

Decreto legislativo 9 settembre
2026 n. 160
Pubblicato sulla "Gazzetta
Ufficiale" del 15 settembre 2026 n.
214

Intelligenza artificiale, sì al ristoro per i danni prodotti dal sistema e pronto un nuovo reato

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

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'attività 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, nonché 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 tratta-

mento 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;

Vista la direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità 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 responsabilità amministrativa

delle persone giuridiche, delle società e delle associazioni anche prive di personalità 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, nonché 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 autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché 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 modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità 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:

TITOLO I

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

CAPO I

Disposizioni generali

ARTICOLO 1

Oggetto e finalità

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^[1], e della legge 23 settembre 2025, n. 132^[2].

2. Le disposizioni del presente titolo si applicano nel rispetto dei diritti fondamentali e delle libertà garantite 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, di non discriminazione, di sorveglianza umana e di trasparenza di cui all'articolo 3 della legge n. 132 del 2025^[3].

1 Si veda l'appendice.

2 «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», pubblicata sulla "Gazzetta Ufficiale" del 25 settembre 2025 n. 223.

3 **L'articolo 3 della legge 132/2025** è il seguente:
(Principi generali)

1. La ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengono 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.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati.

3. I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità e dei principi di cui al comma 1, assicurando la sorveglianza e l'intervento umano.

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 attività e per le finalità di polizia.

ARTICOLO 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^[4], 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^[5], 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^[6];

d) «pratiche vietate»: le pratiche di IA vietate a norma dell'articolo 5 del regolamento (UE) 2024/1689^[7];

e) «sistema di IA ad alto rischio»: un sistema di IA classificato ad alto rischio, conformemente all'articolo 6 del regolamento (UE) 2024/1689^[8] 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^[9];

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^[10];

h) «dati operativi sensibili»: i dati relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, indicati dall'articolo 3, punto 38), del regolamento (UE) 2024/1689^[11];

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^[12];

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) «Autorità 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^[13];

n) «Garante»: il Garante per la protezione dei dati personali, istituito dal codice in materia di protezione

4. L'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l'esercizio delle competenze e funzioni delle istituzioni territoriali sulla base dei principi di autonomia e sussidiarietà e non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo.

5. La presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi di intelligenza artificiale e per i modelli di intelligenza artificiale per finalità generali.

6. Al fine di garantire il rispetto dei diritti e dei principi di cui al presente articolo deve essere assicurata, quale preconditione essenziale, la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

7. La presente legge garantisce alle persone con disabilità il pieno accesso ai sistemi di intelligenza artificiale e alle relative funzionalità o estensioni, su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio, in conformità alle disposizioni della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, fatta a New York il 13 dicembre 2006, ratificata e resa esecutiva in Italia ai sensi della legge 3 marzo 2009, n. 18.

4 Si veda l'appendice.

5 Si veda la nota 2.

6 Si veda l'appendice.

7 Si veda l'appendice.

8 Si veda l'appendice.

9 Si veda l'appendice.

10 Si veda l'appendice.

11 Si veda l'appendice.

12 Si veda l'appendice.

13 **L'articolo 20 della legge 132/2025** è il seguente:

(Autorità nazionali per l'intelligenza artificiale)

1. Al fine di garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale, l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) sono designate quali Autorità nazionali per l'intelligenza artificiale, ferma restando l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689.

Conseguentemente, nel rispetto dei principi di cui alla presente legge e ferme restando le funzioni già rispettivamente attribuite:

a) l'AgID è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, fatto salvo quanto previsto dalla lettera b). L'AgID provvede altresì a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea;

b) l'ACN, anche ai fini di assicurare la tutela della cybersicurezza, come definita dall'articolo 1, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è responsabile per la vigilanza, ivi incluse le

dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196^[14];

o) «Forze di polizia»: le Forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121^[15];

p) «attività di polizia»: le attività di contrasto definite dall'articolo 3, punto 46), del regolamento (UE) 1689/2024^[16], svolte, nell'esercizio delle rispettive attribuzioni e funzioni, dagli organi, uffici e comandi delle Forze di polizia;

q) «finalità 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^[17], e per i quali sono svolte le attività 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^[18], e all'articolo 3 del regolamento (UE) 2024/1689^[19].

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

1. La ricerca, la sperimentazione, lo sviluppo, l'adde-

attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN è altresì responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza;

c) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea, sentiti il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale e il Ministero della giustizia per i modelli e i sistemi di intelligenza artificiale applicabili all'attività giudiziaria. Resta fermo quanto previsto dall'articolo 36, commi da 2-bis a 2-novies, del decreto-legge 30 aprile 2019, n. 34, convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58, per quanto concerne la sperimentazione di sistemi di intelligenza artificiale destinati ad essere immessi sul mercato, messi in servizio o usati da istituti finanziari.

2. Ferma restando l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689, l'AgID è designata quale autorità di notifica ai sensi dell'articolo 70 del medesimo regolamento e l'ACN è designata quale autorità di vigilanza del mercato e punto di contatto unico con le istituzioni dell'Unione europea ai sensi del medesimo articolo 70.

3. Le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo. A quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal Capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima. Al suddetto Comitato partecipano, quando si trattano questioni di rispettiva competenza, rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS. Ai componenti del Comitato non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

4. Restano fermi le competenze, i compiti e i poteri del Garante per la protezione dei dati personali e dell'Autorità per le garanzie nelle comunicazioni, quale Coordinatore dei Servizi Digitali ai sensi dell'articolo 15 del decreto-legge 15 settembre 2023, n. 123, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159.

5. All'articolo 8, comma 2, primo periodo, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo le parole: «Presidenza del Consiglio dei ministri» sono aggiunte le seguenti: «nonché dell'Agenzia per l'Italia digitale (AgID)».

14 «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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE», pubblicato sul supplemento ordinario n. 123 alla "Gazzetta Ufficiale" del 29 luglio 2003, n. 174.

15 **L'articolo 16 della legge 121/1981** (Nuovo ordinamento dell'amministrazione della pubblica sicurezza) è il seguente: (Forze di polizia)

Ai fini della tutela dell'ordine e della sicurezza pubblica, oltre alla polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze:

a) l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza;

b) il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica.

Fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, sono altresì forze di polizia e possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica il Corpo degli agenti di custodia e il Corpo forestale dello Stato. Le forze di polizia possono essere utilizzate anche per il servizio di pubblico soccorso.

16 Si veda l'appendice.

17 Si veda l'appendice.

18 **L'articolo 2 della legge 132/2025** è il seguente:

(Definizioni)

1. Ai fini della presente legge, si intendono per:

a) sistema di intelligenza artificiale: il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689;

b) dato: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva;

c) modelli di intelligenza artificiale: i modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689.

2. Per quanto non espressamente previsto, si rimanda alle definizioni di cui al regolamento (UE) 2024/1689.

19 Si veda l'appendice.

stramento, l'adozione, l'applicazione, la convalida e l'utilizzo di sistemi e modelli di intelligenza artificiale per le attività e le finalità delle Forze di polizia avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di cui all'articolo 3 della legge IA^[20], 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 attività di ricerca, sperimentazione, sviluppo e addestramento sono orientate al perseguimento della funzionalità e dell'affidabilità operativa dei sistemi e dei modelli di IA destinati a essere utilizzati dalle Forze di polizia, nella prospettiva di migliorare l'apporto tecnologico dell'intelligenza artificiale alle valutazioni e alle decisioni umane nella relativa attività.

