DECRETO LEGISLATIVO 9 settembre 2026, n. 160

Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attivita' di polizia e di responsabilita' civile e penale. (26G00179)

(GU n.214 del 15-9-2026)

Vigente al: 30-9-2026

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

Capo I
Disposizioni generali

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87, quinto comma, della Costituzione;

Vista la legge 23 agosto 1988, n. 400 recante «Disciplina dell'attivita' di Governo e ordinamento della Presidenza del Consiglio dei Ministri» e, in particolare, l'articolo 14;

Vista la legge 24 dicembre 2012, n. 234, recante «Norme generali sulla partecipazione dell'Italia all'attuazione della normativa e delle politiche dell'Unione europea»;

Vista la legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» e, in particolare, l'articolo 24, commi 1, 2, lettera h), 3 e 5;

Visto il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale);

Visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE concernente regolamento generale sulla protezione dei dati;

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle

autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati;

Vista la direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilita' per danno da prodotti difettosi e che abroga la direttiva 85/374/CEE del Consiglio;

Visto il regio decreto 19 ottobre 1930, n. 1398, recante «Approvazione del testo definitivo del codice penale»;

Visto il regio decreto 28 ottobre 1940, n. 1443, recante «Codice di procedura civile» e, in particolare, l'articolo 116;

Visto il regio decreto 16 marzo 1942, n. 262, recante «Approvazione del testo del Codice civile», e, in particolare, gli articoli 2050 e 2051;

Vista la legge 23 aprile 1959, n. 189, recante «Ordinamento del Corpo della guardia di finanza»;

Vista la legge 1° aprile 1981, n. 121, recante «Nuovo ordinamento dell'Amministrazione della pubblica sicurezza»;

Visto il decreto del Presidente della Repubblica 22 settembre 1988, n. 447, recante «Approvazione del codice di procedura penale»;

Visto il decreto legislativo 28 luglio 1989, n. 271, recante «Norme di attuazione, di coordinamento e transitorie del codice di procedura penale»;

Visto il decreto legislativo 19 marzo 2001, n. 68, recante «Adeguamento dei compiti del Corpo della Guardia di finanza, a norma dell'articolo 4 della legge 31 marzo 2000, n. 78»;

Visto il decreto legislativo 8 giugno 2001, n. 231, recante «Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300»;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;

Visto il decreto legislativo 15 marzo 2010, n. 66, recante «Codice dell'ordinamento militare» e, in particolare, il Libro primo, Titolo IV, Capo V, in materia di compiti e attribuzioni dell'Arma dei carabinieri;

Visto il decreto legislativo 19 agosto 2016, n. 177, recante «Disposizioni in materia di razionalizzazione delle funzioni di polizia e assorbimento del Corpo forestale dello Stato, ai sensi dell'articolo 8, comma 1, lettera a), della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche»;

Visto il decreto legislativo 18 maggio 2018, n. 51, recante «Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio»;

Visto il decreto del Presidente della Repubblica 29 gennaio 1999, n. 34, concernente «Regolamento recante norme per la determinazione della struttura ordinativa del Corpo della Guardia di finanza, ai sensi dell'articolo 27, commi 3 e 4, della legge 27 dicembre 1997, n. 449»;

Visto il decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, concernente «Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalita' di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalita' di polizia, da organi, uffici e comandi di polizia»;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 10 giugno 2026;

Acquisito il parere del Garante per la protezione dei dati personali;

Acquisito il parere della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, espresso nella seduta del 20 luglio 2026;

Acquisiti i pareri delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 4 agosto 2026;

Sulla proposta del Presidente del Consiglio dei ministri e dei Ministri per gli affari europei, il PNRR e le politiche di coesione, dell'interno e della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, della difesa e dell'economia e delle finanze;

Emana
il seguente decreto legislativo:

Art. 1

Oggetto e finalita'

1. Il presente titolo reca disposizioni in materia di utilizzo di sistemi di intelligenza artificiale da parte degli organi, uffici e comandi delle Forze di Polizia, in relazione alle specifiche funzioni esercitate, coerentemente con le norme e i principi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, e della legge 23 settembre 2025, n. 132.

2. Le disposizioni del presente titolo si applicano nel rispetto dei diritti fondamentali e delle liberta' garantite dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle liberta' fondamentali, nonche' dei principi di proporzionalita', di non discriminazione, di sorveglianza umana e di trasparenza di cui all'articolo 3 della legge n. 132 del 2025.

3. Il presente titolo non comporta nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi e i modelli di intelligenza artificiale utilizzati nelle attivita' e per le finalita' di polizia.

