimento, la definizione:

- delle **modalità del trattamento automatizzato dei dati biometrici** estratti o rilevati dalle immagini del volto delle persone che accedono ai luoghi o agli eventi caratterizzati da esigenze di ordine e sicurezza pubblica e della loro **memorizzazione locale** in una base di dati di riferimento per il confronto biometrico a posteriori;
- le **misure tecniche e organizzative** necessarie a garantire un adeguato livello di **sicurezza del trattamento**;
- gli **adempimenti** a carico del titolare del trattamento ai sensi del regolamento IA.

Il **comma 12** individua i **soggetti abilitati**, senza nuovi o maggiori oneri per la finanza pubblica, all'**installazione** e alla **manutenzione** dei sistemi di videosorveglianza con l'attivazione delle tecnologie di riconoscimento facciale. In particolare, essi sono:

- i **gestori** dei luoghi o eventi connotati da esigenze di ordine e sicurezza pubblica;

- gli **organizzatori o promotori** degli eventi medesimi ovvero **chi ha la disponibilità** delle strutture in cui tali eventi hanno luogo, in accordo con i proprietari degli stessi luoghi o strutture.

Si prevede, inoltre, che, in tali circostanze, i sistemi di cui sopra siano **concessi in comodato d'uso gratuito alla Questura**, la quale ne assume la totale disponibilità.

Infine, il **comma 13** reca la **clausola di invarianza finanziaria**, prevedendo che l'attuazione delle suesposte disposizioni non deve comportare nuovi o maggiori oneri per la finanza pubblica.

**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**

**CAPO I – DISPOSIZIONI SANZIONATORIE E IN MATERIA DI
PROCEDIMENTO PENALE**

**Articolo 11
(Definizioni)**

L'**articolo 11** individua le **definizioni** applicabili al **Titolo II** del decreto – recante le– mediante rinvio integrale all'articolo 3 del regolamento sull'intelligenza artificiale.

L'**articolo 11** reca il quadro definitorio comune a tutte le disposizioni del Titolo II dello schema di decreto relativo alle disposizioni penali, sostanziali e processuali in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale, nonché le disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi. Il **comma 1**, unico dell'articolo, stabilisce che, ai fini del Titolo II, si applicano le definizioni di cui all'**articolo 3** del regolamento sull'intelligenza artificiale (UE) 2024/1689.

Secondo la relazione illustrativa, la scelta del rinvio dinamico è volta a evitare duplicazioni definitorie e ad assicurare la piena uniformità terminologica con il quadro eurounitario, in coerenza con le indicazioni del § 3 della circolare della Presidenza del Consiglio dei ministri 2 maggio 2001 (recante «*Guida alla redazione dei testi normativi*»), in tema di rapporti fra atti normativi.

Ai fini delle disposizioni del Titolo II assumono rilievo, in particolare, le seguenti definizioni recate dall'articolo 3 del regolamento. Con riguardo alle disposizioni penali e a quelle sulla responsabilità civile, che fanno leva sul sistema di IA e sui soggetti della catena del valore (segnatamente le posizioni di garanzia richiamate dall'articolo 12), rilevano le nozioni di:

«**sistema di IA**» (articolo 3, punto 1): un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può

presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dagli input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

«**fornitore**» (articolo 3, punto 3): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che sviluppa, o fa sviluppare, un sistema di IA o un modello di IA per finalità generali e lo immette sul mercato o mette in servizio il sistema con il proprio nome o marchio, a titolo oneroso o gratuito;

«**importatore**» (articolo 3, punto 6): una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona stabilita in un paese terzo;

«**distributore**» (articolo 3, punto 7): una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione;

«**deployer**» (articolo 3, punto 4): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, salvo che il sistema sia utilizzato nel corso di un'attività personale non professionale;

«**operatore**» (articolo 3, punto 8): un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore;

«**modello di IA per finalità generali**» (articolo 3, punto 63): un modello di IA – anche addestrato con grandi quantità di dati mediante autosupervisione su larga scala – caratterizzato da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti, integrabile in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli utilizzati per attività di ricerca, sviluppo o prototipazione prima dell'immissione sul mercato.

Con riguardo alle disposizioni processuali penali, e in particolare all'articolo 359-ter del codice di procedura penale (introdotto dall'articolo 13), rilevano inoltre le nozioni in materia biometrica:

«**dati biometrici**» (articolo 3, punto 34): i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici;

«**identificazione biometrica**» (articolo 3, punto 35): il riconoscimento automatizzato di caratteristiche umane di tipo fisico, fisiologico, comportamentale o psicologico, allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di persone memorizzati in una banca dati;

«sistema di identificazione biometrica remota» (articolo 3, punto 41): un sistema di IA finalizzato a identificare persone fisiche, senza il loro coinvolgimento attivo e in genere a distanza, mediante il confronto dei loro dati biometrici con quelli contenuti in una banca dati di riferimento;

«sistema di identificazione biometrica remota “in tempo reale”» (articolo 3, punto 42): un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, comprendendo non solo l'identificazione istantanea ma anche quella con ritardi limitati, così da evitare l'elusione delle norme.

Articolo 12 (Modifiche al codice penale)

L'**articolo 12** inserisce nel codice penale il nuovo delitto di **omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi**, di cui all'art. 437-bis.

L'**articolo 12** inserisce nel codice penale il nuovo **art. 437-bis** che contiene **due diverse fattispecie penali** aventi ad oggetto i sistemi di intelligenza artificiale:

- la prima, che concerne l'**omessa adozione di misure di sicurezza** nella loro progettazione o nel loro utilizzo (commi primo e terzo);
- la seconda, che concerne la loro **alterazione illecita** (comma secondo).

Dal punto di vista sistematico, l'art. 437-bis si colloca tra i delitti di comune pericolo mediante violenza, di cui al capo I del titolo VI (dei delitti contro l'incolumità pubblica) del codice penale.

Il reato di **omessa adozione di misure di sicurezza** di cui al **primo comma** dell'art. 437-bis è direttamente **attuativo del criterio di delega contenuto all'art. 24, comma 5, lett. b), della legge 132/2025 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale)**, ai sensi del quale è richiesta «l'introduzione di autonome fattispecie di reato, punite **a titolo di dolo o di colpa**, incentrate sull'**omessa** adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato».

Essa è caratterizzata da una **condotta di carattere omissivo** che può concretizzarsi:

- ✓ nella **mancata adozione delle misure tecniche di sicurezza** che investono tutto il ciclo di vita del **sistema di IA** classificato come **ad alto rischio**⁹ (dalla fase iniziale, che comprende progettazione,

⁹ Si ricorda che il regolamento (UE) 2024/1689 (AI Act) classifica i sistemi di IA sulla base del rischio che essi possono portare ai diritti e alla sicurezza. Ai sensi dell'art. 6 del citato regolamento, è considerato ad alto rischio il sistema destinato a essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I al regolamento o è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio sempre ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I (devono verificarsi entrambe le condizioni). Altri sistemi ad alto rischio sono elencati

produzione e addestramento del sistema, al suo collocamento sul mercato fino alla fase di utilizzo professionale vero e proprio) e che sono considerate idonee a prevenire difetti di funzionamento del sistema medesimo;

- ✓ nella **mancata adozione di misure di sorveglianza umana**.

L'approccio del legislatore delegato è di tipo precauzionale, in linea con l'impianto generale del regolamento (UE) 2024/1689 basato sulla classificazione dei rischi, ma è temperato dalla previsione secondo cui il reato si realizza solo qualora i beni giuridici tutelati siano sottoposti ad un **pericolo concreto** (come peraltro richiesto dal già citato criterio di delega).

La cornice edittale è diversamente graduata a seconda che l'omissione ponga un concreto pericolo:

- **alla vita o all'incolumità pubblica o individuale**, nel qual caso il colpevole è punito con la **reclusione da 1 a 5 anni**;
- **all'incolumità pubblica o alla sicurezza dello Stato**, nel qual caso il colpevole è punito con la **reclusione da 2 a 8 anni**.

Si osserva che la messa in pericolo dell'incolumità pubblica risulterebbe punibile, ai sensi del primo comma dell'art. 437-bis, tanto con la reclusione da 1 a 5 anni quanto con la reclusione da 2 a 8 anni. Si valuti la necessità di un coordinamento.

Il delitto è punibile, ai sensi del **terzo comma**, anche a titolo di **colpa grave**: in tal caso si applicherà una **riduzione di pena da un terzo ad un sesto**.

In proposito si ricorda che il più volte richiamato criterio di delega di cui all'art. 24, comma 5, lett. b), non limita la punibilità alla sola colpa grave. Tale scelta del legislatore delegato risponde, secondo quanto argomentato nella relazione illustrativa, «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».

Il reato **di alterazione illecita dei sistemi**, di cui al secondo comma dell'art. 437-bis, è volto invece a punire chiunque, non essendo coinvolto nelle attività indicate al primo comma (progettazione, produzione, addestramento, immissione sul mercato utilizzo professionale) e non

nell'allegato III (ad es. sistemi di identificazione biometrica remota oppure sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche).

potendo quindi lecitamente agire su un **sistema di IA ad alto rischio**, lo altera, cagionando un **pericolo concreto**:

- **alla vita o all'incolumità individuale**, nel qual caso è punito con la **reclusione da 2 a 6 anni**;
- **all'incolumità pubblica o alla sicurezza dello Stato**, nel qual caso il colpevole è punito con la **reclusione da 3 a 10 anni**.

La **condotta** tipica del reato in esame è, a differenza del reato di cui al primo comma, **di tipo commissivo**, implicando un'azione del reo.

Secondo la relazione illustrativa «[s]i 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», circostanza confermata anche dal fatto che la disposizione, per espressa previsione normativa, trova applicazione solo qualora il fatto non integri un più grave reato.

«La disposizione» continua la relazione illustrativa «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» il che varrebbe anche a giustificare il più grave trattamento sanzionatorio.

Articolo 13 (Modifiche al codice di procedura penale)

L'articolo 13 reca modifiche al codice di procedura penale, introducendo la disciplina volta a regolare l'utilizzo di sistemi intelligenza artificiale per l'identificazione biometrica remota in tempo reale all'interno dei procedimenti penali.