3. Le Forze di polizia, in conformità 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 attività di polizia, allo scopo di incrementarne l'efficacia e l'efficienza.

4. L'utilizzo dei sistemi e dei modelli di IA nell'attività 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 è effettuata da personale individuato dalle procedure interne di ciascuna Forza di polizia ed è documentata in modo da assicurarne la tracciabilità.

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^[22] 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 attività 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 disponibilità delle Forze di

polizia in forza di norme di legge o regolamentari ovvero di atti amministrativi generali, è 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 attività 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.

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

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'attività di polizia, possono attivare collaborazioni con università, enti di ricerca e soggetti pubblici e privati, anche per il tramite di società in house o di società a totale partecipazione pubblica controllate dallo Stato, nel rispetto della disciplina dell'Unione europea in materia di concorrenza e di aiuti di Stato.

2. Il trattamento di dati per le finalità di cui al comma 1 è 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'attività 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 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, nel rispetto del codice della proprietà industriale di cui al decreto legislativo 10 febbraio 2005, n. 30^[23], dell'articolo 64 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382^[24], e della normativa di settore applicabile. I me-

20 Si veda la nota 3.

21 Si veda l'appendice.

22 «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 autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio», pubblicato sulla "Gazzetta Ufficiale" del 24 maggio 2018 n. 119.

23 «Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273», pubblicato sul supplemento ordinario n. 28 alla "Gazzetta Ufficiale" del 4 marzo 2005 n. 52.

24 **L'articolo 64 del Dpr 382/1980**, abrogato dall'articolo 7 del Dlgs 204/1998, era il seguente:
(Comitato per l'Anagrafe nazionale delle ricerche)

All'Anagrafe nazionale delle ricerche affluiranno 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. Sono fatte salve le disposizioni relative alla protezione dei segreti.

desimi rapporti individuano altresì, nel rispetto del decreto legislativo n. 51 del 2018^[25], i ruoli svolti dai soggetti coinvolti nel trattamento dei dati personali, specificando quando gli stessi operano quali titolari, controllori o responsabili del trattamento e disciplinando i relativi obblighi e responsabilità, anche con riferimento alle misure di sicurezza e alla documentazione delle operazioni di trattamento. È in ogni caso assicurata la titolarità in capo alle Forze di polizia 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

1. Il presente articolo costituisce base giuridica ai sensi dell'articolo 59, paragrafo 2, del regolamento IA^[26], nonché del decreto legislativo 18 maggio 2018, n. 51^[27], 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^[28], 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.

2. La partecipazione delle Forze di polizia agli spazi

di sperimentazione di cui al comma 1 è finalizzata allo sviluppo, alla realizzazione e alla prova di sistemi di IA, in particolare ad alto rischio, destinati alle attività di polizia, nel rispetto della protezione dei dati personali e della tutela dei diritti e delle libertà 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^[29], prevede il coinvolgimento del Garante laddove la stessa comporti, per il suo funzionamento, il trattamento di dati personali, ed è 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.

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^[30], su proposta delle Autorità 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 modalità di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e le attività del presente articolo.

Le amministrazioni, gli istituti e gli enti pubblici e privati che svolgono attività di ricerca scientifica e tecnologica per poter accedere ai finanziamenti pubblici devono essere iscritti in apposito schedario a cura dell'anagrafe nazionale delle ricerche. Le amministrazioni e gli enti erogatori sono tenuti a comunicare all'Anagrafe nazionale i finanziamenti concessi per l'attività di ricerca.

Le Università, le facoltà, i dipartimenti, gli istituti, il Consiglio nazionale delle ricerche e le altre amministrazioni ed enti interessati potranno accedere ai dati dell'Anagrafe nazionale delle ricerche.

All'Anagrafe sovrintende un comitato così composto:

- 1) il Ministro della pubblica istruzione o un suo delegato;
- 2) il Ministro per il coordinamento della ricerca scientifica e tecnologica o un suo delegato;
- 3) un rappresentante del Ministro della sanità;
- 4) un rappresentante del Ministro dell'industria, del commercio e dell'artigianato;
- 5) un rappresentante del Ministro dell'agricoltura;
- 6) un rappresentante del Ministro per i beni culturali e ambientali;
- 7) un rappresentante del Consiglio nazionale delle ricerche;
- 8) due rappresentanti degli enti ed istituti pubblici di ricerca designati dal Ministro incaricato del coordinamento della ricerca scientifica e tecnologica;
- 9) due rappresentanti eletti dai rettori delle Università;
- 10) due rappresentanti eletti dal Consiglio universitario nazionale;
- 11) il dirigente generale dell'istruzione universitaria o un suo delegato.

Le funzioni di segretario sono svolte da un funzionario del Ministero della pubblica istruzione con qualifica non inferiore a primo dirigente.

Il comitato si avvarrà per i supporti tecnici e amministrativi dei mezzi a disposizione del Ministero della pubblica istruzione e del relativo personale.

25 Si veda la nota 22.

26 Si veda l'appendice.

27 Si veda la nota 22.

28 Si veda l'appendice.

29 Si veda l'appendice.

30 **L'articolo 17 della legge 400/1988** (Disciplina dell'attività di Governo e ordinamento della presidenza del Consiglio dei Ministri) è il seguente:

(Regolamenti)

1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il parere del Consiglio di Stato che deve pronunciarsi entro novanta giorni dalla richiesta, possono essere emanati regolamenti per disciplinare:

- a) l'esecuzione delle leggi e dei decreti legislativi, nonché dei regolamenti comunitari;
- b) l'attuazione e l'integrazione delle leggi e dei decreti legislativi recanti norme di principio, esclusi quelli relativi a materie riservate alla competenza regionale;
- c) le materie in cui manchi la disciplina da parte di leggi o di atti aventi forza di legge, sempre che non si tratti di materie comunque riservate alla legge;
- d) l'organizzazione ed il funzionamento delle amministrazioni pubbliche secondo le disposizioni dettate dalla legge;

ARTICOLO 6

Formazione del personale di polizia

1. Le Forze di polizia provvedono ad attivare, presso i rispettivi istituti di formazione, specifici corsi in materia di intelligenza artificiale applicata alle attività di polizia, secondo modalità stabilite da ciascuna amministrazione nell'ambito delle risorse disponibili a legislazione vigente.