Art. 2

Definizioni

1. Ai fini del presente titolo, si intende per:

a) «regolamento IA»: il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale);

b) «legge IA»: la legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»;

c) «sistema di IA»: un sistema di intelligenza artificiale definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689;

d) «pratiche vietate»: le pratiche di IA vietate a norma dell'articolo 5 del regolamento (UE) 2024/1689;

e) «sistema di IA ad alto rischio»: un sistema di IA classificato ad alto rischio, conformemente all'articolo 6 del regolamento (UE) 2024/1689 in combinato disposto con il suo allegato III;

f) «categorie particolari di dati personali»: le categorie di dati di cui all'articolo 3, punto 37), del regolamento (UE) 2024/1689;

g) «dati relativi a condanne penali e reati»: i dati personali di cui all'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

h) «dati operativi sensibili»: i dati relativi ad attivita' di prevenzione, accertamento, indagine o perseguimento di reati, indicati dall'articolo 3, punto 38), del regolamento (UE) 2024/1689;

i) «output»: previsioni, contenuti, raccomandazioni o decisioni generate da un sistema di IA ai sensi dell'articolo 3, punto 1), del regolamento (UE) 2024/1689;

l) «scraping non mirato»: l'estrazione e la 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;

m) «Autorita' nazionali per l'intelligenza artificiale»: l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN), ai sensi dell'articolo 20, comma 1, della legge 23 settembre 2025, n. 132;

n) «Garante»: il Garante per la protezione dei dati personali, istituito dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196;

o) «Forze di polizia»: le Forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121;

p) «attivita' di polizia»: le attivita' di contrasto definite dall'articolo 3, punto 46), del regolamento (UE) 1689/2024, svolte, nell'esercizio delle rispettive attribuzioni e funzioni, dagli organi, uffici e comandi delle Forze di polizia;

q) «finalita' di polizia»: i 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, richiamati nei punti 45) e 46) dell'articolo 3 del regolamento (UE) 1689/2024, e per i quali sono svolte le attivita' di polizia di cui alla lettera s);

2. Per quanto non espressamente previsto dal presente decreto, si

applicano le definizioni di cui all'articolo 2 della legge 23 settembre 2025, n. 132, e all'articolo 3 del regolamento (UE) 2024/1689.

Capo II
Disposizioni in materia di ricerca, sviluppo, addestramento, formazione, sperimentazione e utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia

Art. 3

Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attivita' di polizia

1. La ricerca, la sperimentazione, lo sviluppo, l'addestramento, l'adozione, l'applicazione, la convalida e l'utilizzo di sistemi e modelli di intelligenza artificiale per le attivita' e le finalita' delle Forze di polizia avvengono nel rispetto dei diritti fondamentali e delle liberta' previste dalla Costituzione, del diritto dell'Unione europea e dei principi di cui all'articolo 3 della legge IA, secondo un approccio antropocentrico, proporzionato e fondato sul rischio, che tenga conto della classificazione dei sistemi di IA e delle diverse categorie di interessati.

2. Le attivita' di ricerca, sperimentazione, sviluppo e addestramento sono orientate al perseguimento della funzionalita' e dell'affidabilita' operativa dei sistemi e dei modelli di IA destinati a essere utilizzati dalle Forze di polizia, nella prospettiva di migliorare l'apporto tecnologico dell'intelligenza artificiale alle valutazioni e alle decisioni umane nella relativa attivita'.

3. Le Forze di polizia, in conformita' con l'assetto istituzionale vigente e nell'ambito delle proprie competenze, utilizzano i sistemi e i modelli di intelligenza artificiale e i relativi output in funzione strumentale e di supporto alle relative attivita' di polizia, allo scopo di incrementarne l'efficacia e l'efficienza.

4. L'utilizzo dei sistemi e dei modelli di IA nell'attivita' di polizia, conformemente agli obblighi stabiliti dal regolamento IA e fermo restando quanto previsto dal comma 5 in ordine alla sorveglianza umana sui sistemi di IA ad alto rischio, deve 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 e' effettuata da personale individuato dalle procedure interne di ciascuna Forza di polizia ed e' documentata in modo da assicurarne la tracciabilita'.

5. Le Forze di Polizia assicurano che per i sistemi di IA ad alto rischio la sorveglianza umana sia effettiva e conforme a quanto previsto dall'articolo 14 del regolamento IA e che il personale preposto possieda le necessarie competenze e formazione al fine di prevenire e ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali.

6. Il trattamento di dati personali nelle attivita' di cui al comma 1, incluse le categorie particolari di dati personali, i dati operativi sensibili e i dati relativi a condanne penali e reati nella disponibilita' delle Forze di polizia in forza di norme di legge o regolamentari ovvero di atti amministrativi generali, e' svolto nel rispetto della normativa in materia di protezione dei dati personali, di cui al decreto legislativo 18 maggio 2018, n. 51, ferme restando le specifiche disposizioni dettate dal regolamento IA per i sistemi ad alto rischio e quelle contenute nel capo III del presente titolo.

