



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

COMUNICAZIONE N. 102

AI PRESIDENTI DEGLI OMCEO

AI PRESIDENTI DELLE CAM

AI PRESIDENTI DELLE CAO

Oggetto: decreto legislativo 9 settembre 2026, n. 160 - Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale.

Cari Presidenti,

Si segnala per opportuna conoscenza che sulla Gazzetta Ufficiale n. 214 del 15-9-2026 è stato pubblicato il decreto legislativo indicato in oggetto di cui **si riportano di seguito le disposizioni di maggiore interesse così come illustrate nel dossier dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati.**

Articolo 8 (Coordinamento con le Autorità settoriali di vigilanza del mercato)

L'articolo 8 reca misure di coordinamento tra l'ACN e le Autorità nazionali settoriali sulla vigilanza dei prodotti disciplinati sia dal regolamento IA sia dalla normativa unionale di armonizzazione e prevede forme di accordo tra le diverse autorità e un meccanismo di risoluzione dei conflitti di competenza.

In particolare, il comma 1 prevede che l'Agenzia per cybersicurezza nazionale - ACN, nell'esercizio dei poteri di vigilanza e ispettivi, garantisce il coordinamento e la collaborazione con le pertinenti autorità settoriali di vigilanza del mercato responsabili dell'esecuzione della normativa di armonizzazione dei prodotti dell'Unione europea.

Le autorità settoriali di vigilanza del mercato sono le amministrazioni di cui all'articolo 3 del decreto legislativo n. 157 del 2022, designate da ciascuno Stato membro quali autorità responsabili dell'esecuzione alla normativa di armonizzazione dell'Unione europea elencata nell'allegato I del regolamento IA che reca venti atti normativi unionali che vanno dalle macchine, alla sicurezza dei giocattoli, **ai dispositivi medici**, agli aeromobili (articolo 1, comma 2, lettera c), del provvedimento in esame).

Ai sensi dell'articolo 74, paragrafo 3, del regolamento IA, per i sistemi di IA ad alto

FNOMCeO Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

rischio collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nel citato allegato I, sezione A, del regolamento IA, l'autorità di vigilanza del mercato è l'autorità responsabile delle attività di vigilanza del mercato designata a norma degli atti giuridici indicati nell'allegato (primo comma).

Il decreto legislativo n. 157 del 2022 (recante disposizioni di attuazione del regolamento (UE) 2019/1020 sulla vigilanza del mercato e sulla conformità dei prodotti, soggetti alla normativa di armonizzazione dell'Unione europea) individua tra le autorità settoriali di vigilanza del mercato il Ministero della salute.

Articolo 39 (Sistemi di intelligenza artificiale nelle pubbliche amministrazioni e valorizzazione del capitale umano)

L'articolo 39 definisce le attività del Ministro per la pubblica amministrazione ai fini dell'utilizzo dell'intelligenza artificiale nel settore della pubblica amministrazione, diretto tra l'altro al reclutamento e alla formazione del personale, anche attraverso l'utilizzo della Scuola nazionale dell'Amministrazione e la collaborazione di università, enti di ricerca e istituzioni dell'alta formazione artistica, musicale e coreutica.

In particolare, per la suddetta finalità, il Ministro per la pubblica amministrazione (comma 1):

- indirizza e coordina le politiche di reclutamento, di formazione di base, di formazione continua, di riqualificazione professionale e di alta formazione dei dipendenti pubblici;
- adotta le misure volte a sostenere l'introduzione, l'utilizzo e la diffusione dei sistemi di intelligenza artificiale, favorendo l'innovazione organizzativa e gestionale delle amministrazioni pubbliche, la semplificazione amministrativa e la accelerazione dei procedimenti.

A tal fine si prevede che il Ministro per la pubblica amministrazione si avvale della Scuola nazionale dell'Amministrazione, nonché della collaborazione, previa convenzione, di università, enti di ricerca e istituzioni dell'alta formazione artistica, musicale e coreutica (AFAM) (comma 2).

Per quanto riguarda l'utilizzo dell'IA nella PA, si ricorda che il Piano triennale per l'informatica nella Pubblica amministrazione 2024-2026 – che fissa gli obiettivi e individua i principali interventi di sviluppo e gestione dei sistemi informativi delle PA (art. 14-*bis* del D.Lgs. 82/2005 Codice dell'amministrazione digitale CAD) – detta i principi generali per il suo utilizzo e prevede l'adozione da parte dell'Agenzia per l'Italia digitale delle Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione e delle Linee Guida per il procurement di IA nella Pubblica Amministrazione, adottate con la Determinazione n.43/2026 e sulle quali è stata aperta una consultazione pubblica



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

terminata l'11 aprile 2026. Dal 18 febbraio al 20 marzo 2025 si è svolta la consultazione pubblica delle Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, adottate con la Determinazione n.17/2025, il cui iter di adozione è in corso.