2. I corsi di cui al comma 1 assicurano, in attuazione dell'articolo 4 del regolamento IA^[31], il conseguimento dei seguenti risultati formativi minimi:

a) comprensione dei principi di funzionamento e delle potenzialità dei sistemi di intelligenza artificiale, con particolare riferimento alle loro applicazioni nelle attività di polizia;

b) conoscenza dei limiti, dei bias e degli errori dei sistemi di intelligenza artificiale, con specifica attenzione al riconoscimento biometrico e all'analisi predittiva;

c) capacità di interpretazione critica degli output dei sistemi di intelligenza artificiale e consapevolezza del ruolo della sorveglianza umana qualificata;

d) consapevolezza delle implicazioni giuridiche, etiche e di responsabilità connesse all'utilizzo dei sistemi di intelligenza artificiale a fini di polizia, con specifico riferimento alla disciplina di cui al regolamento IA, al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016^[32], e al decreto legislativo 18 maggio 2018, n. 51^[33],

e) consapevolezza dei rischi di cybersicurezza connessi all'utilizzo dei sistemi di intelligenza artificiale, anche con riferimento alle indicazioni dell'Agenzia per la cybersicurezza nazionale.

3. I risultati formativi di cui al comma 2, lettere b), c) ed e), sono assicurati nell'ambito degli specifici corsi concernenti i sistemi di IA ad alto rischio in uso nelle attività di polizia ovvero destinati a essere utilizzati nelle medesime attività.

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 pre-venzione 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

1. Nell'ambito delle attività di polizia, l'etichettatura, il filtraggio o la categorizzazione di set di dati biometrici acquisiti in conformità alla normativa vigente, ai sensi dell'articolo 5, paragrafo 1, lettera g), del regolamento IA^[34], sono consentiti a condizione che:

a) non siano finalizzati a inferire o dedurre le carat-

e) Abrogata

2. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato e previo parere delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, sono emanati i regolamenti per la disciplina delle materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi della Repubblica, autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari.

3. Con decreto ministeriale possono essere adottati regolamenti nelle materie di competenza del ministro o di autorità sottordinate al ministro, quando la legge espressamente conferisca tale potere.

Tali regolamenti, per materie di competenza di più ministri, possono essere adottati con decreti interministeriali, ferma restando la necessità di apposita autorizzazione da parte della legge. I regolamenti ministeriali ed interministeriali non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo. Essi debbono essere comunicati al Presidente del Consiglio dei ministri prima della loro emanazione.

4. I regolamenti di cui al comma 1 ed i regolamenti ministeriali ed interministeriali, che devono recare la denominazione di "regolamento", sono adottati previo parere del Consiglio di Stato, sottoposti al visto ed alla registrazione della Corte dei conti e pubblicati nella Gazzetta Ufficiale.

4 bis. L'organizzazione e la disciplina degli uffici dei Ministeri sono determinate, con regolamenti emanati ai sensi del comma 2, su proposta del Ministro competente d'intesa con il Presidente del Consiglio dei ministri e con il Ministro del tesoro, nel rispetto dei principi posti dal decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, con i contenuti e con l'osservanza dei criteri che seguono:

a) riordino degli uffici di diretta collaborazione con i Ministri ed i Sottosegretari di Stato, stabilendo che tali uffici hanno esclusive competenze di supporto dell'organo di direzione politica e di raccordo tra questo e l'amministrazione;

b) individuazione degli uffici di livello dirigenziale generale, centrali e periferici, mediante diversificazione tra strutture con funzioni finali e con funzioni strumentali e loro organizzazione per funzioni omogenee e secondo criteri di flessibilità eliminando le duplicazioni funzionali;

c) previsione di strumenti di verifica periodica dell'organizzazione e dei risultati;

d) indicazione e revisione periodica della consistenza delle piante organiche;

e) previsione di decreti ministeriali di natura non regolamentare per la definizione dei compiti delle unità dirigenziali nell'ambito degli uffici dirigenziali generali.

4-ter. Con regolamenti da emanare ai sensi del comma 1 del presente articolo, si provvede al periodico riordino delle disposizioni regolamentari vigenti, alla ricognizione di quelle che sono state oggetto di abrogazione implicita e all'espressa abrogazione di quelle che hanno esaurito la loro funzione o sono prive di effettivo contenuto normativo o sono comunque obsolete.

31 Si veda l'appendice.

32 «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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», pubblicato sulla "Gazzetta Ufficiale dell'Unione Europea" del 4 maggio 2016 n. 119.

33 Si veda la nota 22.

34 Si veda l'appendice.

teristiche di cui all'articolo 5, paragrafo 1, lettera g), del regolamento IA^[35];

b) siano funzionali ad attività di comparazione o ricerca ovvero ad ulteriori attività, comunque effettuate conformemente alla normativa vigente ed esclusivamente per finalità 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 finalità incompatibili con quelle per cui sono stati raccolti.

2. Il trattamento di dati personali nelle attività 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^[36], e 96, dello stesso regolamento^[37], ed è svolto nel rispetto di quanto previsto dal decreto legislativo 18 maggio 2018, n. 51^[38].

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

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 è ammesso per le finalità di prevenzione di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto ii), del regolamento IA^[39]. I sistemi di cui al primo periodo possono essere utilizzati, altresì, 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'arti-

colo 5, paragrafo 1, primo comma, lettera h), punto i), del regolamento IA^[40].

2. L'utilizzo dei sistemi di IA di cui al comma 1 è consentito esclusivamente per confermare l'identità 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 finalità 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 può 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 attività di polizia. Il contenuto della banca dati di cui al primo periodo è formato appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalità, che sono cancellati al termine della validità 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. È 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 è subordinato a una richiesta del questore o del comandante provinciale dell'Arma dei carabinieri e della Guardia di finanza, ovvero dei responsabili dei Servizi centrali di cui all'articolo 12 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203^[41], al procuratore della Re-

35 Si veda l'appendice.

36 Si veda l'appendice.

37 Si veda l'appendice.

38 Si veda la nota 22.

39 Si veda l'appendice.

40 Si veda l'appendice.

41 **L'articolo 12 del DL 152/1991** (Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa) è il seguente:

(Servizi centrali e interprovinciali della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza)

1. Per assicurare il collegamento delle attività investigative relative a delitti di criminalità organizzata, le amministrazioni interessate provvedono a costituire servizi centrali e interprovinciali della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza.

2. In determinate regioni e per particolari esigenze, i servizi prestati dal comma 1 possono essere costituiti in servizi interforze. Alla costituzione e alla organizzazione dei servizi interforze provvede con decreto il Ministro dell'interno, di concerto con i Ministri di grazia e giustizia, della difesa e delle finanze, assicurando la pari valorizzazione delle forze di polizia che vi partecipano.

3. A fini informativi, investigativi e operativi, i servizi indicati nei commi 1 e 2 si coordinano fra loro, nonché, se necessario, con gli altri organi o servizi di polizia giudiziaria previsti dalla legge e con gli organi di polizia esteri eventualmente interessati.

4. Quando procede a indagini per delitti di criminalità organizzata, il pubblico ministero si avvale di regola, congiuntamente, dei servizi di polizia giudiziaria della Polizia di Stato, dell'Arma dei carabinieri e, se richiesto dalla specificità degli accertamenti, del Corpo della guardia di finanza, ai quali, a norma dei commi 1 e 2, è attribuito il compito di svolgere indagini relative a tali delitti.

5. Il pubblico ministero impartisce le opportune direttive per l'effettivo coordinamento investigativo e operativo tra i diversi organismi di polizia giudiziaria.

pubblica presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione ovvero di ricerca, con indicazione della finalità 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, nonché con riferimento ad una area territoriale delimitata e alla indicazione delle persone specificamente interessate e ricercate. La medesima autorizzazione può essere concessa, altresì, soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento IA^[42].