7. Le attivita' di cui al presente articolo sono effettuate senza nuovi od ulteriori obblighi rispetto a quanto disposto dal regolamento IA, ferme restando le esclusioni previste dallo stesso regolamento.

Art. 4

Collaborazione nell'ambito della ricerca e sperimentazione scientifica finalizzata alla realizzazione di sistemi e modelli di intelligenza artificiale per l'attivita' di polizia

1. Le Forze di polizia, nell'ambito di specifici progetti di ricerca e sperimentazione scientifica volti alla realizzazione di sistemi di intelligenza artificiale o di dispositivi che utilizzano tecnologie di intelligenza artificiale per l'attivita' di polizia, possono attivare collaborazioni con universita', enti di ricerca e soggetti pubblici e privati, anche per il tramite di societa' in house o di societa' a totale partecipazione pubblica controllate dallo Stato, nel rispetto della disciplina dell'Unione europea in materia di concorrenza e di aiuti di Stato.

2. Il trattamento di dati per le finalita' di cui al comma 1 e' svolto nel rispetto della normativa in materia di protezione dei dati

personali, con la previsione di apposite clausole che escludano, in particolare, la condivisione di dati operativi sensibili e l'acquisizione o l'utilizzazione, anche indirette, da parte dei soggetti con i quali sono attivate le 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'attivita' di polizia, fatto salvo il ricorso a dati sintetici ovvero a dati reali sottoposti a tecniche di mascheramento o di pseudonimizzazione.

3. I rapporti di collaborazione di cui al comma 1 disciplinano espressamente la titolarita' dei diritti di proprieta' intellettuale, industriale e di sfruttamento economico dei risultati della ricerca, dei modelli derivati, dei dati di addestramento e del software, nel rispetto del codice della proprieta' industriale di cui al decreto legislativo 10 febbraio 2005, n. 30, dell'articolo 64 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e della normativa di settore applicabile. I medesimi rapporti individuano altresi', nel rispetto del decreto legislativo n. 51 del 2018, i ruoli svolti dai soggetti coinvolti nel trattamento dei dati personali, specificando quando gli stessi operano quali titolari, contitolari o responsabili del trattamento e disciplinando i relativi obblighi e responsabilita', anche con riferimento alle misure di sicurezza e alla documentazione delle operazioni di trattamento. E' in ogni caso assicurata la titolarita' in capo alle Forze di polizia dei modelli addestrati su dati operativi sensibili.

Art. 5

Sviluppo, realizzazione e prova di determinati sistemi di IA per finalita' di polizia negli spazi di sperimentazione normativa

1. Il presente articolo costituisce base giuridica ai sensi dell'articolo 59, paragrafo 2, del regolamento IA, nonche' del decreto legislativo 18 maggio 2018, n. 51, per il trattamento di dati personali, inclusi i dati relativi a reati e le categorie particolari di dati di cui all'articolo 3, punto 37), dello stesso regolamento IA, effettuato dalle Forze di polizia nell'ambito di spazi di sperimentazione normativa per l'intelligenza artificiale, quando tale trattamento e' necessario per finalita' di polizia.

2. La partecipazione delle Forze di polizia agli spazi di sperimentazione di cui al comma 1 e' finalizzata allo sviluppo, alla realizzazione e alla prova di sistemi di IA, in particolare ad alto

rischio, destinati alle attivita' di polizia, nel rispetto della protezione dei dati personali e della tutela dei diritti e delle liberta' fondamentali.

3. Negli spazi di cui al presente articolo, la sperimentazione avviene nel rispetto delle condizioni cumulativamente previste dall'articolo 59, paragrafo 1, del regolamento IA, prevede il coinvolgimento del Garante laddove la stessa comporti, per il suo funzionamento, il trattamento di dati personali, ed e' oggetto di collaborazione e raccordo con le Autorita' nazionali per l'intelligenza artificiale, fermo restando la tutela dei dati operativi sensibili e l'esclusiva titolarita' e responsabilita' del trattamento degli stessi da parte delle amministrazioni competenti.

4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta delle Autorita' nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'interno, sentiti il Ministro dell'economia e delle finanze e il Garante, sono definite le modalita' di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e le attivita' del presente articolo.

[omissis]

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

Art. 7

Etichettatura, filtraggio e categorizzazione di dati biometrici nell'attivita' di polizia

1. Nell'ambito delle attivita' di polizia, l'etichettatura, il filtraggio o la categorizzazione di set di dati biometrici acquisiti in conformita' alla normativa vigente, ai sensi dell'articolo 5, paragrafo 1, lettera g), del regolamento IA, sono consentiti a condizione che:

a) non siano finalizzati a inferire o dedurre le caratteristiche di cui all'articolo 5, paragrafo 1, lettera g), del regolamento IA;

b) siano funzionali ad attivita' di comparazione o ricerca ovvero ad ulteriori attivita', comunque effettuate conformemente alla

normativa vigente ed esclusivamente per finalita' di polizia;

c) non costituiscano l'unico fondamento di decisioni che producono effetti giuridici nei confronti di persone fisiche;

d) il titolare del trattamento adotti misure idonee a prevenire il reimpiego dei dati e dei risultati per finalita' incompatibili con quelle per cui sono stati raccolti.