L'articolo 13 introduce, all'interno del codice di procedura penale, il nuovo art. 359-ter c.p.p. rubricato “**Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale**”.

La **relazione illustrativa** sottolinea come attraverso la norma in esame viene data attuazione al criterio di delega contenuto all'art. 24, comma 5, lett. e) della L. n. 132 del 2025 (“Deleghe al Governo in materia di intelligenza artificiale”). Nello specifico, tale disposizione prevede quale criterio di delega la “regolazione dell'utilizzo dei sistemi di intelligenza artificiale **nelle indagini preliminari**, nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza”.

A tal riguardo, il **comma 1** dispone che può essere autorizzato l'impiego di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale nei casi in cui si proceda per uno dei delitti previsti dall'allegato II del Regolamento UE 2024/1689, che siano puniti con la **reclusione non inferiore nel massimo a 4 anni**.

L'utilizzo di tali strumenti è consentito quando bisogna:

- **confermare l'identificazione** di una persona nei confronti della quale sussistono sufficienti indizi della commissione dei predetti reati;
- procedere alla **ricerca mirata**, ivi compresa la **localizzazione**, di una persona indiziata dei medesimi delitti

Si ricorda che l'Allegato II del Regolamento UE 2024/1689 (cd. “AI Act”) reca l'elenco di tutti i reati a cui fa riferimento l'art. 5, par. 1, lett. h, punto iii). Quest'ultima disposizione permette l'utilizzo di sistemi di identificazione biometrica remota «in tempo reale», in spazi accessibili al pubblico, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale, allorquando sia necessario localizzare o identificare una persona sospettata di aver commesso un reato, di cui al predetto

allegato II, punibile nello Stato membro con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno 4 anni.

I reati contenuti all'interno dell'Allegato II sono:

- terrorismo;
- tratta di esseri umani;
- sfruttamento sessuale di minori e pornografia minorile;
- traffico illecito di stupefacenti o sostanze psicotrope;
- traffico illecito di armi, munizioni ed esplosivi;
- omicidio volontario, lesioni gravi;
- traffico illecito di organi e tessuti umani;
- traffico illecito di materie nucleari e radioattive;
- sequestro, detenzione illegale e presa di ostaggi;
- reati che rientrano nella competenza giurisdizionale della Corte penale internazionale;
- illecita cattura di aeromobile o nave;
- violenza sessuale;
- reato ambientale;
- rapina organizzata o a mano armata;
- sabotaggio;
- partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

Il **comma 2** regola i casi in cui bisogna ricorrere ai predetti sistemi di intelligenza artificiale nelle **attività di ricerca di un latitante** nei confronti del quale occorre eseguire una **misura cautelare coercitiva** ovvero un **ordine di esecuzione**, non sospeso, che dispone la carcerazione, sempre per i medesimi delitti del comma 1. In tali ipotesi è possibile procedere alla localizzazione della persona ricercata tramite identificazione biometrica remota in tempo reale, mediante i predetti 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** prende in esame la **banca dati** da utilizzare per le operazioni investigative di cui ai commi precedenti. In particolare, si precisa che i confronti biometrici di cui ai commi 1 e 2 possono basarsi esclusivamente su **banche dati di riferimento idonee** a perseguire le **finalità prescritte**. Inoltre, tali banche dati devono contenere, qualora siano disponibili, i dati biometrici e le relative informazioni identificative, riguardanti i soggetti, anche non identificati, presi in considerazione dai commi 1 e 2. Il contenuto della banca dati può essere alimentato anche da banche dati già in uso alla polizia giudiziaria o ad essa accessibili, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle indagini.

Il **comma 4** non si rivolge all'autore del reato, bensì alle persone offese. Infatti, tale disposizione consente di utilizzare i sistemi di intelligenza artificiale, con le medesime modalità dei commi che precedono, per la **ricerca di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani**.

Si segnala che tale previsione ricalca quanto prescritto dall'art. 5, *lett. h*), punto i), in forza del quale è permesso l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico, per la ricerca delle vittime dei reati sopra riportati.

I **commi 5, 6 e 7** disciplinano il procedimento attraverso cui vengono autorizzate le operazioni investigative che permettono l'impiego di sistemi intelligenza artificiale. In particolare, si prevede che il **pubblico ministero richieda** la prescritta **autorizzazione** all'identificazione biometrica remota in tempo reale al **giudice per le indagini preliminari (comma 5)**.

Appare opportuno osservare che il comma 2 consente l'impiego di sistemi IA di rilevazione biometrica per ricercare un latitante nei confronti del quale bisogna eseguire una misura cautelare coercitiva ovvero un ordine di esecuzione della pena della reclusione. Sul punto, si osserva che la misura cautelare può essere applicata anche al di fuori delle indagini preliminari, mentre l'ordine di esecuzione della pena presuppone una sentenza di condanna.

Alla luce delle considerazioni che precedono, si valuti l'opportunità di approfondire il profilo relativo alla competenza nell'autorizzazione all'impiego di sistemi di IA per l'identificazione biometrica remota in tempo reale (in particolare, valutando se possa essere disposta anche da autorità giudiziarie diverse dal GIP, in relazione alla fase processuale in cui tale autorizzazione viene adottata).

Ai sensi del **comma 6**, il **GIP autorizza** tale impiego con **decreto motivato**. Tale provvedimento deve:

- circoscrivere l'indicazione dell'area geografica in cui è possibile utilizzare lo strumento in esame;
- indicare le persone specificamente ricercate;
- determinare il tempo necessario per compiere le operazioni che non può in ogni caso superare i 15 giorni. Tale termine è comunque prorogabile dal giudice, con decreto motivato e su richiesta del PM, per periodi successivi di 15 giorni, sempre che permangano le condizioni che ne hanno determinato l'adozione.

La norma chiarisce, altresì, che l'autorizzazione è concessa dal giudice solo previa effettuazione delle valutazioni prescritte dall'art. 5, par. 2 Regolamento UE n. 2024/1689.

Nello specifico, l'art. 5, par. 2 dispone che l'utilizzo di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto di cui alla par. 1, *lett. h* (ricerca vittime di determinati reati, prevenzione di una minaccia alla vita o all'incolumità delle persone fisiche ovvero di una minaccia reale di un attacco terroristico, localizzazione o identificazione di persona indiziata di aver commesso uno dei reati di cui all'Allegato II) è consentito solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:

- a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del pregiudizio che discenderebbe dal mancato uso del sistema;
- b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

Sempre l'art. 5, par. 2 stabilisce, inoltre, che l'adozione dei predetti sistemi deve rispettare le tutele e le condizioni, necessarie e proporzionate in relazione al loro utilizzo, in conformità al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. Peraltro, l'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico può essere impiegato per compiere le suddette operazioni solo dopo che l'autorità di contrasto ha proceduto ad una valutazione circa l'impatto sui diritti fondamentali ai sensi dell'art. 27 del regolamento ("Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio") e dopo che abbia registrato il sistema di IA nella banca dati UE ai sensi dell'art. 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo.

Il **comma 7** disciplina i casi in cui può essere disposto l'utilizzo dei sistemi di IA di rilevazione biometrica in situazioni di urgenza. In particolare, si prevede che quando ricorrono **situazioni di urgenza** e vi è fondato motivo di ritenere che **dal ritardo** possa derivare **pregiudizio grave e irreparabile** per le operazioni descritte dai commi precedenti (cfr. commi da 1 a 4), l'utilizzo dei sistemi di IA possa essere autorizzato con **decreto motivato del PM**. La norma precisa che, in ogni caso, il pubblico ministero possa adottare il suddetto provvedimento solamente nei casi in cui sono presenti le **condizioni** di cui al precedente comma 6, secondo periodo (v. *supra*).

Occorre rilevare che il secondo periodo del comma 6 individua il contenuto dell'autorizzazione mentre il terzo periodo concerne le condizioni che consentono l'adozione dell'autorizzazione.

Si valuti l'opportunità di aggiornare il riferimento normativo.

Il decreto è comunicato immediatamente e comunque non oltre 24 ore al GIP, il quale lo convalida, se ricorrono i presupposti, non oltre le successive 24 ore e autorizza la prosecuzione dell'attività investigativa.

Si stabilisce, inoltre, che qualora nelle **medesime situazioni di urgenza non sia possibile attendere il provvedimento del PM**, all'attivazione dei sistemi di identificazione biometrica **procedono gli ufficiali di polizia giudiziaria**. Questi ultimi, senza ritardo e comunque **entro le successive 12 ore**, trasmettono la **richiesta** di autorizzazione **al PM**, il quale, se ne ricorrono i presupposti, **richiede al giudice la convalida entro 24 ore dall'avvio del sistema**. Il **giudice**, se ritiene sussistenti i presupposti **convalida il decreto di autorizzazione del PM entro le successive 48 ore**, nonché autorizza la prosecuzione dell'attività, con le indicazioni di cui al comma 6 (v. *supra*).

Come sottolineato dalla **relazione illustrativa**, l'autorizzazione all'impiego di sistemi di IA per la rilevazione biometrica remota in tempo reale in ipotesi di urgenza si articola in un meccanismo di doppia convalida analogo a quello previsto dall'art. 267, comma 2 c.p.p. in materia di intercettazioni. In particolare, quest'ultima disposizione stabilisce che nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il PM dispone l'intercettazione con decreto motivato, che va comunicato immediatamente e comunque non oltre le 24 ore al GIP. Il giudice, entro 48 ore dall'adozione del provvedimento, decide sulla convalida con decreto motivato. Se il decreto del PM non viene convalidato nel termine stabilito, l'intercettazione non può essere proseguita e i risultati acquisiti non possono essere utilizzati.

Appare opportuno sottolineare che per i casi di intercettazioni urgenti non è prevista una disciplina analoga a quella prescritta in questa sede dal comma 7, secondo periodo che consente agli ufficiali di polizia giudiziaria di attivare direttamente il sistema di identificazione biometrica remota in tempo reale allorquando non sia possibile attendere il provvedimento del PM.