6. Nei casi d'urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave e irreparabile per le finalità di cui al comma 1, l'utilizzo del sistema di IA può 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 è 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 è 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^[43]. 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^[44], di cui all'allegato al decreto legislativo 28 luglio 1989, n. 271.

6. Al secondo comma dell'art. 13 della legge 1° aprile 1981, n. 121, è aggiunto, in fine, il seguente periodo: "Assicura unità di indirizzo e coordinamento dei compiti e delle attività degli ufficiali ed agenti di pubblica sicurezza nella provincia, promuovendo le misure occorrenti".

7. Al secondo comma dell'art. 18 della legge 1° aprile 1981, n. 121, è aggiunto, in fine, il seguente periodo: "Del Comitato fa parte anche il direttore generale dell'Amministrazione penitenziaria".

8. Entro tre mesi dalla data di entrata in vigore della legge di conversione del presente decreto, il Ministro dell'interno emana direttive per la realizzazione a livello provinciale, nell'ambito delle potestà attribuite al prefetto a norma del comma 6, di piani coordinati di controllo del territorio da attuarsi a cura dei competenti uffici della Polizia di Stato e dei comandi provinciali dell'Arma dei carabinieri e della Guardia di finanza, ai quali possono partecipare, previa richiesta al sindaco, contingenti dei corpi o servizi di polizia municipale.

42. Si veda l'appendice.

43. Si veda la nota 22.

44. **L'articolo 226 delle norme di attuazione al Cpp** è il seguente: (Intercettazione e controlli preventivi sulle comunicazioni)

1. Il Ministro dell'interno o, su sua delega, i 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 nonché il questore o il comandante provinciale dei Carabinieri e della Guardia di finanza, richiedono al procuratore della Repubblica presso il tribunale del Capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo ovvero, nel caso non sia determinabile, del distretto in cui sono emerse le esigenze di prevenzione, l'autorizzazione all'intercettazione di comunicazioni o conversazioni, anche per via telematica nonché all'intercettazione di comunicazioni o conversazioni tra presenti anche se queste avvengono nei luoghi indicati dall'articolo 614 del codice penale, quando sia necessario per l'acquisizione di notizie concernenti la prevenzione di delitti di cui all'articolo 407, comma 2, lettera a), n. 4 e 51, comma 3-bis, del codice, nonché di quelli di cui all'articolo 51, comma 3-quater, del codice, commessi mediante l'impiego di tecnologie informatiche o telematiche. Il Ministro dell'interno può altresì delegare il Direttore della Direzione investigativa antimafia limitatamente ai delitti di cui all'articolo 51, comma 3-bis, del codice.

2. Il procuratore della Repubblica, qualora vi siano elementi investigativi che giustificano l'attività di prevenzione e lo ritenga necessario, autorizza l'intercettazione per la durata massima di giorni quaranta, prorogabile per periodi successivi di giorni venti ove permangano i presupposti di legge. L'autorizzazione alla prosecuzione delle operazioni è data dal pubblico ministero con decreto motivato, nel quale deve essere dato chiaramente atto dei motivi che rendono necessaria la prosecuzione delle operazioni.

3. Delle operazioni svolte e dei contenuti intercettati è redatto verbale sintetico che, unitamente ai supporti utilizzati, è depositato presso il procuratore che ha autorizzato le attività entro cinque giorni dal termine delle stesse. Il predetto termine è di dieci giorni se sussistono esigenze di traduzione delle comunicazioni o conversazioni. Il procuratore, verificata la conformità delle attività compiute all'autorizzazione, dispone l'immediata distruzione dei supporti e dei verbali.

3-bis. In deroga a quanto previsto dal comma 3, il procuratore può autorizzare, per un periodo non superiore a ventiquattro mesi, la conservazione dei dati acquisiti, anche relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, quando gli stessi sono indispensabili per la prosecuzione dell'attività finalizzata alla prevenzione di delitti di cui al comma 1.

4. Con le modalità e nei casi di cui ai commi 1 e 3, può essere autorizzato il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni.

5. In ogni caso gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale, fatti

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 conformità all'articolo 5, paragrafo 2, del regolamento IA^[45], per l'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale per le finalità 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^[46], ed effettua la valutazione d'impatto sulla protezione dei dati di cui agli articoli 23 e 24 del decreto legislativo n. 51 del 2018^[47].

2. Ogni utilizzo di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale per le finalità di cui al comma 1 è registrato automaticamente in appositi file di log, non modificabili, comprendenti necessariamente i dati previsti dall'articolo 12, paragrafo 3, del regolamento IA^[48]. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili esclusivamente alle sole autorità competenti per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale.

3. Restano fermi i termini di conservazione dei dati personali previsti, per finalità di polizia, dall'articolo 10 del regolamento, di cui al decreto del Presidente della Repubblica 15 gennaio 2018, n. 15^[49].

4. Dopo l'utilizzo dei sistemi di cui al comma 1, il titolare del trattamento effettua notifica al Garante, in

salvi i fini investigativi. In ogni caso le attività di intercettazione preventiva di cui ai commi precedenti, e le notizie acquisite a seguito delle attività medesime, non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate.

45 Si veda l'appendice.

46 Si veda l'appendice.

47 **L'articolo 23 del Dlgs 51/2018** (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 autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio) è il seguente:
(Valutazione d'impatto sulla protezione dei dati)

1. Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta 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.

2. La valutazione di cui al comma 1 contiene 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 presente decreto.

L'articolo 24 del Dlgs 51/2018 è il seguente:

(Consultazione preventiva del Garante)

1. Salvo quanto previsto dall'articolo 37, comma 6, il titolare del trattamento o il responsabile del trattamento consultano il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se:

- a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure
- b) 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.

2. Il Garante è consultato nel corso dell'esame di un progetto di legge o di uno schema di decreto legislativo ovvero di uno schema di regolamento o decreto non avente carattere regolamentare, suscettibile di rilevare ai fini della garanzia del diritto alla protezione dei dati personali.

3. Il Garante può stabilire un elenco di trattamenti soggetti a consultazione preventiva ai sensi del comma 1.

4. Il titolare del trattamento trasmette al Garante la valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 e, su richiesta, ogni altra informazione, al fine di consentire a detta autorità di effettuare una valutazione della conformità del trattamento, dei rischi per la protezione dei dati personali dell'interessato e delle relative garanzie.

5. Ove ritenga che il trattamento di cui al comma 1 violi le disposizioni del presente decreto, il Garante fornisce, entro un termine di sei settimane dal ricevimento della richiesta di consultazione, un parere per iscritto al titolare del trattamento e, se esistente, al responsabile del trattamento. Il Garante si avvale dei poteri di cui all'articolo 37, comma 3.

6. Il termine di cui al comma 5 può essere prorogato di un mese nel caso di trattamento complesso. Il Garante informa della proroga e dei motivi del ritardo il titolare del trattamento e, se esistente, il responsabile del trattamento, entro un mese dal ricevimento della richiesta di consultazione.