2. Il trattamento di dati personali nelle attivita' di cui al comma 1 tiene conto, ai fini dell'adempimento dei connessi obblighi previsti dal regolamento IA, della classificazione dei sistemi di IA, avuto riguardo anche agli orientamenti della Commissione europea sull'attuazione pratica del regolamento IA, ai sensi degli articoli 6, paragrafo 5, e 96, dello stesso regolamento, ed e' svolto nel rispetto di quanto previsto dal decreto legislativo 18 maggio 2018, n. 51.

Art. 8

Sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale per finalita' di prevenzione, nonche' di ricerca delle persone scomparse e delle vittime di specifici reati

1. Fermo restando quanto previsto dall'articolo 359-ter del codice di procedura penale, introdotto dall'articolo 13 del presente decreto, l'utilizzo di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale in luoghi pubblici o aperti al pubblico da parte degli organi, uffici e comandi delle Forze di polizia e' ammesso per le finalita' di prevenzione di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto ii), del regolamento IA. I sistemi di cui al primo periodo possono essere utilizzati, altresi', per la ricerca di una persona scomparsa o di persone specifiche, vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale, ai sensi dell'articolo 5, paragrafo 1, primo comma, lettera h), punto i), del regolamento IA.

2. L'utilizzo dei sistemi di IA di cui al comma 1 e' consentito esclusivamente per confermare l'identita' delle persone di cui al medesimo comma 1 specificamente interessate ovvero per la ricerca mirata, anche in modo dinamico e compresa la localizzazione, di persone specificamente individuate o individuabili in relazione alla minaccia da prevenire o alla ricerca da eseguire.

3. Il confronto biometrico avviene esclusivamente con una banca dati di riferimento adeguata per ciascuna delle finalita' di cui al comma 1, contenente i dati biometrici e le relative informazioni

identificative, ove disponibili, riferiti alle persone, anche non identificate anagraficamente, di cui al comma 2. La banca dati di cui al primo periodo puo' essere derivata da dati contenuti in banche dati in uso alle Forze di polizia o tenute da altre pubbliche amministrazioni e accessibili alle predette Forze, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle attivita' di polizia. Il contenuto della banca dati di cui al primo periodo e' formato appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalita', che sono cancellati al termine della validita' dell'autorizzazione, in modo da garantire che il set di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse. E' in ogni caso vietato l'uso di banche dati biometriche alimentate, in tutto o in parte, mediante tecniche di scraping non mirato ovvero costituite in violazione delle disposizioni vigenti in materia di protezione dei dati personali.

4. L'utilizzo dei sistemi di IA di cui al comma 1 e' subordinato a una richiesta del questore o del comandante provinciale dell'Arma dei carabinieri e della Guardia di finanza, ovvero dei responsabili dei Servizi centrali di cui all'articolo 12 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, al procuratore della Repubblica presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione ovvero di ricerca, con indicazione della finalita' perseguita, della durata prevista, dell'area territoriale interessata, delle persone interessate e ricercate, delle banche dati di riferimento utilizzate e dei sistemi e delle tecnologie impiegati.

5. L'autorizzazione deve essere concessa con riguardo a uno specifico evento o per il tempo strettamente necessario, in ogni caso non superiore a quindici giorni, prorogabili dal procuratore della Repubblica, con decreto motivato per periodi successivi di quindici giorni qualora permangano le condizioni di cui al comma 1, nonche' con riferimento ad una area territoriale delimitata e alla indicazione delle persone specificamente interessate e ricercate. La medesima autorizzazione puo' essere concessa, altresi', soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento IA.

6. Nei casi d'urgenza, quando vi e' fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave e irreparabile per le finalita' di cui al comma 1, l'utilizzo del sistema di IA puo' essere avviato, su disposizione del questore, dei comandanti o dei

responsabili indicati al comma 4, dall'organo di polizia procedente, previa comunicazione, anche in forma orale, al procuratore della Repubblica, e a condizione che sia limitato a quanto strettamente necessario, in ogni caso con delimitazione dell'area interessata e indicazione delle persone ricercate.

7. Nei casi di cui al comma 6, la richiesta di autorizzazione e' trasmessa al procuratore della Repubblica senza ritardo e in ogni caso entro ventiquattro ore dall'inizio delle operazioni. Il procuratore della Repubblica, ove ritenga sussistenti le condizioni di cui al medesimo comma 6, provvede nelle successive ventiquattro ore.