Il **comma 8** dispone che i risultati ottenuti dai sistemi di intelligenza artificiale non possono essere utilizzati qualora gli stessi siano stati impiegati fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni procedurali prescritte dai commi 6 e 7 (v. *supra*). 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
***(Modifica alle norme di attuazione, di coordinamento e transitorie
del codice di procedura penale)***

L'**articolo 14**, intervenendo sull'art. 104, comma 1, delle norme di attuazione del codice di procedura penale, è volto a consentire il **sequestro preventivo dei contenuti online generati con sistemi di intelligenza artificiale**.

La modifica interviene su una disposizione recentemente introdotta ad opera del decreto-legge 23/2026 (art. 2, comma 2-*bis*), ovvero la lettera *e-bis*) dell'art. 104, comma 1, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al d.lgs. 271/1989.

La lettera citata ha inserito, tra le cose sottoponibili a sequestro preventivo, i contenuti *online* del profilo personale e i relativi dati. L'intervento emendativo recato dall'articolo in commento, volto a dare attuazione al **criterio di delega contenuto all'art. 24, comma 5, lett. a), della legge 132/2025 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale)**, precisa che tali **contenuti online**, non più necessariamente afferenti al profilo personale, sono **sottoponibili a sequestro anche se generati attraverso l'utilizzo di sistemi di IA**, senza specificare, come previsto dal criterio di delega, che tali contenuti devono essere stati generati illecitamente.

Restano ferme le **modalità di esecuzione del sequestro** descritte nella lettera *e-bis*): il sequestro avviene tramite un **ordine di rimozione** dei contenuti e dei dati o un **ordine di inabilitazione dell'accesso** al profilo, fatta salva la possibilità di consentire la fruizione dei contenuti estranei alle condotte illecite, se tecnicamente possibile. L'ordine è rivolto ai prestatori di servizi di *hosting*, ai fornitori di piattaforme on line o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione, individuati sulla base della definizione di servizio di cui all'art. 1, par. 1, lett. b), della direttiva 2015/1535, vale a dire «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

Il **sequestro preventivo** è una misura cautelare reale, prevista dall'art. 321 c.p.p., che viene disposta dal giudice, su richiesta del PM, per impedire che la libera disponibilità di una cosa pertinente a un reato possa aggravare le conseguenze del reato stesso, prostrarle o facilitarne altri. L'art. 104 disp. att. c.p.p. contiene l'**elenco delle cose sulle quali può essere eseguito il sequestro preventivo** ovvero:

a) sui mobili e sui crediti;

- b) sugli immobili o mobili registrati;
- c) sui beni aziendali organizzati per l'esercizio di un'impresa;
- d) sulle azioni e sulle quote sociali;
- e) sugli strumenti finanziari dematerializzati, ivi compresi i titoli del debito pubblico;
- e-bis) sui contenuti online del profilo personale e sui relativi dati.

Norme di attuazione, coordinamento e transitorie del codice di procedura penale (D.Lgs. 271/1989)	
Testo vigente	Modificazioni apportate dall'art. 14 dell'AG 418
Art. 104 (Esecuzione del sequestro preventivo)	Art. 104 (idem)
1. Il sequestro preventivo è eseguito:	1. <i>Identico:</i>
a) sui mobili e sui crediti, secondo le forme prescritte dal codice di procedura civile per il pignoramento presso il debitore o presso il terzo in quanto applicabili;	a) <i>identica;</i>
b) sugli immobili o mobili registrati, con la trascrizione del provvedimento presso i competenti uffici;	b) <i>identica;</i>
c) sui beni aziendali organizzati per l'esercizio di un'impresa, oltre che con le modalità previste per i singoli beni sequestrati, con l'immissione in possesso dell'amministratore, con l'iscrizione del provvedimento nel registro delle imprese presso il quale è iscritta l'impresa;	c) <i>identica;</i>
d) sulle azioni e sulle quote sociali, con l'annotazione nei libri sociali e con l'iscrizione nel registro delle imprese;	d) <i>identica;</i>
e) sugli strumenti finanziari dematerializzati, ivi compresi i titoli del debito pubblico, con la registrazione nell'apposito conto tenuto dall'intermediario ai sensi dell'articolo 34 del decreto legislativo 24 giugno	e) <i>identica;</i>

1998, n. 213. Si applica l'articolo 10, comma 3, del decreto legislativo 21 maggio 2004, n. 170;	
e-bis) sui contenuti online del profilo personale e sui relativi dati, mediante ordine ai prestatori di servizi di hosting, ai fornitori di piattaforme online o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione quali definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di rimuovere i contenuti e i dati o disabilitare l'accesso al profilo, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite.	e-bis) sui contenuti online generati anche con sistemi di intelligenza artificiale e sui relativi dati, mediante ordine ai prestatori di servizi di hosting, ai fornitori di piattaforme online o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione quali definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di rimuovere i contenuti e i dati o disabilitare l'accesso al profilo, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite.
2. Si applica altresì la disposizione dell'articolo 92.	2. <i>Identico.</i>

Articolo 15

(Modifiche alla responsabilità amministrativa degli enti)

L'**articolo 15** apporta modifiche alla disciplina concernente la responsabilità amministrativa degli enti, ricomprendendo tra i cd. reati presupposto le fattispecie di “Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi” (art. 437-*bis* c.p.) e di “Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale” (art. 612-*quater* c.p.). La norma, inoltre, regola le sanzioni applicabili agli enti nel caso di commissione dei suddetti reati.

L'**articolo 15** introduce il nuovo art. 25-*vicies* all'interno del D.lgs. n. 231 del 2001 che prevede quali nuovi reati presupposto per la configurazione della responsabilità amministrativa degli enti i “**reati commessi con l'uso di sistemi di intelligenza artificiale**”.

La **relazione illustrativa** evidenzia come attraverso la norma in esame viene data attuazione al criterio di delega contenuto all'art. 24, comma 5, *lett. c)* della L. n. 132 del 2025 (“Deleghe al Governo in materia di intelligenza artificiale”). Nel dettaglio, tale norma prevede quale criterio di delega la “precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente”.

Nello specifico, il **comma 1** dispone che qualora risulti commesso il delitto, introdotto dallo schema in esame, di “Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi” di cui all'**art. 437-*bis* c.p.** (v. scheda di lettura articolo 12 per maggior approfondimento), nell'interesse o a vantaggio della persona giuridica, a quest'ultima si applica la **sanzione amministrativa pecuniaria da 600 a 1000 quote**.

Per quanto concerne la cornice editale, la **relazione illustrativa** spiega che la forbice sanzionatoria si colloca nella “fascia alta del catalogo” delle sanzioni, riflettendo la gravità della lesione posta in essere. Il parametro di riferimento è offerto dall'art. 25-*septies* del D.lgs. n. 231 del 2001, inerente al reato presupposto dell'Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, ove si stabilisce l'applicazione di una sanzione pecuniaria fino a 1000 quote.

Il **comma 2**, invece, stabilisce che nel caso di commissione del delitto di “Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza

artificiale” di cui all’**art. 612-quater c.p.**, nell’interesse o a vantaggio dell’ente, quest’ultimo sia punito con la **sanzione amministrativa pecuniaria da 200 a 700 quote**.

Si ricorda che l’art. 612-quater c.p., introdotto dall’art. 26, comma 1, *lett. c)* della L. n. 132 del 2025 (“Disposizioni e deleghe al Governo in materia di intelligenza artificiale”), punisce con la reclusione da 1 a 5 anni chiunque cagioni ad una persona un danno ingiusto attraverso la cessione, la pubblicazione ovvero la diffusione, senza l’altrui consenso, di immagini, video o voci falsificati o alterati mediante l’utilizzo di sistemi di intelligenza artificiale e idonei a indurre in inganno con riferimento alla loro genuinità. La norma, inoltre, stabilisce il regime di punibilità a querela della persona offesa per il predetto reato. Tuttavia, è prescritta la procedibilità d’ufficio se il fatto è connesso con un ulteriore delitto per il quale si deve procedere d’ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, ovvero nei riguardi di una pubblica autorità a causa delle funzioni esercitate.

Infine, il **comma 3** regola le **sanzioni amministrative interdittive** applicabili alla persona giuridica nelle ipotesi di commissione dei reati *ex artt. 437-bis c.p. e 612-quater c.p.*

In particolare, è prescritta l’applicazione delle seguenti sanzioni interdittive:

- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito (art. 9, comma 2, *lett. b)* del D.lgs. n. 231 de 2001);
- divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio (art. 9, comma 2, *lett. c)* del D.lgs. n. 231 de 2001);
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l’eventuale revoca di quelli già concessi (art. 9, comma 2, *lett. d)* del D.lgs. n. 231 de 2001);
- divieto di pubblicizzare beni o servizi (art. 9, comma 2, *lett. e)* del D.lgs. n. 231 de 2001).

La **relazione illustrativa** chiarisce che tra le sanzioni interdittive applicabili non è presente quella *sub* art. 9, comma 2, *lett. a)*, ossia l’interdizione dell’esercizio dell’attività in ragione del principio di proporzionalità. Infatti, in tal modo “si privilegiano le misure incidenti sull’operatività dell’ente nei settori connessi all’illecito, evitando la sanzione integralmente paralizzante dell’attività”.

• **La responsabilità amministrativa degli enti ex D.lgs. n. 231 del 2001**

Il D.lgs. n. 231/2001 ha introdotto una forma di **responsabilità amministrativa dell'ente**, distinta dalla responsabilità penale della persona fisica che ha materialmente commesso il reato, muovendosi lungo due direttrici principali: da un lato, utilizzando la tecnica del reato presupposto al fine di imputare all'ente una responsabilità propria e, dall'altro, richiedendo l'implementazione di un modello aziendale capace di sollevare l'ente dalla propria responsabilità.