48 Si veda l'appendice.

49 **L'articolo 10 del Dpr 15/2018** (Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia) è il seguente:
(Termini di conservazione dei dati)

1. I dati personali oggetto di trattamento sono conservati per un periodo di tempo non superiore a quello necessario per il conseguimento delle finalità di polizia di cui all'articolo 3.

2. I dati personali soggetti a trattamento automatizzato, trascorsa la metà del tempo massimo di conservazione di cui al comma 3, se uguale o superiore a quindici anni, sono 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.

3. Fatto salvo quanto previsto dai commi 6 e 7, i dati personali non possono essere conservati oltre il termine massimo fissato come segue:

conformità a quanto previsto dall'articolo 5, paragrafo 4, del regolamento IA^[50]. La notifica, effettuata previo nulla osta dell'autorità giudiziaria competente che può 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 più attivazioni del sistema di IA per l'identificazione biometrica remota in tempo reale nello stesso contesto operativo ovvero di più utilizzi omogenei del predetto sistema, la notifica di cui al presente comma può essere effettuata in modo periodico e cumulativo, secondo i termini previsti dal decreto di cui al comma 5, ferma restando la necessità del nulla osta preventivo dell'autorità 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 Autorità 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 finalità 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 affidabilità e accuratezza dei sistemi di IA per l'identificazione biometrica remota in tempo reale;
- b) le modalità 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 rife-

- a) dati relativi a provvedimenti di natura interdittiva, di sicurezza e cautelare, nonché a misure restrittive della libertà personale conseguenti ad una sentenza di condanna - 20 anni dalla cessazione della loro efficacia;
 - b) dati relativi a misure di prevenzione di carattere personale e patrimoniale - 25 anni dalla cessazione della loro efficacia;
 - c) dati relativi a procedimenti, misure e provvedimenti su cui interviene una procedura di annullamento, invalidazione o revoca - 3 anni dalla data di inoppugnabilità del provvedimento di annullamento, invalidazione o revoca;
 - d) dati relativi a provvedimenti che dichiarano l'estinzione della pena o del reato - 8 anni dall'inoppugnabilità del provvedimento;
 - e) dati derivanti da attività informativa e ispettiva svolta per le finalità di cui all'articolo 3 - 15 anni dall'ultimo trattamento;
 - f) dati relativi ad attività di polizia giudiziaria conclusa con provvedimento di archiviazione - 20 anni dall'emissione del provvedimento;
 - g) dati relativi ad attività di polizia giudiziaria conclusa con sentenza di assoluzione o di non doversi procedere - 20 anni dal passaggio in giudicato della sentenza;
 - h) dati relativi ad attività di polizia giudiziaria conclusa con sentenza di condanna - 25 anni dal passaggio in giudicato della sentenza;
 - i) dati relativi ad attività di indagine o polizia giudiziaria che non hanno dato luogo a procedimento penale - 15 anni dall'ultimo trattamento;
 - l) dati relativi ad attività di prevenzione generale e soccorso pubblico - 5 anni dalla raccolta;
 - m) dati relativi a controlli di polizia - 20 anni dalla raccolta;
 - n) dati raccolti per l'analisi criminale e di prevenzione - 10 anni dall'elaborazione dell'analisi;
 - o) dati relativi a provvedimenti di espulsione e rimpatrio di stranieri - 30 anni dall'esecuzione;
 - p) dati relativi a nulla osta, licenze, autorizzazioni di polizia - 5 anni dalla scadenza o dalla revoca del titolo;
 - q) dati relativi alla detenzione delle armi o parti di esse, di munizioni finite e di materie esplodenti di qualsiasi genere - 5 anni dalla cessazione della detenzione;
 - r) dati relativi a persone detenute negli istituti penitenziari - 30 anni dalla scarcerazione a seguito di espiazione della pena in caso di condanna - 5 anni dalla scarcerazione a seguito di decreto di archiviazione o non luogo a procedere o di sentenza di assoluzione;
 - s) dati relativi a persone sottoposte a misure di sicurezza detentive - 25 anni dalla scadenza del termine di efficacia della misura;
 - t) dati relativi alla gestione delle attività operative - 10 anni dall'ultimo trattamento;
 - u) dati raccolti mediante sistemi di ripresa fotografica, audio e video nei servizi di ordine pubblico e di polizia giudiziaria - 3 anni dalla raccolta; dati raccolti mediante sistemi di videosorveglianza o di ripresa fotografica, audio e video di documentazione dell'attività operativa - 18 mesi dalla raccolta. Si applicano i diversi termini di conservazione di cui alla lettera b), quando i dati personali sono confluiti in un procedimento per l'applicazione di una misura di prevenzione, o quelli di cui alle lettere a), f), g), h) e i), quando i dati personali sono confluiti in un procedimento penale.
4. I termini di conservazione di cui al comma 3 sono aumentati di due terzi quando i dati personali sono trattati nell'ambito di attività preventiva o repressiva relativa ai delitti di cui all'articolo 51, commi 3-bis, 3-quater e 3-quinquies, del codice di procedura penale, nonché per le ulteriori ipotesi indicate dall'articolo 407, comma 2, lettera a), del codice di procedura penale.
5. Il Capo dell'ufficio o il comandante del reparto, prima della scadenza dei termini di cui al comma 3, ove sia strettamente necessario per il conseguimento delle finalità di polizia di cui all'articolo 3, può decidere, sulla base dei criteri definiti dal Capo della polizia - direttore generale della pubblica sicurezza ovvero, su sua delega, dal vice direttore generale di cui all'articolo 4, comma 6, del decreto-legge 29 ottobre 1991, n. 345, convertito, con modificazioni, dalla legge 30 dicembre 1991, n. 410, di aumentare la durata di conservazione, indicandone i motivi in relazione al caso specifico e l'ulteriore periodo di trattamento, che non può comunque superare i due terzi di quelli fissati al comma 3.
6. I dati personali soggetti a trattamento non automatizzato, sono conservati per il periodo di tempo previsto dalle disposizioni sullo scarto dei documenti d'archivio delle pubbliche amministrazioni se superiore a quello di cui al comma 3.
7. Sono fatti salvi i diversi termini e modalità di conservazione dei dati personali previsti da disposizioni di legge o di regolamento, da atti normativi dell'Unione europea o dal diritto internazionale in relazione a specifici trattamenti effettuati per le finalità di cui all'articolo 3.
8. Decorso i termini di cui ai commi 1, 3, 4, 5 e 7, i dati personali soggetti a trattamento automatizzato sono cancellati o resi anonimi, i dati personali non soggetti a trattamento automatizzato restano assoggettati alle disposizioni sullo scarto dei documenti d'archivio delle pubbliche amministrazioni.

⁵⁰ Si veda l'appendice.

rimento impiegate per il confronto biometrico, anche con riferimento alle relative misure di sicurezza, ai tempi e alle modalità di cancellazione dei dati e alle garanzie di non incrementalità 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 è 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 modalità di esecuzione della notifica di cui al comma 4;

h) gli ulteriori adempimenti cui il titolare del trattamento è tenuto in conformità a quanto previsto dal regolamento IA.