8. Se non sono osservate le condizioni e i termini previsti dai commi 4, 5, 6 e 7, ovvero in caso di mancata autorizzazione, l'uso del sistema di intelligenza artificiale oggetto dell'autorizzazione e' immediatamente interrotto e tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, fatti salvi gli elementi acquisiti legittimamente sotto altra base giuridica conforme al decreto legislativo n. 51 del 2018. I risultati forniti dai sistemi di intelligenza artificiale in violazione delle disposizioni del presente articolo non possono essere utilizzati.

9. Si applicano le disposizioni di cui all'articolo 226, comma 5, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui all'allegato al decreto legislativo 28 luglio 1989, n. 271.

Art. 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

1. In conformita' all'articolo 5, paragrafo 2, del regolamento IA, per l'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale per le finalita' di cui all'articolo 8 del presente decreto o di cui all'articolo 359-ter del codice di procedura penale, introdotto dall'articolo 13 del presente decreto, il titolare del trattamento completa in via preventiva una valutazione di impatto sui diritti fondamentali secondo quanto previsto dall'articolo 27 dello stesso regolamento IA, ed effettua la valutazione d'impatto sulla protezione dei dati di cui agli articoli 23 e 24 del decreto legislativo n. 51 del 2018.

2. Ogni utilizzo di sistemi di intelligenza artificiale per

l'identificazione biometrica remota in tempo reale per le finalita' di cui al comma 1 e' registrato automaticamente in appositi file di log, non modificabili, comprendenti necessariamente i dati previsti dall'articolo 12, paragrafo 3, del regolamento IA. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili esclusivamente alle sole autorita' competenti per finalita' di verifica della liceita' del trattamento, di controllo interno e nell'ambito di un procedimento penale.

3. Restano fermi i termini di conservazione dei dati personali previsti, per finalita' di polizia, dall'articolo 10 del regolamento, di cui al decreto del Presidente della Repubblica 15 gennaio 2018, n. 15.

4. Dopo l'utilizzo dei sistemi di cui al comma 1, il titolare del trattamento effettua notifica al Garante, in conformita' a quanto previsto dall'articolo 5, paragrafo 4, del regolamento IA. La notifica, effettuata previo nulla osta dell'autorita' giudiziaria competente che puo' differirlo per un periodo non superiore a tre mesi, rinnovabile per una sola volta, in presenza di specifiche esigenze di segretezza, contiene le informazioni essenziali sull'autorizzazione rilasciata e sul risultato conseguito con l'utilizzo del sistema, e non include dati operativi sensibili. Nel caso di piu' attivazioni del sistema di IA per l'identificazione biometrica remota in tempo reale nello stesso contesto operativo ovvero di piu' utilizzi omogenei del predetto sistema, la notifica di cui al presente comma puo' essere effettuata in modo periodico e cumulativo, secondo i termini previsti dal decreto di cui al comma 5, ferma restando la necessita' del nulla osta preventivo dell'autorita' giudiziaria nei termini di cui al secondo periodo.

5. Con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, sentiti il Garante e le Autorita' nazionali per l'intelligenza artificiale, coerentemente con le norme del regolamento IA, sono individuati, in relazione all'uso dei sistemi di IA per l'identificazione biometrica remota in tempo reale per le finalita' di cui all'articolo 8 del presente decreto o di cui all'articolo 359-ter del codice di procedura penale, introdotto dall'articolo 13 del presente decreto:

a) i requisiti tecnici minimi di affidabilita' e accuratezza dei sistemi di IA per l'identificazione biometrica remota in tempo reale;

b) le modalita' di monitoraggio periodico delle prestazioni dei sistemi, con particolare riguardo alla rilevazione e alla mitigazione di eventuali bias o effetti discriminatori;

c) i requisiti tecnici minimi delle banche dati di riferimento

impiegate per il confronto biometrico, anche con riferimento alle relative misure di sicurezza, ai tempi e alle modalita' di cancellazione dei dati e alle garanzie di non incrementalita' del set di confronto per ogni singolo utilizzo autorizzato;

d) le misure tecniche e organizzative necessarie a garantire un adeguato livello di sicurezza del trattamento;

e) le misure tecniche e organizzative necessarie a impedire accessi illeciti ai dati;

f) le informazioni che il titolare del trattamento e' tenuto ad allegare alla richiesta di autorizzazione ai sensi dell'articolo 8 del presente decreto o dell'articolo 359-ter del codice di procedura penale, introdotto dall'articolo 13 del presente decreto, in ordine alle caratteristiche tecniche del sistema, ai risultati delle verifiche di accuratezza e ai meccanismi di gestione degli errori;

g) le modalita' di esecuzione della notifica di cui al comma 4;

h) gli ulteriori adempimenti cui il titolare del trattamento e' tenuto in conformita' a quanto previsto dal regolamento IA.