Si ricorda che il **reato presupposto** è quello senza la commissione del quale non potrebbe essere commesso un secondo reato che trova per l'appunto in esso il proprio presupposto. Nel caso delle persone giuridiche, il comportamento illecito messo in atto da uno o più soggetti che rivestano una posizione di vertice all'interno dell'ente, o da soggetti sottoposti a direzione o vigilanza da parte dei primi, riveste la qualità di reato presupposto, sul quale si innesta la responsabilità amministrativa della persona giuridica. **La responsabilità dell'ente e quella dell'autore del reato presupposto rimangono comunque ben distinte**: quest'ultimo sarà chiamato a rispondere penalmente per il reato presupposto, mentre l'ente risponderà sotto forma di sanzione amministrativa per aver consentito la commissione, da parte di uno dei suoi membri, di un reato. Da ciò discende il permanere della responsabilità in capo all'ente anche qualora l'autore del reato non fosse stato identificato, non fosse imputabile ovvero nel caso in cui il reato si fosse estinto per una causa diversa dall'amnistia. Inoltre, a norma dell'art. 5 del D.lgs. n. 231 del 2001, per la configurazione della responsabilità amministrativa in capo all'ente si richiede che il reato sia commesso nel suo interesse ovvero a suo vantaggio dai soggetti prima richiamati. Infatti, l'ente non è chiamato a rispondere dei fatti commessi nell'interesse proprio del soggetto agente ovvero nell'interesse di terzi.

D'altro canto, il legislatore ha previsto la possibilità per l'ente di esimersi da responsabilità attraverso l'implementazione di un **modello aziendale efficace ad evitare**, o quantomeno a ridurre, **la possibilità che siano commessi reati da parte dei suoi vertici o di coloro che sono ad essi sottoposti**. Tale modello è delineato negli articoli 6 e 7 del d.lgs. 231/2001. L'art. 6 prende in considerazione i reati commessi da soggetti che rivestono nell'ente una posizione apicale, escludendo la responsabilità dell'ente stesso qualora questo provi di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi. I modelli organizzativi devono preliminarmente individuare le attività nel cui ambito possono essere commessi reati, al fine di adottare specifici protocolli volti alla prevenzione dei reati stessi, devono stabilire le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati e prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello. Oltre all'implementazione di un simile modello organizzativo, per evitare la sanzione l'ente deve altresì provare che non vi sia stata omessa o

insufficiente vigilanza da parte dell'organismo a ciò preposto, che deve essere dotato di autonomi poteri di iniziativa e di controllo e che, oltre a vigilare su tali modelli, deve provvedere al loro aggiornamento e che coloro che hanno commesso il reato lo hanno fatto eludendo fraudolentemente i modelli di organizzazione e di gestione adottati. A seguito della modifica introdotta dalla legge 30 novembre 2017, n. 179 (c.d. *whistleblowing*), è inoltre richiesto che i modelli di organizzazione includano anche sistemi che consentano la segnalazione, da parte sia dei soggetti in posizione apicale, sia dei soggetti sottoposti, di illeciti di cui siano venuti a conoscenza in ragione delle funzioni svolte. Il modello deve essere impostato in modo tale che sia garantita la riservatezza dell'identità del segnalante e deve prevedere espressamente il divieto di atti ritorsione o discriminatori nei suoi confronti. La nullità del licenziamento ritorsivo o discriminatorio è invece prevista *ex lege*.

Nel caso di reati commessi da soggetti sottoposti all'altrui direzione, di cui all'art. 7, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, ma è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. Tale modello deve prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio e deve comprendere attività di verifica periodica sull'efficacia del modello (e conseguentemente una sua eventuale modifica) ed un idoneo apparato sanzionatorio.

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** estende l'accesso probatorio a ogni azione risarcitoria da IA, limitando le presunzioni legali di causalità alle sole violazioni degli obblighi del Regolamento (UE) 2024/1689. La norma assicura la coerenza eurounitaria facendo salve le tutele del GDPR e della responsabilità da prodotto difettoso, evitando riduzioni delle garanzie previste dagli statuti speciali. Introduce infine il foro aggiuntivo del consumatore presso la propria residenza o domicilio, correggendo l'asimmetria informativa e logistica tra utente individuale e fornitore del sistema.

Il **comma 1** dell'articolo 16 dello schema di decreto legislativo definisce l'ambito di applicazione oggettivo e soggettivo delle norme processuali introdotte per agevolare l'accertamento della responsabilità civile derivante dall'impiego di sistemi algoritmici. Tale disposizione stabilisce che la disciplina contenuta nel successivo articolo 17, relativa alle modalità di accesso agli elementi di prova, trovi applicazione in tutte le controversie volte a ottenere il **risarcimento del danno cagionato nell'utilizzo di un sistema di intelligenza artificiale**, abbracciando in modo onnicomprensivo sia le fattispecie di **responsabilità contrattuale** sia quelle di natura **extracontrattuale**. La norma funge da raccordo procedurale necessario per superare l'asimmetria informativa che caratterizza il rapporto tra danneggiato e utilizzatore o fornitore del sistema, rendendo operativi gli strumenti di *disclosure* probatoria ogniqualvolta la pretesa risarcitoria sia fondata sugli effetti dannosi prodotti dall'output o dal malfunzionamento di un'IA.

Il quadro normativo delle azioni di risarcimento si articola su un sistema multilivello che integra la disciplina codicistica nazionale con le recenti riforme europee, in particolare il **Regolamento (UE) 2024/1689 (AI Act)** e la **Direttiva (UE) 2024/2853** in materia di responsabilità da prodotto difettoso. Sotto il profilo della **responsabilità contrattuale**, il fondamento dell'azione risiede nell'articolo 1218 c.c., che sanziona l'inadempimento delle obbligazioni inerenti all'esercizio di un'attività professionale. In questo contesto, l'evoluzione tecnologica impone una rimeditazione della **diligenza professionale ex articolo 1176, comma 2, c.c.**,

che declina verso una vera e propria "**diligenza algoritmica**". Tale parametro obbliga il professionista a una scelta consapevole di sistemi affidabili e a una verifica critica dei risultati prodotti, al fine di evitare che l'utilizzo acritico di output errati si traduca in una prestazione negligente. La giurisprudenza di merito ha già iniziato a sanzionare, sebbene prevalentemente sul piano della responsabilità processuale aggravata ex art. 96 c.p.c., la condotta di avvocati che hanno presentato in giudizio atti contenenti citazioni inesistenti generate da IA, le cosiddette "allucinazioni algoritmiche" (**Trib. Torino, 16 settembre 2025, n. 2120; Trib. Latina, 23 settembre 2025; Trib. Siracusa, 20 febbraio 2026**). Per l'esplicito riferimento all'utilizzo dell'intelligenza artificiale generativa nella redazione degli atti processuali occorre da ultimo rammentare **l'ordinanza Cass., Sez. VII pen., n. 11431/2026**. In tale ordinanza la Corte censura il fenomeno delle *hallucinations* dell'intelligenza artificiale, richiamando implicitamente il dovere del difensore di verificare l'attendibilità delle fonti giuridiche utilizzate negli atti giudiziari. In un caso, si è esclusa la responsabilità aggravata laddove l'errore dell'IA non fosse sintomatico di malafede ma diretto a rafforzare una linea difensiva già nota (**Trib. Firenze, 14 marzo 2025**).

Nell'alveo della **responsabilità extracontrattuale**, il sistema si sposta verso modelli di natura oggettiva o aggravata per rispondere all'opacità del fenomeno tecnologico. L'**articolo 2050 c.c.**, relativo all'esercizio di attività pericolose, appare particolarmente idoneo a disciplinare i danni derivanti da **sistemi di IA ad alto rischio**, poiché la pericolosità intrinseca di tali strumenti sposta l'onere della prova sulla capacità del convenuto di aver adottato tutte le misure idonee a evitare l'evento. Parallelamente, l'**articolo 2051 c.c.** sulla responsabilità da cosa in custodia viene invocato laddove l'utilizzatore mantenga il controllo effettivo sul sistema, sebbene la dottrina discuta se il controllo remoto del produttore possa elidere tale nesso. Per quanto concerne la **circolazione dei veicoli autonomi**, il quadro normativo si fonda sull'**articolo 2054 c.c.**, che al comma 4 stabilisce una responsabilità "blindata" e oggettiva del proprietario e del conducente per i danni derivanti da vizi di costruzione, lasciando a questi ultimi la possibilità di agire in regresso verso il produttore.

A livello unionale, la nuova Direttiva PL (2024/2853) ha esteso la nozione di **prodotto** includendovi espressamente i **software e i file per la fabbricazione digitale**, consolidando un regime di responsabilità oggettiva del produttore per i danni causati da difetti dei sistemi di IA. La prova della difettosità e del nesso causale può essere facilitata da presunzioni semplici, come già ammesso dalla giurisprudenza di legittimità in ambiti complessi (**Cass. civ. n. 13458/2013; Cass. civ. n. 34027/2022**) e dalla Corte di Giustizia UE, la quale ha affermato che la difettosità può essere presunta in presenza di un malfunzionamento di prodotti della stessa serie (**Corte Giust. UE, 5 marzo 2015, cause riunite C-503/13 e C-504/13**). Infine, l'adempimento agli obblighi di trasparenza e sorveglianza umana previsti dall'AI Act funge da parametro per valutare la colpa del *deployer*, pur non escludendo di per sé la responsabilità in caso di danno effettivo.

Il **comma 2** dell'articolo 16 dello schema di decreto legislativo configura una **clausola di condizionalità processuale** volta a raccordare la disciplina

risarcitoria nazionale con l'apparato sanzionatorio e regolatorio dell'Unione Europea. Tale disposizione stabilisce che i meccanismi agevolativi previsti dagli articoli 18 e 19 trovino applicazione nelle azioni di risarcimento del danno — sia di natura contrattuale che extracontrattuale — esclusivamente qualora il pregiudizio patito derivi direttamente dalla **violazione di uno o più obblighi prescritti dal Regolamento (UE) 2024/1689**. Sotto il profilo tecnico-giuridico, la norma delimita rigorosamente l'ambito di operatività delle presunzioni legali, ancorandole non alla mera occorrenza di un danno nell'utilizzo di un'IA, bensì alla specifica inosservanza dei precetti comportamentali, di sicurezza o di trasparenza stabiliti dal legislatore unionale.