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

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 modalità previste dai commi 2 e 3. L'attivazione è 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 è 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 conformità all'articolo 26, paragrafo 10, primo comma, del regolamento IA⁵¹, l'autorizzazione di cui al comma 2 non è 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 è effettuato sotto la diretta ed esclusiva responsabilità 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 penale⁵² che procede in relazione al reato. Se non è 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

⁵¹ Si veda l'appendice.

⁵² **L'articolo 57 del Cpp** è il seguente:

(Ufficiali e agenti di polizia giudiziaria)

1. Salve le disposizioni delle leggi speciali, sono ufficiali di polizia giudiziaria:

a) 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;

b) gli ufficiali superiori e inferiori ed 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;

c) il sindaco dei comuni ove non abbia sede un ufficio della polizia di Stato ovvero un comando dell'arma dei carabinieri o della guardia di finanza;

2. Sono agenti di polizia giudiziaria:

a) il personale della polizia di Stato ai quali l'ordinamento dell'amministrazione della pubblica sicurezza riconosce tale qualità;

b) i carabinieri, le guardie di finanza, gli agenti di custodia, le guardie forestali e, nell'ambito territoriale dell'ente di appartenenza, le guardie delle province e dei comuni quando sono in servizio.

3. Sono altresì ufficiali e agenti di polizia giudiziaria, nei limiti del servizio cui sono destinati e secondo le rispettive attribuzioni, le persone alle quali le leggi e i regolamenti attribuiscono le funzioni previste dall'articolo 55.

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 altresì 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 è 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^[53]. È 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^[54]. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale.

9. Restano fermi i termini di conservazione dei dati personali previsti, per finalità di polizia, dall'articolo 10

del regolamento di cui al decreto del Presidente della Repubblica 15 gennaio 2018, n. 15^[55].

10. Nessuna decisione che produca effetti giuridici negativi sulla persona cui si riferiscono i dati oggetto del trattamento può essere basata unicamente sui risultati forniti dall'applicazione di riconoscimento facciale. Si osservano, altresì, le garanzie e i limiti di cui all'articolo 8 del decreto legislativo n. 51 del 2018^[56].

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 modalità 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 è tenuto in conformità 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 disponibilità 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, nonché, fermo quanto previsto al comma 5, in relazione ai ruoli svolti nel trattamento dei dati personali, nel rispetto del de-

53 Per gli articoli 23 e 24 del Dlgs 51/2018 si veda la nota 47.

54 Si veda l'appendice.

55 Si veda la nota 50.

56 L'articolo 8 del Dlgs 51/2018 è il seguente:

(Processo decisionale automatizzato relativo alle persone fisiche)

1. Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge.

2. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

3. Le decisioni di cui al comma 1 non possono basarsi sulle categorie particolari di dati personali di cui all'articolo 9 del regolamento UE, salvo che siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato.

4. Fermo il divieto di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea, è vietata la profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 9 del regolamento UE.

creto legislativo n. 51 del 2018^[57]. Nelle ipotesi di cui al primo periodo, i predetti sistemi sono concessi in comodato gratuito alla questura, che ne acquisisce la completa ed esclusiva disponibilità.

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

ARTICOLO 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^[58].

ARTICOLO 12

Modifiche al codice penale

1. Al codice penale, dopo l'articolo 437^[59] è 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 progetta-

zione, 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 è punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni.

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

Se taluno dei fatti previsti dal comma primo è commesso per colpa grave, la pena è 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 è punito con le pene previste dal primo comma, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato».

ARTICOLO 13

Modifiche al codice di procedura penale

1. Al codice di procedura penale, dopo l'articolo 359-bis^[60] è inserito il seguente:

«Art. 359-ter (Identificazione e localizzazione me-

57 Si veda la nota 22.

58 Si veda l'appendice.

59 **L'articolo 437 del Cp** è il seguente:

(Rimozione od omissione dolosa di cautele contro infortuni sul lavoro)

Chiunque omette di collocare impianti, apparecchi o segnali destinati a prevenire disastri o infortuni sul lavoro, ovvero li rimuove o li danneggia, è punito con la reclusione da sei mesi a cinque anni.

Se dal fatto deriva un disastro o un infortunio, la pena è della reclusione da tre a dieci anni.

60 **L'articolo 359-bis del Cpp** è il seguente:

(Prelievo coattivo di campioni biologici su persone viventi)

1. Fermo quanto disposto dall'articolo 349, comma 2-bis, quando devono essere eseguite le operazioni di cui all'articolo 224-bis e non vi è il consenso della persona interessata, il pubblico ministero ne fa richiesta al giudice per le indagini preliminari che le autorizza con ordinanza quando ricorrono le condizioni ivi previste.

2. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave o irreparabile pregiudizio alle indagini, il pubblico ministero dispone lo svolgimento delle operazioni con decreto motivato contenente i medesimi elementi previsti dal comma 2 dell'articolo 224-bis, provvedendo a disporre l'accompagnamento coattivo, qualora la persona da sottoporre alle operazioni non si presenti senza addurre un legittimo impedimento, ovvero l'esecuzione coattiva delle operazioni, se la persona comparsa rifiuta di sottoporvisi. Entro le quarantotto ore successive il pubblico ministero richiede al giudice per le indagini preliminari la convalida del decreto e dell'eventuale provvedimento di accompagnamento coattivo. Il giudice provvede con ordinanza al più presto e comunque entro le quarantotto ore successive, dandone avviso immediatamente al pubblico ministero e al difensore.

3. Nei casi di cui ai commi 1 e 2, le disposizioni degli articoli 132, comma 2, e 224-bis, commi 2, 4 e 5, si applicano a pena di nullità delle operazioni e di inutilizzabilità delle informazioni così acquisite. Si applicano le disposizioni di cui al comma 2 dell'articolo 191. 3-bis. Nei casi di cui agli articoli 589-bis e 590-bis del codice penale, qualora il conducente rifiuti di sottoporsi agli accertamenti dello stato di ebbrezza alcolica ovvero di alterazione correlata all'uso di sostanze stupefacenti o psicotrope, se vi è fondato motivo di ritenere che dal ritardo possa derivare grave o irreparabile pregiudizio alle indagini, il decreto di cui al comma 2 e gli ulteriori provvedimenti ivi previsti possono, nei casi di urgenza, essere adottati anche oralmente e successivamente confermati per iscritto. Gli ufficiali di polizia giudiziaria procedono all'accompagnamento dell'interessato presso il più vicino presidio ospedaliero al fine di sottoporlo al necessario prelievo o accertamento e si procede all'esecuzione coattiva delle operazioni se la

dante 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 2024⁶¹, 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, può 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, può essere autorizzata la localizzazione della persona ricercata tramite identificazione biometrica remota in tempo reale con l'uso di sistemi di intelligenza artificiale, procedendo al confronto dei suoi dati biometrici con quelli di individui memorizzati in una banca dati di riferimento.