Art. 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

1. In tutti i casi in cui specifiche disposizioni di legge consentono l'installazione di sistemi di videosorveglianza, tali sistemi possono essere integrati con componenti di intelligenza artificiale, nel rispetto della normativa in materia di protezione dei dati personali e del regolamento IA. Le componenti di intelligenza artificiale, destinate al riconoscimento facciale, non possono essere attivate se non nei casi, alle condizioni e con le modalita' previste dai commi 2 e 3. L'attivazione e' effettuata successivamente all'acquisizione delle immagini, con un intervallo di tempo tale da non configurare un'identificazione biometrica remota in tempo reale ai sensi del regolamento IA.

2. Per procedere al riconoscimento facciale a posteriori, mediante i sistemi integrati di cui al comma 1 di una persona oggetto di ricerca mirata in quanto indiziata della commissione di un reato, il pubblico ministero, su istanza degli ufficiali di polizia giudiziaria che hanno avviato i predetti sistemi, chiede al giudice per le indagini preliminari l'autorizzazione all'utilizzo dei medesimi sistemi senza ritardo e comunque entro quarantotto ore dal loro

avvio. Il giudice, qualora ne ricorrano i presupposti, autorizza l'utilizzo con decreto motivato entro le successive quarantotto ore. Se non sono osservati i termini previsti dal primo periodo ovvero in caso di mancata autorizzazione, l'uso delle tecnologie di riconoscimento facciale collegato alla richiesta di autorizzazione e' immediatamente interrotto e tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato.

3. In conformita' all'articolo 26, paragrafo 10, primo comma, del regolamento IA, l'autorizzazione di cui al comma 2 non e' richiesta quando le tecnologie di riconoscimento facciale di cui al comma 1 sono utilizzate esclusivamente dopo la commissione di un reato al solo fine dell'identificazione iniziale di una persona potenzialmente indiziata della commissione del reato, sulla base di elementi oggettivi e verificabili direttamente connessi al fatto di reato. Nei casi di cui al primo periodo, l'utilizzo delle tecnologie e' effettuato sotto la diretta ed esclusiva responsabilita' dell'ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine e della sicurezza pubblica ovvero, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria di cui all'articolo 57, comma 1, lettere a) e b), del codice di procedura penale che procede in relazione al reato. Se non e' osservato quanto previsto dal presente comma, i risultati ottenuti mediante le tecnologie di riconoscimento facciale di cui al comma 1 non possono essere utilizzati e tutti i dati personali, i risultati e gli output acquisiti o prodotti sono cancellati, salvo che costituiscano corpo del reato.

4. Sulla base dei criteri di cui al comma 12, lettera a), l'utilizzo dei sistemi di videosorveglianza previsti dal comma 1, nei casi ivi contemplati, comporta il trattamento automatizzato, delle immagini del volto delle persone che accedono a luoghi o a eventi per i quali sussistono particolari esigenze di ordine e sicurezza pubblica, senza elaborazione dei relativi dati biometrici. Le immagini sono memorizzate, a livello locale, nella base dati di riferimento di cui al comma 12, lettera b). Nella medesima base dati sono altresi' memorizzati, senza ricorrere a tecnologie di riconoscimento biometrico, i corrispondenti dati anagrafici e, ove previsto un posto assegnato, il relativo identificativo, acquisiti mediante la scansione elettronica dei titoli di accesso. Successivamente alla commissione di un fatto di reato, l'attivazione delle tecnologie di riconoscimento facciale comporta l'elaborazione dei dati biometrici delle immagini presenti nella base dati locale di

cui al primo periodo, cui sono associati i dati memorizzati ai sensi del secondo periodo, per l'effettuazione del confronto a posteriori con i dati biometrici estratti dalle immagini del volto della persona indiziata del reato.

5. Il titolare del trattamento dei dati personali effettuato con l'utilizzo dei sistemi integrati dalle componenti di IA e dalle tecnologie di cui al comma 1 e' il Ministero dell'interno - Dipartimento della pubblica sicurezza.

6. Per i trattamenti di dati personali svolti con i sistemi integrati di cui al comma 1, il titolare del trattamento di cui al comma 5 effettua in via preventiva la valutazione d'impatto sulla protezione dei dati e consulta il Garante ai sensi degli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51. E' possibile effettuare un'unica valutazione d'impatto sulla protezione dei dati valida per tutti i sistemi analoghi.

7. I dati personali trattati con i sistemi integrati ai sensi del comma 1 sono conservati nella base di dati di riferimento individuata ai sensi del comma 12, lettera b), per sette giorni dalla raccolta e sono cancellati automaticamente decorso tale termine.