L'**articolo 18 dello schema**, richiamato dalla disposizione in esame, introduce una significativa deroga all'onere probatorio ordinario in materia di **nesso di causalità**. La norma stabilisce una **presunzione iuris tantum** (relativa), operante nel caso in cui il danno sia conseguenza della violazione degli obblighi del Regolamento IA: in tale ipotesi, il collegamento eziologico tra la condotta inadempiente e l'evento lesivo è presunto, sollevando il danneggiato dalla necessità di ricostruire l'iter logico-tecnico che ha portato il sistema a produrre un output dannoso. Resta comunque ferma la facoltà per il convenuto di fornire la **prova contraria**, dimostrando l'interruzione del nesso causale o l'intervento di fattori esterni idonei a escludere la propria responsabilità.

L'**articolo 19 dello schema** completa il quadro normativo disciplinando la **rilevanza della conformità** del sistema di intelligenza artificiale ai parametri europei. La disposizione sancisce espressamente che la conformità del sistema agli obblighi previsti dal Regolamento (UE) 2024/1689 **non esclude di per sé la responsabilità del convenuto**. Tale principio si applica anche laddove la conformità sia stata formalmente **certificata** ai sensi delle procedure di valutazione previste dal Capo III, Sezione 5 del Regolamento medesimo. In tal modo, il legislatore nazionale intende chiarire che l'adempimento formale agli standard tecnici e regolamentari non costituisce un esimente automatico né una "clausola di salvaguardia" assoluta, qualora l'utilizzo concreto del sistema IA produca comunque un danno ingiusto meritevole di ristoro.

Sebbene la norma nazionale non enumeri analiticamente ogni singolo precetto unionale, essa opera un rinvio recettizio all'intero apparato di doveri e requisiti che il legislatore europeo ha imposto ai vari attori della catena del valore dell'intelligenza artificiale, differenziandoli in base al livello di rischio del sistema.

In primo luogo, rilevano i **divieti assoluti relativi alle pratiche di IA inaccettabili** disciplinati dall'articolo 5 dell'AI Act, i quali proibiscono, tra l'altro, l'impiego di tecniche subliminali, manipolative o ingannevoli volte a distorcere materialmente il comportamento umano in modo da causare danni significativi, nonché lo sfruttamento delle vulnerabilità di persone fisiche o

gruppi. La violazione di tali divieti costituisce un presupposto fondamentale per l'attivazione dei meccanismi probatori agevolati previsti dal decreto nazionale.

Per quanto concerne i **sistemi di IA ad alto rischio**, il Regolamento impone una serie di requisiti tecnici e organizzativi stringenti che fungono da parametro per valutare la condotta del fornitore e del distributore. Tra questi obblighi rientrano l'istituzione e il mantenimento di un **sistema di gestione dei rischi** per l'intero ciclo di vita del prodotto (Articolo 9), l'adozione di pratiche di **governance dei dati** per garantire che i set di addestramento siano pertinenti e privi di distorsioni (Articolo 10) e la redazione di una **documentazione tecnica** dettagliata che dimostri la conformità (Articolo 11). Sono inoltre richiamati gli obblighi di **registrazione automatica degli eventi (logging)** per garantire la tracciabilità (Articolo 12) e il dovere di garantire la **trasparenza algoritmica**, fornendo ai deployer informazioni che permettano di interpretare correttamente gli output (Articolo 13).

Un rilievo centrale assumono le disposizioni sulla **sorveglianza umana** (Articolo 14), che impongono ai fornitori di progettare sistemi supervisionabili da persone fisiche e ai deployer di affidare tale compito a personale competente, dotato dell'autorità di annullare o ribaltare le decisioni algoritmiche. A completare il quadro dei sistemi ad alto rischio intervengono gli obblighi relativi ai livelli di **accuratezza, robustezza e cibersicurezza** (Articolo 15).

Si devono altresì ritenere richiamati gli **obblighi specifici in capo ai deployer** (Articolo 26), i quali sono tenuti ad adottare misure tecniche e organizzative per utilizzare i sistemi conformemente alle istruzioni ricevute, a monitorarne costantemente il funzionamento sospendendone l'uso in caso di rischio e a garantire la pertinenza dei dati di input. Infine, si possono ritenere compresi anche gli **obblighi di trasparenza per determinati sistemi di IA** (Articolo 50), quali il dovere di informare le persone fisiche quando interagiscono con un'IA, l'obbligo di contrassegnare gli output generati artificialmente, come i "deep fake", e il dovere di segnalare l'utilizzo di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica

Il **comma 3** dell'articolo 16 dello schema di decreto legislativo configura una **clausola di salvezza** di natura tecnico-normativa, volta a garantire la coerenza del nuovo intervento con il quadro giuridico eurolunitario preesistente. Sotto il profilo tecnico-giuridico, la disposizione sancisce l'impregiudicabilità delle tutele apprestate da specifici regimi speciali di responsabilità, impedendo che l'introduzione delle nuove norme processuali in materia di intelligenza artificiale determini effetti di restrizione o di deroga tacita a statuti protettivi già consolidati nell'ordinamento.

Nello specifico, la norma richiama e mantiene ferme le disposizioni contenute nell'**articolo 82 del Regolamento (UE) 2016/679 (GDPR)**, il quale disciplina il diritto al risarcimento e la responsabilità civile del titolare o del responsabile del trattamento per i danni cagionati da operazioni di trattamento dei dati personali non conformi al medesimo regolamento.

Contestualmente, il comma in esame fa salva l'operatività della normativa nazionale di recepimento della **Direttiva (UE) 2024/2853**, relativa alla responsabilità per danno da prodotti difettosi, assicurando così che il danneggiato possa continuare ad azionare i rimedi previsti dallo statuto speciale del produttore laddove il sistema di intelligenza artificiale integri i requisiti di difettosità previsti dalla fonte unionale.

L'**articolo 82 del Regolamento (UE) 2016/679 (GDPR)** disciplina in modo organico il **diritto al risarcimento e la responsabilità civile** derivante da operazioni di trattamento dei dati personali effettuate in violazione delle prescrizioni del regolamento medesimo. La disposizione stabilisce il principio cardine secondo cui chiunque subisca un danno materiale o immateriale a causa di un'infrazione del GDPR ha il diritto di ottenere il ristoro del pregiudizio patito dal titolare del trattamento o dal responsabile del trattamento.

Sotto il profilo dei criteri di imputazione, il titolare risponde del danno cagionato dal trattamento che violi il regolamento, mentre il responsabile è chiamato a rispondere solo se non ha adempiuto agli obblighi specificamente diretti ai responsabili o se ha agito in modo difforme o contrario alle istruzioni del titolare [Contesto generale basato sui richiami normativi]. La norma configura un modello di **responsabilità aggravata**, prevedendo che il titolare o il responsabile siano esonerati esclusivamente qualora riescano a dimostrare che l'evento dannoso **non è loro in alcun modo imputabile**. Un aspetto fondamentale sottolineato dalle fonti riguarda l'attribuzione di **rimedi individuali effettivi**, garantendo ai singoli e ai gruppi interessati un autonomo diritto di azione per ottenere il risarcimento, a differenza di quanto inizialmente previsto da altri quadri normativi europei in materia tecnologica. All'interno dell'ordinamento nazionale, l'operatività di tale regime speciale viene espressamente fatta salva dall'**articolo 16, comma 3, dello schema di decreto legislativo** sull'intelligenza artificiale. Questa clausola di salvezza assicura che le nuove tutele processuali civili non determinino una riduzione del livello di protezione già garantito dal GDPR, operando secondo una logica di **piena complementarità** tra lo statuto della protezione dei dati e la nuova disciplina sulla responsabilità algoritmica.

La normativa nazionale di recepimento della **Direttiva (UE) 2024/2853**, la cui attuazione deve completarsi entro il **9 dicembre 2026**, costituisce un pilastro fondamentale del sistema di **responsabilità oggettiva del produttore** adattato alle sfide dell'economia digitale. L'operatività di tale regime speciale viene espressamente preservata dall'**articolo 16, comma 3, dello schema di decreto legislativo** sull'intelligenza artificiale attraverso una **clausola di salvezza** che impedisce ogni effetto di restrizione o deroga tacita alle tutele già esistenti o in via di consolidamento. Sotto il profilo sostanziale, la nuova disciplina **amplia la nozione di prodotto** includendovi esplicitamente il **software** e i sistemi di intelligenza artificiale, garantendo così che il danneggiato possa invocare il regime di responsabilità senza l'onere della prova della colpa ogniqualvolta il sistema presenti un difetto di sicurezza. Il contenuto innovativo della normativa si riflette nella rimodulazione del concetto di **difetto**, il quale viene ora valutato alla

luce del *consumer expectation test* integrato con i rischi specifici dell'IA, quali la capacità di **auto-apprendimento post-commercializzazione** e l'interazione dinamica con altri ecosistemi digitali. Un rilievo centrale assume la persistenza della responsabilità del fabbricante nelle ipotesi in cui mantenga un **controllo effettivo** sul sistema tramite aggiornamenti o servizi correlati, rendendolo responsabile anche per i **difetti sopravvenuti** alla messa in servizio. Sul piano processuale, la disciplina introduce strumenti di **disclosure probatoria** che permettono al giudice di ordinare l'esibizione di prove pertinenti in capo al convenuto, facilitando il superamento dell'**asimmetria informativa** tipica del settore tecnologico. Tale meccanismo è supportato da un articolato sistema di **presunzioni legali iuris tantum** che sollevano l'attore dall'onere di dimostrare la difettosità o il nesso causale in casi di **elevata complessità tecnica o scientifica**, purché la domanda risarcitoria sia ritenuta plausibile e il danno sia coerente con il malfunzionamento allegato. Infine, la normativa estende la platea dei legittimati passivi a un'ampia categoria di **operatori economici**, tra cui importatori, distributori e gestori di piattaforme, stabilendo una **responsabilità solidale** volta a garantire l'effettività del risarcimento indipendentemente dalla localizzazione geografica del produttore originale.