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 finalità di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate, di cui ai medesimi commi 1 e 2. La banca dati di cui al primo periodo può 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'autorità 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 è formato appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalità, che sono cancellati al termine della validità 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. È 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 modalità di cui ai commi 1, 2 e 3 può essere autorizzata la ricerca mirata, nell'ambito di un procedimento penale, di specifiche vittime di sot-

trazione, 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 è delimitata l'area geografica di applicazione, sono indicate le persone specificamente ricercate ed è determinato il tempo strettamente necessario, che non può 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 può essere concessa soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento (UE) 2024/1689⁶².

7. Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare pregiudizio grave e irreparabile per le finalità 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 è 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'attività, 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 pro-

persona rifiuta di sottoporvisi. Del decreto e delle operazioni da compiersi è data tempestivamente notizia al difensore dell'interessato, che ha facoltà di assistervi, senza che ciò possa comportare pregiudizio nel compimento delle operazioni. Si applicano le previsioni di cui ai commi 1 e 2 dell'articolo 365. Entro le quarantotto ore successive, il pubblico ministero richiede la convalida del decreto e degli eventuali ulteriori provvedimenti al giudice per le indagini preliminari, che provvede al più presto e comunque entro le quarantotto ore successive, dandone immediato avviso al pubblico ministero e al difensore. Le operazioni devono sempre svolgersi nel rispetto delle condizioni previste dai commi 4 e 5 dell'articolo 224-bis.

61 Si veda l'appendice.

62 Si veda l'appendice.

dotti sono cancellati, salvo che costituiscano corpo del reato.».

ARTICOLO 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^[63], 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».

ARTICOLO 15

Modifiche al decreto legislativo 8 giugno 2001, n. 231

1. Al decreto legislativo 8 giugno 2001, n. 231, dopo l'articolo 25-undevicies^[64], è 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^[65], 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)^[66]».

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

1. Le disposizioni di cui all'articolo 17 si applicano

63 L'articolo 104 delle disposizioni di attuazione del Cpp, come modificato dal presente provvedimento, è il seguente:

(Esecuzione del sequestro preventivo)

1. Il sequestro preventivo è eseguito:

- 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;
 - b) sugli immobili o mobili registrati, con la trascrizione del provvedimento presso i competenti uffici;
 - 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;
 - d) sulle azioni e sulle quote sociali, con l'annotazione nei libri sociali e con l'iscrizione nel registro delle imprese;
 - 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 1998, n. 213. Si applica l'articolo 10, comma 3, del decreto legislativo 21 maggio 2004, n. 170.
- 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.

64 L'articolo 25-noviesdecies del Dlgs 231/2001 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300) è il seguente:

[Alias Art. 25-undevicies] (Delitti contro gli animali)

1. In relazione alla commissione dei delitti previsti dagli articoli 544-bis, 544-ter, 544-quater, 544-quinquies e 638 del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.
2. Nel caso di condanna o di applicazione della pena su richiesta delle parti, a norma dell'articolo 444 del codice di procedura penale, o di decreto penale di condanna, ai sensi dell'articolo 459 del codice di procedura penale, per i delitti di cui al comma 1 del presente articolo, si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, del presente decreto per una durata non superiore a due anni.
3. I commi 1 e 2 non si applicano ai casi previsti dall'articolo 19-ter delle disposizioni di coordinamento e transitorie per il codice penale.

65 L'articolo 612-quater del Cp è il seguente:

(Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale)

Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.

66 L'articolo 9 del Dlgs 231/2001 è il seguente:

(Sanzioni amministrative)

1. Le sanzioni per gli illeciti amministrativi dipendenti da reato sono:

- a) la sanzione pecuniaria;
- b) le sanzioni interdittive;
- c) la confisca;
- d) la pubblicazione della sentenza.

2. Le sanzioni interdittive sono:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

alle azioni di risarcimento del danno, sia contrattuale sia extracontrattuale, cagionato nell'utilizzo di un sistema di intelligenza artificiale.

2. Le disposizioni di cui agli articoli 18 e 19 si applicano alle azioni di risarcimento del danno di cui al comma 1 quando il danno deriva dalla violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024.

3. Restano ferme le disposizioni di cui all'articolo 82 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016^[67], e della normativa nazionale di recepimento della direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024^[68].

4. Nelle azioni di cui ai commi 1 e 2, quando il danneggiato è una persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, è altresì competente il giudice del luogo in cui il danneggiato ha la residenza o il domicilio.

ARTICOLO 17

Accesso alle prove

1. Nelle azioni di risarcimento del danno di cui all'articolo 16, comma 1, il giudice, su istanza della parte che allega di avere subito il danno, ordina all'altra parte o al terzo che ne dispone, l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento

del sistema di intelligenza artificiale, quando l'istante presenta fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema di intelligenza artificiale e il danno lamentato.

2. Tra gli elementi di prova di cui al comma 1 rientrano:

a) i registri di cui all'articolo 12 del regolamento (UE) 2024/1689^[69];

b) la documentazione relativa al sistema di gestione dei rischi di cui all'articolo 9 del regolamento (UE) 2024/1689^[70];

c) le informazioni pertinenti contenute nella documentazione tecnica di cui all'articolo 11 del regolamento (UE) 2024/1689^[71];

d) le informazioni relative ai parametri e alle modalità di supervisione umana di cui all'articolo 14 del regolamento (UE) 2024/1689^[72].

3. L'ordine di esibizione è limitato a quanto necessario e proporzionato rispetto alla domanda. Il giudice tiene conto degli interessi di tutte le parti, con particolare riguardo alla tutela dei segreti commerciali e delle informazioni riservate.

4. Quando l'esecuzione dell'ordine di cui al comma 1 comporta il rischio di divulgazione di segreti commerciali o di altre informazioni riservate, il giudice adotta le misure idonee a garantirne la tutela. Si applica l'articolo 121-ter del codice della proprietà industriale, di cui al decreto legislativo 10 febbraio 2005, n. 30^[73].

c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

e) il divieto di pubblicizzare beni o servizi.

67 **L'articolo 82 del Regolamento (UE) n. 679/2016** (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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) è il seguente: (Diritto al risarcimento e responsabilità)

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

68 «Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio», pubblicata sulla "Gazzetta Ufficiale dell'Unione Europea", serie L, del 18 novembre 2024.

69 Si veda l'appendice.

70 Si veda l'appendice.

71 Si veda l'appendice.

72 Si veda l'appendice.

73 **L'articolo 121-ter del Dlgs 30/2005** è il seguente:

(Tutela della riservatezza dei segreti commerciali nel corso dei procedimenti giudiziari)

1. Nei procedimenti giudiziari relativi all'acquisizione, all'utilizzazione o alla rivelazione illecite dei segreti commerciali di cui

5. Se la parte, senza giustificato motivo, non adempie, anche parzialmente, all'ordine di esibizione, il giudice può desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile^[74]. Quando l'inadempimento riguarda la documentazione di cui al comma 2, il giudice, valutato ogni altro elemento di prova, ritiene come ammessi i fatti allegati dall'istante.

6. Se il terzo, senza giustificato motivo, non adempie, anche parzialmente, all'ordine di esibizione, il giudice lo condanna a una pena pecuniaria da euro 1.500 a euro 10.000.

ARTICOLO 18

Presunzione del nesso di causalità

1. Quando il danno deriva dalla violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689, il nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria.