8. Gli accessi e le operazioni di trattamento sui sistemi di cui al presente articolo devono essere effettuati esclusivamente dalle persone autorizzate e registrati automaticamente in appositi file di log, non modificabili, conformemente a quanto previsto dall'articolo 12, paragrafo 3, del regolamento IA. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili per finalita' di verifica della liceita' del trattamento, di controllo interno e nell'ambito di un procedimento penale.

9. Restano fermi i termini di conservazione dei dati personali previsti, per finalita' di polizia, dall'articolo 10 del regolamento di cui al decreto del Presidente della Repubblica 15 gennaio 2018, n. 15.

10. Nessuna decisione che produca effetti giuridici negativi sulla persona cui si riferiscono i dati oggetto del trattamento puo' essere basata unicamente sui risultati forniti dall'applicazione di riconoscimento facciale. Si osservano, altresi', le garanzie e i limiti di cui all'articolo 8 del decreto legislativo n. 51 del 2018.

11. I sistemi di cui al comma 1 non possono essere in alcun caso utilizzati con l'attivazione delle tecnologie di riconoscimento facciale in modo non mirato, senza alcun collegamento con un reato o con un procedimento penale, ovvero a fini di controllo e di identificazione biometrica generalizzati o indiscriminati delle persone.

12. Con decreto del Ministro dell'interno, sentito il Garante, sono indicati:

a) i criteri per l'individuazione dei luoghi e degli eventi di cui al comma 4;

b) le modalita' del trattamento automatizzato delle immagini del volto, senza elaborazione dei dati biometrici, delle persone che accedono ai luoghi o agli eventi di cui al comma 4, e della loro memorizzazione a livello locale, ai sensi del primo e del secondo periodo del comma anzidetto, in una base dati di riferimento, per l'elaborazione e il confronto, esclusivamente a posteriori rispetto alla commissione di un fatto di reato, dei dati biometrici;

c) le misure tecniche e organizzative necessarie a garantire un adeguato livello di sicurezza del trattamento;

d) gli adempimenti cui il titolare del trattamento e' tenuto in conformita' a quanto previsto dal regolamento IA.

13. All'installazione e alla manutenzione delle componenti di IA e delle tecnologie biometriche di cui al comma 1 possono provvedere, senza nuovi o maggiori oneri per la finanza pubblica, i gestori dei luoghi di cui al comma 4, gli organizzatori o promotori degli eventi di cui al medesimo comma, ovvero chi ha la disponibilita' delle strutture ove tali eventi si svolgono, in accordo con i proprietari degli stessi luoghi o strutture, con particolare riferimento agli enti locali per le rispettive piattaforme di videosorveglianza, nonche', fermo quanto previsto al comma 5, in relazione ai ruoli svolti nel trattamento dei dati personali, nel rispetto del decreto legislativo n. 51 del 2018. Nelle ipotesi di cui al primo periodo, i predetti sistemi sono concessi in comodato gratuito alla questura, che ne acquisisce la completa ed esclusiva disponibilita'.

14. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare 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 ARTIFICIALE 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

Art. 11

Definizioni

1. Ai fini del presente titolo si applicano le definizioni di cui all'articolo 3 del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024.

Art. 12

Modifiche al codice penale

1. Al codice penale, dopo l'articolo 437 e' inserito il seguente:

«Art. 437-bis (Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi). - Chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana e' punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo per la vita o l'incolumita' pubblica o individuale. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena e' della reclusione da due a otto anni.

Salvo che il fatto costituisca piu' grave reato, chiunque, al di fuori dei casi indicati al primo comma, altera sistemi di intelligenza artificiale ad alto rischio e' punito, qualora dal fatto derivi un pericolo per la vita o l'incolumita' pubblica o individuale, con la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena e' della reclusione da tre a dieci anni.

Se taluno dei fatti previsti dal comma primo e' commesso per colpa grave, la pena e' ridotta da un terzo a un sesto.

L'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio che omette intenzionalmente di adottare misure di sorveglianza umana e' punito con le pene previste dal primo comma, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumita' pubblica o individuale oppure un pericolo per la sicurezza dello Stato».

Art. 13

Modifiche al codice di procedura penale

1. Al codice di procedura penale, dopo l'articolo 359-bis e'

inserito il seguente:

«Art. 359-ter (Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale) - 1. Quando occorre confermare l'identificazione di una persona nei confronti della quale vi sono sufficienti indizi della commissione di uno dei delitti di cui all'allegato II al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, puniti con la pena della reclusione non inferiore nel massimo a quattro anni, ovvero procedere alla ricerca mirata, ivi compresa la localizzazione, di una persona indiziata dei medesimi delitti, puo' essere autorizzato l'impiego di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale.