Il **comma 4** introduce una specifica **regola di competenza territoriale derogatoria** volta a rafforzare la tutela del danneggiato che rivesta la qualifica di **consumatore**. La disposizione stabilisce che, nelle azioni di risarcimento del danno — sia di natura contrattuale che extracontrattuale — derivanti dall'utilizzo di sistemi di intelligenza artificiale, qualora il soggetto leso sia una **persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale** eventualmente svolta, la competenza spetti altresì al **giudice del luogo in cui il danneggiato ha la residenza o il domicilio**.

Sotto il profilo tecnico-giuridico, tale previsione configura un **foro speciale alternativo**, che si ispira al modello delineato dall'articolo 66-bis del Codice del Consumo, distinguendosi tuttavia per la sua natura non esclusiva, in quanto si pone come criterio di collegamento **aggiuntivo** rispetto ai criteri ordinari di competenza previsti dal codice di procedura civile. La *ratio legis* dell'intervento risiede nella necessità di garantire l'effettività della tutela giurisdizionale assicurando la **prossimità del giudice** rispetto alla vittima in controversie caratterizzate da un'elevata complessità tecnica, nelle quali l'**asimmetria di posizione** tra l'utente individuale e il fornitore o deployer del sistema algoritmico è particolarmente marcata. In questo scenario, il legislatore intende facilitare l'accesso alla giustizia per la parte debole, evitando che gli oneri logistici legati alla celebrazione del giudizio in fori remoti possano pregiudicare il ristoro del danno patito a causa dell'opacità dei sistemi di IA.

Articolo 17 (Accesso alle prove)

L'**articolo 17** introduce un meccanismo di esibizione delle prove volto a superare l'asimmetria informativa nei contenziosi relativi ai sistemi di IA, consentendo al giudice di ordinare l'accesso a documenti e dati tecnici pertinenti quando il danneggiato dimostri la verosimiglianza della propria domanda. La norma individua le principali categorie di documentazione rilevante (*logging*, gestione dei rischi, documentazione tecnica e sorveglianza umana), imponendo il rispetto dei principi di necessità, proporzionalità e tutela dei segreti commerciali. Sono inoltre previste conseguenze processuali e sanzioni in caso di mancata ottemperanza all'ordine di esibizione, al fine di garantire l'effettività della tutela risarcitoria.

L'**articolo 17, comma 1**, dello schema di decreto legislativo disciplina lo strumento processuale cardine volto a superare l'**asimmetria informativa** e l'**opacità tecnologica** che gravano sul soggetto danneggiato dall'impiego di sistemi algoritmici. La norma attribuisce al giudice il potere di ordinare, su istanza della parte che allega di aver subito il pregiudizio, l'**esibizione di elementi di prova specificamente pertinenti** relativi al funzionamento del sistema di intelligenza artificiale. Tale ordine può essere diretto non solo alla controparte processuale, ma anche a un **terzo che ne disponga**, assicurando così una *disclosure* probatoria ampia e funzionale alla ricostruzione dei fatti.

L'attivazione di questo meccanismo istruttorio è subordinata a un preciso onere di allegazione in capo all'istante, il quale deve presentare fatti ed elementi idonei a rendere **verosimile la fondatezza della domanda**, con particolare riguardo al nesso eziologico tra il risultato prodotto dall'IA e il danno lamentato. Lo standard della **verosimiglianza** rappresenta una scelta deliberata del legislatore per calibrare l'accesso alle prove in un contesto di oggettiva difficoltà probatoria, evitando al contempo istanze meramente esplorative.

Come precisato dalla **Relazione illustrativa**, tale scelta normativa risponde alla necessità di superare l'oggettiva **asimmetria informativa** e l'**opacità tecnologica** proprie dei sistemi algoritmici, recependo in tal senso le indicazioni contenute nella proposta di direttiva unionale sulla responsabilità civile da intelligenza artificiale, nonostante il suo formale ritiro. La disposizione si configura come un presupposto operativo essenziale per l'effettività delle tutele in sede civile, applicandosi in modo uniforme a tutte le azioni risarcitorie

indipendentemente dal titolo della pretesa, sia essa di natura **contrattuale o extracontrattuale**. In merito alle condizioni di attivazione di tale strumento, sempre la **Relazione illustrativa** chiarisce che il potere del giudice di ordinare l'esibizione di prove pertinenti relative al funzionamento del sistema di IA — ordine che può essere rivolto alla controparte o a un terzo — è subordinato alla sussistenza di uno standard di **verosimiglianza**. L'istante deve infatti presentare fatti ed elementi idonei a rendere plausibile la fondatezza della domanda, con specifico riguardo al collegamento eziologico tra l'*output* prodotto dal sistema e il danno patito. Questo standard è stato deliberatamente prescelto dal legislatore per calibrare l'accesso alle informazioni tecniche in un contesto di estrema difficoltà probatoria, evitando al contempo istanze meramente esplorative che possano pregiudicare la **riservatezza** o i **segreti commerciali** dei soggetti coinvolti.

Sotto il profilo degli effetti, la **Relazione tecnica** sottolinea la neutralità finanziaria della norma, osservando che l'intervento si limita a disciplinare i mezzi probatori e la ripartizione dell'onere istruttorio senza istituire nuovi uffici o funzioni amministrative. Il legislatore nazionale ha inteso così valorizzare la funzione probatoria dei documenti e dei registri (*logging*) previsti dal Regolamento (UE) 2024/1689, assicurando che la complessità intrinseca del software e le dinamiche di apprendimento automatico del sistema (*machine learning*) non impediscano al danneggiato di ricostruire la dinamica dell'evento lesivo. In definitiva, l'istituto garantisce che la *compliance* regolatoria si traduca in una reale accessibilità degli elementi di prova, rendendo il sistema di responsabilità civile compatibile con le sfide dell'economia digitale

Il **comma 2 dell'articolo 17** dello schema di decreto legislativo identifica l'oggetto materiale dell'ordine di esibizione probatoria, delineando attraverso un'**elencazione meramente esemplificativa** le tipologie documentali di maggiore ricorrenza e rilievo nelle controversie civili aventi ad oggetto sistemi algoritmici. Nello specifico, la disposizione opera un rinvio alle evidenze documentali prescritte dal **Regolamento (UE) 2024/1689 (AI Act)**, includendovi espressamente i **registri di registrazione automatica degli eventi (*logging*)** di cui all'articolo 12, la documentazione relativa al **sistema di gestione dei rischi** prevista dall'articolo 9, le informazioni pertinenti racchiuse nella **documentazione tecnica** ex articolo 11 e i dati riguardanti i parametri e le modalità di **sorveglianza umana** stabiliti dall'articolo 14 del medesimo regolamento unionale.

Secondo quanto precisato dalla **Relazione illustrativa**, la tecnica normativa di ancorare l'accesso alle prove alla documentazione obbligatoria prevista dal legislatore europeo persegue una duplice finalità di sistema. In via principale, la norma intende assicurare al danneggiato la **concreta accessibilità** a documenti che il fornitore o il *deployer* sono già tenuti per legge a predisporre, mitigando così le difficoltà di individuazione del materiale probatorio in un contesto di elevata complessità tecnica. In via sussidiaria, l'intervento mira a valorizzare la

funzione probatoria degli obblighi di compliance, trasformando i presidi regolatori di trasparenza e tracciabilità in strumenti operativi funzionali all'accertamento della responsabilità civile e alla ricostruzione del percorso decisionale del sistema. Sotto il profilo della tecnica processuale, il richiamo a tali categorie documentali tipizzate agevola il giudice nella valutazione della **pertinenza degli elementi di prova** di cui viene chiesta l'esibizione, fornendo un parametro di riferimento certo rispetto agli obblighi di conservazione gravanti sugli operatori economici. In definitiva, la disposizione funge da raccordo necessario tra il piano regolatorio della sicurezza dei prodotti e il piano processuale del risarcimento del danno, garantendo che l'**opacità tecnologica** non si traduca in un'impossibilità di tutela giurisdizionale per il soggetto leso.

L'**articolo 9 del Regolamento (UE) 2024/1689** impone l'istituzione e il mantenimento di un **sistema di gestione dei rischi** configurato come un processo iterativo e continuo che deve accompagnare il sistema di IA ad alto rischio per l'intero ciclo di vita. Tale sistema è finalizzato all'identificazione e all'analisi dei pericoli noti o ragionevolmente prevedibili per la salute, la sicurezza e i diritti fondamentali, includendo la valutazione delle criticità derivanti sia dall'uso conforme alla finalità prevista sia dalle condizioni di uso improprio prevedibile. Il processo impone l'adozione di misure di attenuazione mirate affinché ogni rischio residuo associato ai pericoli individuati sia considerato accettabile, tenendo conto delle conoscenze tecniche e della formazione attesa dal deployer. Parallelamente, l'**articolo 11** stabilisce l'obbligo di predisporre una **documentazione tecnica** dettagliata prima dell'immissione sul mercato o della messa in servizio, la quale deve essere tenuta costantemente aggiornata per dimostrare la conformità ai requisiti di sicurezza. Tale apparato documentale deve fornire alle autorità nazionali e agli organismi notificati informazioni chiare sulla logica degli algoritmi, sulle specifiche di progettazione, sull'architettura del software, sulle risorse computazionali utilizzate e sulle procedure di addestramento e convalida dei dati. Ai fini della trasparenza e della tracciabilità, l'**articolo 12** prescrive che i sistemi di IA ad alto rischio consentano tecnicamente la **registrazione automatica degli eventi (logging)** per tutta la durata del loro ciclo di vita. Tale registrazione deve permettere al deployer e al fornitore di individuare situazioni che possano determinare modifiche sostanziali o presentare rischi per la sicurezza, agevolando il monitoraggio delle prestazioni in contesti reali e documentando dati critici quali il periodo di ciascun utilizzo, le banche dati di riferimento consultate e l'identificativo delle persone fisiche coinvolte nella verifica dei risultati. Infine, l'**articolo 14** disciplina la **sorveglianza umana**, stabilendo che i sistemi siano progettati con interfacce uomo-macchina adeguate che permettano a persone fisiche competenti di supervisionarne efficacemente il funzionamento. La sorveglianza umana ha lo scopo di prevenire o minimizzare i rischi residui per i diritti fondamentali, garantendo che l'operatore possa interpretare correttamente gli output, monitorare anomalie o disfunzioni e, laddove necessario, intervenire per arrestare il sistema o ribaltare le decisioni algoritmiche, giungendo a imporre una verifica separata da parte di almeno due persone fisiche per le applicazioni tecnologicamente più invasive

Il **comma 3** definisce i **criteri direttivi e i limiti intrinseci** del potere istruttorio del giudice in materia di accesso probatorio, introducendo un necessario correttivo alla portata dell'ordine di esibizione. La disposizione codifica espressamente i principi di **necessità e proporzionalità**, stabilendo che l'ordine di esibizione debba essere rigorosamente circoscritto a quanto indispensabile rispetto all'oggetto materiale della domanda risarcitoria allegata dall'istante.