ARTICOLO 19

Rilevanza della conformità al regolamento (UE) 2024/1689

1. Fermo quanto previsto dalla normativa nazionale di recepimento della direttiva (UE) 2024/2853, la conformità del sistema di intelligenza artificiale agli obblighi previsti dal regolamento (UE) 2024/1689, anche se certificata ai sensi del capo III, sezione 5, del medesimo

regolamento^[75], non esclude di per sé la responsabilità del convenuto.

ARTICOLO 20

Azione diretta nei confronti dell'impresa di assicurazione

1. Chi intende promuovere l'azione di cui all'articolo 16 può chiedere preventivamente al soggetto a cui ritiene che sia imputabile il danno se è assistito da un contratto di assicurazione della responsabilità civile relativo al danno medesimo. La richiesta di cui al primo periodo non costituisce condizione di procedibilità della domanda. Il soggetto nei cui confronti è formulata la richiesta comunica entro trenta giorni dalla sua ricezione, l'esistenza di un contratto di assicurazione della responsabilità civile relativo al danno dedotto, gli estremi del contratto e la denominazione dell'impresa di assicurazione. In caso di omessa o incompleta comunicazione, il giudice può desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile^[76].

2. Il danneggiato ha azione diretta per il risarcimento del danno nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile al convenuto, nei limiti delle somme per le quali è stipulato il contratto di assicurazione.

3. Sono opponibili al danneggiato le eccezioni derivanti dal contratto di assicurazione, purché anteriori al sinistro.

all'articolo 98, il giudice può vietare ai soggetti da lui nominati o delegati, alle parti e ai loro rappresentanti e consulenti, ai difensori, al personale amministrativo, ai testimoni, e agli altri soggetti che a qualunque titolo hanno accesso ai provvedimenti, agli atti e ai documenti presenti nel fascicolo d'ufficio, l'utilizzo o la rivelazione dei segreti commerciali oggetto del procedimento che ritenga riservati. Il provvedimento di divieto di cui al primo periodo è pronunciato su istanza di parte e mantiene efficacia anche successivamente alla conclusione del procedimento nel corso del quale è stato emesso.

2. Il provvedimento di cui al comma 1 perde la sua efficacia:

a) se con sentenza, passata in giudicato, è accertato che i segreti commerciali oggetto di causa erano privi dei requisiti di cui all'articolo 98;

b) se i segreti commerciali diventano generalmente noti o facilmente accessibili agli esperti e agli operatori del settore.

3. Nei procedimenti giudiziari di cui al comma 1 il giudice, su istanza di parte, può adottare i provvedimenti che, nel rispetto dei principi regolatori del giusto processo, appaiano più idonei a tutelare la riservatezza dei segreti commerciali oggetto di causa, ed in particolare:

a) limitare ad un numero ristretto di soggetti l'accesso alle udienze e agli atti e ai documenti presenti nel fascicolo d'ufficio;

b) disporre, nei provvedimenti che definiscono i procedimenti di cui al comma 1, resi disponibili anche a soggetti diversi dalle parti, l'oscuramento o l'omissione delle parti contenenti i segreti commerciali.

4. Ai fini di cui al comma 3, lettera b), il giudice, con il provvedimento, indica le parti dello stesso che il cancelliere è tenuto ad oscurare o omettere all'atto del rilascio di copia a soggetti diversi dalle parti. Agli stessi fini il giudice ordina che, all'atto del deposito del provvedimento, la cancelleria vi apponga un'annotazione dalla quale risulti il divieto per le parti di diffondere il provvedimento in versione integrale.

74 **L'articolo 116 del Cpc** è il seguente:

(Valutazione delle prove)

Il giudice deve valutare le prove secondo il suo prudente apprezzamento, salvo che la legge disponga altrimenti.

Il giudice può desumere argomenti di prova dalle risposte che le parti gli danno a norma dell'articolo seguente, dal loro rifiuto ingiustificato a consentire le ispezioni che egli ha ordinate e, in generale, dal contegno delle parti stesse nel processo.

75 **Gli articoli da 40 a 49 della sezione 5 («Norme, valutazione della conformità, certificati, registrazione») del capo III del regolamento n. 2024/1689**, riguardano i seguenti ambiti:

Articolo 40, «Norme armonizzate e prodotti della normazione»;

Articolo 41, «Specifiche comuni»;

Articolo 42, «Presunzione di conformità a determinati requisiti»;

Articolo 43, «Valutazione della conformità»;

Articolo 44, «Certificati»;

Articolo 45, «Obblighi di informazione degli organismi notificati»;

Articolo 46, «Deroga alla procedura di valutazione della conformità»;

Articolo 47, «Dichiarazione di conformità UE»;

Articolo 48, «Marcatura CE»;

Articolo 49, «Registrazione».

76 Si veda la nota 74.

4. L'impresa di assicurazione che effettua il pagamento ha diritto di rivalsa verso l'assicurato, nella misura in cui avrebbe avuto titolo contrattuale per rifiutare o ridurre la propria prestazione.

5. Nel giudizio promosso ai sensi del comma 2 è litisconsorte necessario il soggetto individuato quale responsabile del danno.

6. L'azione diretta di cui al comma 2 è soggetta al medesimo termine di prescrizione dell'azione nei confronti del soggetto individuato quale responsabile del danno.

TITOLO III DISPOSIZIONI FINALI

CAPO I Disposizioni transitorie e finanziarie

ARTICOLO 21 *Disposizioni transitorie sull'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia*

1. I sistemi di IA che, alla data di entrata in vigore

del presente decreto, formano oggetto di rapporti contrattuali o sono in fase di sviluppo o di sperimentazione per finalità di polizia ovvero sono già in uso nell'attività di polizia, sono resi compatibili con le disposizioni del capo II del titolo I, da ciascuna Forza di polizia per quanto di rispettiva competenza, entro un anno dalla predetta data.

2. Per le disposizioni del titolo I la cui applicazione è prevista direttamente ovvero dipende dal regolamento IA, si osservano i termini di entrata in vigore e di compiuta attuazione dello stesso regolamento.

ARTICOLO 22

Clausola di invarianza finanziaria

1. Le amministrazioni interessate provvedono alle attività previste dal presente decreto mediante l'utilizzo delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.



BonelliErede

Master Corporate governance compliance integrata e gestione dei rischi

2° edizione

Organizzato da **BonelliErede** e **Il Sole 24 ORE Professionale**, il Master offre una visione completa sugli assetti di corporate governance, la compliance aziendale e i principali profili di rischio, con un approccio concreto e orientato all'operatività.

Un **percorso intensivo** dedicato a **giuristi d'impresa, avvocati** e **commercialisti** che desiderano consolidare le proprie competenze

sui principali profili di rischio per l'impresa: dal Modello 231 alla privacy e cybersicurezza, fino ai settori bancario, finanziario e assicurativo, alla tutela dell'ambiente, alla sicurezza sul lavoro e al diritto penale d'impresa.

Un **Master** pensato per **supportare** i **professionisti** nell'**analisi** e nella **gestione** delle principali tematiche che interessano la **governance d'impresa**.



Scopri il programma e
le modalità di partecipazione