2. Quando occorre procedere alla ricerca di un latitante ai fini dell'esecuzione di un'ordinanza che dispone una misura cautelare coercitiva per uno dei delitti indicati al comma 1, ovvero di un ordine di esecuzione non sospeso che dispone la carcerazione per i medesimi delitti, puo' essere autorizzata la localizzazione della persona ricercata tramite identificazione biometrica remota in tempo reale con l'uso di sistemi di intelligenza artificiale, procedendo al confronto dei suoi dati biometrici con quelli di individui memorizzati in una banca dati di riferimento.

3. Nei casi di cui ai commi 1 e 2, il confronto biometrico avviene esclusivamente con una banca dati di riferimento adeguata per ciascuna delle finalita' di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate, di cui ai medesimi commi 1 e 2. La banca dati di cui al primo periodo puo' essere derivata da dati contenuti in banche dati in uso alla polizia giudiziaria o tenute da altre pubbliche amministrazioni e accessibili alla stessa o all'autorita' giudiziaria, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle indagini. Il contenuto della banca dati di cui al primo periodo e' formato appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalita', che sono cancellati al termine della validita' dell'autorizzazione, in modo da garantire che il set di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse. E' in ogni caso vietato l'uso di banche dati biometriche alimentate, in tutto o in parte, mediante tecniche di scraping non mirato, ovvero costituite in violazione delle disposizioni vigenti in materia di protezione dei dati personali.

4. Con le stesse modalita' di cui ai commi 1, 2 e 3 puo' essere

autorizzata la ricerca mirata, nell'ambito di un procedimento penale, di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani.

5. Nei casi di cui ai commi da 1 a 4 il pubblico ministero richiede l'autorizzazione all'impiego del sistema di intelligenza artificiale per l'identificazione biometrica remota in tempo reale al giudice per le indagini preliminari.

6. Il giudice per le indagini preliminari autorizza l'impiego del sistema di intelligenza artificiale di cui al comma 5 con decreto motivato. Nel provvedimento di autorizzazione e' delimitata l'area geografica di applicazione, sono indicate le persone specificamente ricercate ed e' determinato il tempo strettamente necessario, che non puo' in ogni caso superare i quindici giorni, prorogabili dal giudice, con decreto motivato, su richiesta del pubblico ministero, per periodi successivi di quindici giorni, qualora permangano le condizioni. L'autorizzazione puo' essere concessa soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento (UE) 2024/1689.

7. Quando ricorrono ragioni di urgenza e vi e' fondato motivo di ritenere che dal ritardo possa derivare pregiudizio grave e irreparabile per le finalita' di cui ai commi da 1 a 4, il pubblico ministero, con provvedimento adottato nel rispetto delle indicazioni di cui al comma 6, secondo periodo, dispone l'utilizzo del sistema di intelligenza artificiale per l'identificazione biometrica remota in tempo reale con decreto motivato. Il decreto e' comunicato immediatamente e comunque non oltre ventiquattro ore al giudice per le indagini preliminari, il quale, se ne ricorrono i presupposti, nelle successive quarantotto ore, convalida il provvedimento e autorizza la prosecuzione. Negli stessi casi di cui al primo periodo, se non sia possibile, per la situazione di urgenza, attendere il provvedimento del pubblico ministero, all'attivazione del sistema di identificazione biometrica remota in tempo reale provvedono gli ufficiali di polizia giudiziaria, i quali, senza ritardo e comunque entro le successive dodici ore, trasmettono la richiesta di autorizzazione al pubblico ministero, il quale, se ne ricorrono i presupposti, richiede al giudice la convalida entro ventiquattro ore dall'avvio del sistema. Il giudice, se ne ricorrono i presupposti, nelle successive quarantotto ore, convalida il provvedimento e autorizza la prosecuzione dell'attivita', con le indicazioni di cui al comma 6.

8. I risultati forniti 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 previste dai commi 6 e 7. In questi casi, tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato.».

Art. 14

Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale

1. All'articolo 104, comma 1, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui all'allegato al decreto legislativo 28 luglio 1989, n. 271, alla lettera e-bis), le parole: «del profilo personale» sono sostituite dalle seguenti: «generati anche con sistemi di intelligenza artificiale».

Art. 15

Modifiche al decreto legislativo 8 giugno 2001, n. 231

1. Al decreto legislativo 8 giugno 2001, n. 231, dopo l'articolo 25-undevicies, e' inserito il seguente:

«Art. 25-vicies (Reati commessi con l'uso di sistemi di intelligenza artificiale). - 1. In relazione al delitto di cui all'articolo 437-bis del codice penale, si applica all'ente la sanzione pecuniaria da seicento a mille quote.

2. In relazione al delitto di cui all'articolo 612-quater del codice penale, si applica all'ente la sanzione pecuniaria da duecento a settecento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b), c), d) ed e).».

[omissis]