Tale previsione, come evidenziato dalla **Relazione Illustrativa**, configura un obbligo in capo all'autorità giudiziaria di operare un preventivo e accurato **bilanciamento tra l'esigenza di effettività della tutela giurisdizionale e i contrapposti interessi dei soggetti coinvolti nel processo**, siano essi parti o terzi detentori delle evidenze tecniche.

Un rilievo centrale all'interno della norma è attribuito alla clausola di salvaguardia relativa alla **tutela dei segreti commerciali e delle informazioni riservate**, la quale impone al giudice di tenere in debita considerazione il rischio di pregiudizio che una divulgazione indiscriminata potrebbe arrecare al patrimonio informativo e tecnologico del fornitore o del *deployer*.

Come precisato dalla **Relazione Tecnica**, questa limitazione è funzionale a garantire che lo strumento della *disclosure* non travalichi la propria finalità compensativa dell'asimmetria informativa per trasformarsi in un mezzo di acquisizione di *asset* strategici aziendali o in un'indebita intrusione nei processi di sviluppo protetti dalla proprietà industriale. In definitiva, il comma 3 assicura che la ricerca della prova sul funzionamento del sistema algoritmico avvenga secondo un modulo di **massima cautela procedurale**, rendendo il meccanismo di esibizione compatibile con il mantenimento della competitività e della riservatezza operativa degli operatori economici.

Il **comma 4** disciplina specificamente la gestione del rischio di **divulgazione di segreti commerciali** o di altre informazioni riservate nel corso dell'esecuzione dell'ordine di esibizione probatoria. Sotto il profilo tecnico-giuridico, la norma impone al giudice l'obbligo di adottare misure idonee a garantire la tutela del patrimonio informativo e tecnologico del fornitore o del *deployer* laddove l'accesso agli elementi di prova possa pregiudicare interessi di proprietà industriale.

Come precisato dalla **Relazione illustrativa**, il legislatore ha scelto di operare un rinvio recettizio all'**articolo 121-ter del Codice della Proprietà Industriale** (d.lgs. n. 30/2005), mutuando integralmente uno strumentario procedurale già sperimentato che consente, tra l'altro, l'oscuramento di parti di documenti o la limitazione dell'accesso alle udienze. Tale previsione è volta a bilanciare

l'effettività della tutela giurisdizionale del danneggiato con la necessità di preservare gli *asset* strategici aziendali, evitando che il meccanismo di *disclosure* si trasformi in uno strumento di acquisizione indebita di segreti industriali.

Il **comma 5** regola le conseguenze processuali del **mancato adeguamento all'ordine di esibizione**. In caso di inadempimento ingiustificato, la norma attribuisce al giudice il potere di desumere **argomenti di prova** ai sensi dell'articolo 116 del codice di procedura civile. Qualora l'inadempimento riguardi specificamente la documentazione tipizzata dal secondo comma (come i registri di *logging* o il sistema di gestione dei rischi), il legislatore introduce una sanzione istruttoria ancora più severa, stabilendo che il giudice possa ritenere come **ammessi i fatti allegati dall'istante**, previa valutazione di ogni altro elemento di prova disponibile.

Questa disposizione, come sottolineato dalla **Relazione Tecnica**, mira a dare effettività all'obbligo di trasparenza, trasformando il rifiuto di collaborazione tecnica in un fattore determinante per l'accertamento della responsabilità civile

Il **comma 6** infine introduce una misura di coercizione indiretta volta a garantire l'effettività dell'accesso probatorio. La disposizione stabilisce infatti una **sanzione pecuniaria di entità compresa tra 1.500 e 10.000 euro** a carico del **terzo inadempiente** che ometta ingiustificatamente di ottemperare all'ordine di esibizione degli elementi di prova relativi al funzionamento del sistema di intelligenza artificiale.

La *ratio* di tale previsione risiede nella necessità di dotare il giudice di uno strumento sanzionatorio efficace per superare l'**asimmetria informativa** e l'**opacità tecnologica**, assicurando che i detentori delle evidenze tecniche non possano frustrare le pretese risarcitorie del danneggiato attraverso condotte meramente omissive.

L'**articolo 116 del codice di procedura civile**, rubricato "Valutazione delle prove", disciplina il potere discrezionale del giudice nella ricostruzione dei fatti di causa, delineando il passaggio dal sistema delle prove legali a quello del libero convincimento. Al primo comma, la norma sancisce il principio fondamentale secondo cui il giudice deve valutare le prove secondo il suo **prudente apprezzamento**, configurando tale modulo valutativo come la regola generale del processo civile. Questo parametro, che la dottrina definisce di "prova libera", impone al magistrato l'uso della ragione e delle massime d'esperienza per determinare l'attendibilità e l'efficacia dei singoli mezzi istruttori, con l'unico limite della doverosa motivazione sull'iter logico seguito. Il precetto prevede tuttavia una riserva di legge ("salvo che la legge disponga altrimenti"), preservando le ipotesi eccezionali di **prova legale**, nelle quali l'efficacia probatoria è predeterminata dal legislatore in modo vincolante, come nel caso

dell'atto pubblico, della confessione o del giuramento decisorio, sottraendo così tali elementi alla libera valutazione del decidente. Il secondo comma dell'articolo attribuisce al giudice il potere sussidiario di desumere **argomenti di prova** dal contegno processuale delle parti, offrendo uno strumento pratico per l'integrazione del convincimento. Tali elementi conoscitivi possono essere tratti specificamente dalle risposte fornite dalle parti in sede di interrogatorio libero ex articolo 117 c.p.c., dal rifiuto ingiustificato di consentire le ispezioni ordinate dal giudice e, in termini generali, dalla condotta complessiva tenuta dai contendenti nel corso del giudizio.

Articolo 18 (Presunzione del nesso di causalità)

L'**articolo 18** introduce una **presunzione relativa del nesso di causalità** tra la violazione degli obblighi previsti dal regolamento (UE) 2024/1689 (AI Act) e il danno lamentato dal soggetto leso.

L'**articolo 18** disciplina la **presunzione del nesso di causalità**, ponendosi come il pilastro fondamentale dell'intervento sulla ripartizione dell'onere probatorio nelle azioni di risarcimento. E' in particolare introdotta una **presunzione iuris tantum**, per la quale il collegamento eziologico tra la violazione di un obbligo previsto dal Regolamento (UE) 2024/1689 (AI Act) e il danno si considera sussistente, fatta salva la facoltà per il convenuto di fornire la **prova contraria**.

Come evidenziato dalla **Relazione illustrativa**, l'operatività di tale presunzione è circoscritta ai casi in cui il danno derivi dall'inosservanza di uno o più obblighi regolatori puntuali, configurando un regime più restrittivo rispetto a quello previsto per l'accesso probatorio di cui all'articolo 19. L'alleviamento dell'onere probatorio a favore del danneggiato riguarda **esclusivamente il nesso causale**: non si verifica, pertanto, alcuna inversione automatica per quanto concerne la **colpa** o l'effettiva **violazione dell'obbligo**, elementi che restano integralmente oggetto di prova a carico dell'attore. La *ratio* della norma è quella di facilitare il ristoro del pregiudizio subito a fronte della complessità tecnica dei sistemi algoritmici, evitando che l'opacità del *software* renda impossibile la ricostruzione del percorso causale.

La *ratio legis* dell'intervento risiede nella necessità di superare l'**opacità tecnologica** (effetto "*scatola nera*") e la marcata **asimmetria informativa** che caratterizzano i sistemi algoritmici, rendendo altrimenti "*diabolica*" la prova della dinamica interna al *software* per il soggetto leso. La giurisprudenza ha evidenziato come la complessità dei sistemi di **auto-apprendimento (machine learning)** possa rendere quasi impossibile ricostruire i passaggi intermedi tra l'input e l'output dannoso. In particolare il tema della causalità e della responsabilità professionale è già emerso in casi di "uso improvvido" dell'IA generativa, dove l'impiego acritico di algoritmi ha prodotto "**allucinazioni**" (come citazioni giurisprudenziali inesistenti), portando i giudici a ravvisare una responsabilità aggravata ex art. 96 c.p.c. per **colpa grave** o malafede (Trib. Torino, n. 2120/2025; Trib. Latina, 23 settembre 2025; Trib. Siracusa, 20 febbraio 2026). Anche la **Corte di Cassazione** ha recentemente sottolineato il rischio che il ricorso a strumenti di IA possa indurre il decisore ad abdicare al proprio momento valutativo, compromettendo la terzietà del giudizio (Cass. pen., n. 34481/2025).

Articolo 19

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

L'articolo 19 dello schema di decreto legislativo disciplina la **rilevanza della conformità** dei sistemi di intelligenza artificiale rispetto alle prescrizioni del Regolamento (UE) 2024/1689 (AI Act) nell'ambito dei giudizi di responsabilità civile.

La disposizione stabilisce il principio fondamentale secondo cui l'osservanza degli obblighi previsti dalla normativa unionale e l'eventuale possesso di una **certificazione di conformità** rilasciata ai sensi del medesimo regolamento non costituiscono, di per sé, una causa di esclusione della responsabilità del fornitore o del *deployer*. La norma opera una netta **distinzione tra il piano della compliance regolatoria preventiva e il piano del risarcimento del danno**, garantendo che i presidi di sicurezza amministrativa non si trasformino in un meccanismo di immunità sostanziale in sede giudiziaria.

Come precisato dalla **Relazione Illustrativa**, la *ratio* dell'intervento risiede nella necessità di puntualizzare che la valutazione della conformità effettuata dagli organismi notificati o dagli operatori non pregiudica l'accertamento della colpa o del nesso causale in sede aquiliana o contrattuale. La norma assicura che il giudice possa operare un sindacato pieno sulla condotta del convenuto, fermo restando che l'avvenuto adempimento degli standard di sicurezza europei mantiene un intrinseco **valore probatorio** ai fini della valutazione complessiva del comportamento diligente tenuto dall'operatore economico. Sotto il profilo dell'ambito di applicazione, l'efficacia di tale disposizione è coordinata con il **comma 2 dell'articolo 16**, il quale circoscrive l'operatività di tale criterio alle sole azioni in cui il danno sia derivato dalla violazione di obblighi puntuali previsti dall'AI Act.

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

L'articolo 20 introduce l'azione diretta del danneggiato verso l'assicuratore per i danni da IA. Disciplina la comunicazione preventiva dei dati della polizza e uniforma i termini di prescrizione per garantire simmetria ed effettività alle tutele risarcitorie.

L'**articolo 20** introduce nell'ordinamento l'**azione diretta del danneggiato** nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile per i danni derivanti dall'utilizzo di sistemi di intelligenza artificiale.

Come si precisa nella **relazione illustrativa** la norma modella tale strumento di tutela sull'archetipo già consolidato per la responsabilità civile da circolazione di veicoli a motore, richiamando i principi dell'articolo 144 del codice delle assicurazioni private.

Al **comma 1**, la disposizione attribuisce al soggetto leso la facoltà di richiedere preventivamente alla parte individuata come responsabile, prima dell'instaurazione del giudizio, se la stessa sia assistita da una polizza assicurativa per il danno dedotto. Tale istanza non configura una condizione di procedibilità della domanda risarcitoria e non interferisce con le procedure di mediazione obbligatoria o facoltativa. Il destinatario della richiesta ha l'obbligo di comunicare entro trenta giorni l'esistenza del contratto, la denominazione dell'impresa e gli estremi della polizza, venendo altrimenti sanzionato sul piano processuale con il potere del giudice di desumere **argomenti di prova** dal silenzio o dall'incompletezza della risposta ai sensi dell'**articolo 116 del codice di procedura civile**.

È appena il caso di ricordare che l'articolo 116 c.p.c. sancisce al primo comma il principio del **libero convincimento**, imponendo al giudice di valutare le risultanze istruttorie secondo il suo **prudente apprezzamento**, salvo i casi eccezionali di prova legale in cui l'efficacia probatoria è predeterminata in modo vincolante dal legislatore. Questo modulo valutativo richiede al magistrato l'uso della ragione, della logica e delle massime d'esperienza per ricostruire i fatti storici, con l'obbligo di fornire un'argomentazione giustificativa esauriente nella motivazione della sentenza.

Il secondo comma dell'articolo 116 attribuisce al giudice il potere di desumere **argomenti di prova** dalle risposte fornite dalle parti nell'interrogatorio libero, dal loro rifiuto ingiustificato di consentire ispezioni e, in termini generali, dal loro complessivo contegno nel processo.

Il **comma 2** fonda il diritto sostanziale del danneggiato ad agire direttamente contro l'assicuratore per ottenere l'integrale ristoro del pregiudizio subito, sebbene nei limiti delle somme e dei massimali pattuiti nel contratto di assicurazione.

I profili operativi di tale azione sono dettagliati nei commi successivi, i quali stabiliscono al **comma 3** l'opponibilità al danneggiato delle eccezioni derivanti dal contratto assicurativo, a condizione che siano anteriori al sinistro, e al **comma 4** il **diritto di rivalsa** dell'impresa verso l'assicurato qualora sussistano titoli contrattuali per rifiutare o ridurre la prestazione.

Una garanzia procedurale fondamentale è sancita dal **comma 5**, che impone il **litisconsorzio necessario** del soggetto responsabile nel giudizio promosso contro l'assicuratore, assicurando l'unitarietà dell'accertamento sul fatto generatore del danno e prevenendo il rischio di giudicati contraddittori tra l'azione diretta e quella di regresso.

Infine, il **comma 6** opera una piena **simmetria temporale** delle tutele, uniformando il termine di **prescrizione** dell'azione diretta a quello previsto per l'azione nei confronti del responsabile primario, in coerenza con la natura accessoria della garanzia assicurativa.

TITOLO III - DISPOSIZIONI FINALI

CAPO I – DISPOSIZIONI TRANSITORIE E FINANZIARIE

Articolo 21

(Disposizioni transitorie sull'utilizzo dei sistemi di intelligenza)

L'**articolo 21** reca le **disposizioni transitorie** volte a consentire il passaggio al nuovo quadro normativo per i sistemi di IA che, alla data di entrata in vigore del presente provvedimento, siano già oggetto di rapporti contrattuali o in fase di sviluppo o utilizzati per finalità di polizia.

Il **comma 1** stabilisce che **devono essere conformati alle disposizioni del capo II del titolo I** (articoli da 3 a 6) - in materia di ricerca, sviluppo, addestramento, formazione, sperimentazione e utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia - i **sistemi di intelligenza artificiale** che, alla data di entrata in vigore del presente provvedimento, risultano:

- **oggetto di rapporti contrattuali;**
- **in fase di sviluppo o di sperimentazione per finalità di polizia;**
- **già in uso nell'attività di polizia.**

La norma specifica che a ciò deve provvedere, **entro un anno** dalla data di entrata in vigore del provvedimento in esame, **ciascuna Forza di polizia** per quanto di rispettiva competenza.

Il **comma 2** prescrive l'**osservanza dei termini di entrata in vigore e di compiuta attuazione del regolamento (UE) 2024/1689** con riferimento alle **disposizioni del titolo I** – concernenti l'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia - la cui applicazione sia prevista direttamente ovvero dipenda dal regolamento medesimo.

Sul punto la relazione illustrativa precisa che l'osservanza del regolamento IA rileva, oltre che per i termini di entrata in vigore ([articolo 113](#)), anche con riferimento alla relativa disciplina transitoria ([articolo 111](#)).

In particolare, l'articolo 111 del regolamento reca il regime transitorio applicabile ai sistemi di IA e ai modelli di IA per finalità generali già immessi sul mercato o messi in servizio rispetto alle scadenze applicative dell'articolo 113. Il paragrafo 1 riguarda i sistemi di IA componenti dei sistemi IT su larga scala

istituiti dagli atti elencati nell'[allegato X](#) (Sistema d'informazione Schengen, Sistema d'informazione visti, Eurodac, Sistema di ingressi/uscite, Sistema europeo di informazione e autorizzazione ai viaggi, Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi, interoperabilità): se immessi sul mercato o messi in servizio prima del 2 agosto 2027, la conformità alle disposizioni del regolamento IA è richiesta entro il 31 dicembre 2030, fermo restando che i requisiti del regolamento sono comunque considerati nelle valutazioni periodiche previste dai singoli atti istitutivi. Il paragrafo 2 riguarda gli altri sistemi ad alto rischio: se immessi sul mercato o messi in servizio prima del 2 agosto 2026, il regolamento si applica ai relativi operatori solo in caso di modifiche significative della progettazione successive a tale data, salvo che per i sistemi destinati a essere utilizzati da autorità pubbliche, per i quali l'adeguamento è comunque dovuto entro il 2 agosto 2030. Il paragrafo 3 concede ai fornitori di modelli per finalità generali immessi sul mercato prima del 2 agosto 2025 un termine di adeguamento fino al 2 agosto 2027. Nelle fattispecie di cui ai paragrafi 1 e 2 resta fermo, in ogni caso, senza alcuna proroga transitoria, il divieto delle pratiche di IA di cui all'articolo 5 del regolamento, applicabile dal 2 febbraio 2025, ai sensi dell'articolo 113, paragrafo 3, lettera a).

L'articolo 113 del regolamento prevede l'entrata in vigore e l'applicazione dello stesso. La sua applicazione, in via generale, è prevista a decorrere dal 2 agosto 2026, fatto salvo per alcune specifiche disposizioni, le quali si applicano a decorrere dal:

- 2 febbraio 2025: capo I, disposizioni generali (articoli 1-4), e capo II, pratiche di IA vietate (articolo 5);
- 2 agosto 2025: capo III, sezione 4, autorità di notifica e organismi notificati (articoli 28-39); capo V, modelli di IA per finalità generali (articoli 51-56); capo VII, *governance* (articoli 64-70); capo XII, sanzioni (articoli 99-101, con esclusione dell'articolo 101); articolo 78, riservatezza;
- 2 agosto 2027: articolo 6, paragrafo 1 (classificazione ad alto rischio dei sistemi di IA) e obblighi corrispondenti.

La stessa relazione illustrativa, nel delineare la finalità della norma transitoria in esame, evidenzia, inoltre, che essa è volta ad assicurare sia la continuità operativa delle Forze di polizia sia l'adeguamento graduale dei sistemi di IA già operanti alle nuove prescrizioni derivanti dal regolamento IA, dalla legge n. 132 del 2025 sull'intelligenza artificiale e dal presente provvedimento.

Articolo 22 ***(Clausola d'invarianza finanziaria)***

L'articolo 22 reca la **clausola d'invarianza finanziaria** riferita al complesso delle disposizioni dello schema di decreto in esame.

L'**articolo 22** dispone, in conformità a quanto disposto dall'articolo 24, comma 6, della legge n. 132 del 2025, che le amministrazioni interessate provvedono agli adempimenti di loro competenza nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

A tale proposito, il citato comma 6 stabilisce che, ad eccezione della previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di intelligenza artificiale (per cui sono stanziati 100 milioni di euro a valere sulle risorse del programma nazionale "PN scuola 2021-2027"), dall'attuazione delle deleghe di cui all'articolo 24 non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni competenti provvedono ai relativi adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