Articolo 40 (Tutela del lavoratore nei processi decisionali assistiti da sistemi di intelligenza artificiale)

L'articolo 40 dello schema reca norme di tutela del lavoratore relative ai processi decisionali assistiti da sistemi di intelligenza artificiale. Il comma 1 esclude che le decisioni relative alla costituzione, alla modificazione o alla risoluzione del rapporto di lavoro, ivi compresi i provvedimenti disciplinari, siano adottate unicamente sulla base di un trattamento automatizzato, basato su sistemi di intelligenza artificiale, **e richiede che la decisione definitiva sia riservata dal datore di lavoro a una persona fisica, la quale deve esercitare un potere effettivo e autonomo. Il comma 4 stabilisce che il licenziamento intimato in violazione delle suddette prescrizioni è nullo.** Il comma 2 richiama, riguardo all'utilizzo dei sistemi di intelligenza artificiale, il rispetto della dignità e della riservatezza del lavoratore e il principio di non discriminazione. Il comma 3 conferma l'obbligo del datore di lavoro di informare in via preventiva il lavoratore dell'utilizzo di sistemi di intelligenza artificiale e prevede il diritto del lavoratore di ottenere, su richiesta e mediante l'intervento di una persona fisica, una motivazione intelligibile della decisione che lo riguarda, comprensiva dell'indicazione dell'eventuale incidenza dei sistemi di intelligenza artificiale sul processo decisionale e dei principali parametri considerati.

Articolo 41 (Formazione in materia di IA delle università, degli enti pubblici di ricerca e delle istituzioni AFAM)

L'articolo 41 prevede, al comma 1, che le università, gli enti pubblici di ricerca e le istituzioni AFAM possono mettere a disposizione professori, ricercatori e tecnologi, sulla base di appositi accordi, per attività di alfabetizzazione, formazione e divulgazione sull'intelligenza artificiale (IA).

Il comma 2 dispone che la formazione sull'uso sicuro e responsabile dell'IA rivolta ai professionisti può essere organizzata anche da ordini professionali e associazioni di categoria.

Il comma 3 precisa che si tiene conto della partecipazione di professori, ricercatori e tecnologi a queste attività nell'ambito della valutazione della loro carriera scientifica.

Articolo 42 (Integrazione di attività formative nei corsi dell'istruzione superiore e negli ITS Academy)

FNOMCeO Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri

Via Ferdinando di Savoia, 1 – 00196 Roma – Tel. 06 36 20 31 Fax 06 32 22 794 – e-mail: presidenza@fnomceo.it – C.F. 02340010582



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

L'articolo 42 disciplina l'integrazione nei percorsi universitari, nelle istituzioni AFAM e negli istituti tecnologici superiori (*ITS Academy*) di attività formative in materia di intelligenza artificiale.

Il comma 1 prevede l'obbligo per università e istituzioni AFAM di promuovere attività formative sull'intelligenza artificiale, volte a comprenderne il funzionamento tecnico, usarla in modo sicuro e consapevole e interpretarne correttamente i risultati.

Il comma 2 stabilisce che la formazione sull'IA debba coprire gli aspetti tecnici, giuridici, funzionali, etici e relativi ai diritti fondamentali, differenziando l'integrazione dei contenuti in base alle caratteristiche del corso di studio.

Il comma 3 definisce quali sono i contenuti minimi delle predette attività formative e il comma 4 indica le modalità attraverso le quali la formazione potrebbe essere erogata. Il comma 5 affida al MUR il monitoraggio annuale dell'attuazione delle previsioni di cui ai commi precedenti, e il comma 6 demanda a un decreto ministeriale, sentita l'ANVUR, la definizione degli indicatori di monitoraggio, delle modalità operative, dei criteri di valorizzazione nelle politiche di incentivazione e delle forme di partecipazione ai gruppi di lavoro europei. Il comma 7 dispone che gli ITS Academy, con particolare riferimento a quelli afferenti all'Area tecnologica, promuovono percorsi formativi per sviluppare competenze nell'uso consapevole, responsabile e sicuro dell'intelligenza artificiale.

Articolo 43 (Valorizzazione delle attività di ricerca e di trasferimento tecnologico svolte dalle istituzioni della formazione superiore e della ricerca e dagli ITS Academy)

L'articolo 43 introduce disposizioni per la valorizzazione delle attività di ricerca e di trasferimento tecnologico svolte dalle istituzioni della formazione superiore e della ricerca e dagli *ITS Academy*. Il comma 1 autorizza università, enti pubblici di ricerca e istituzioni AFAM a stipulare convenzioni con organismi di ricerca privati e imprese in materia di intelligenza artificiale, per usare infrastrutture e competenze nello svolgimento di attività comuni di ricerca e sperimentazione tecnologica.

Il comma 2 consente agli stessi soggetti di stipulare accordi con le Autorità nazionali per l'intelligenza artificiale, per promuovere e supportare spazi di sperimentazione normativa e altre attività di interesse comune, anche con il mondo produttivo.

Il comma 3 autorizza l'assegnazione temporanea di personale presso le Autorità nazionali per l'IA, per attività di supporto agli spazi di sperimentazione normativa e i commi 4 e 5 dettano una specifica disciplina per regolare periodo di assegnazione.

Il comma 6 prevede la stipula da parte delle istituzioni della formazione superiore e della ricerca di convenzioni con imprese per lo sviluppo e il finanziamento di



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

dottorati in materia di IA e favorire la creazione di *spin-off* universitari e *start-up*.

Il comma 7 promuove la collaborazione degli *ITS Academy* con università, enti di ricerca, istituzioni AFAM e Autorità nazionali in materia di intelligenza artificiale, demandando al Comitato nazionale *ITS Academy* la definizione dei relativi criteri e modalità.

I commi 8 e 9 demandano a un decreto ministeriale l'individuazione dei centri di riferimento per la sperimentazione normativa in materia di IA e la definizione delle modalità di collaborazione con le Autorità nazionali per l'intelligenza artificiale.

Infine, il comma 10 stabilisce che accordi e convenzioni con le Autorità definiscano programmi, impegni, obblighi e responsabilità dei soggetti coinvolti.

Articolo 45 (Formazione in materia di intelligenza artificiale per le professioni)

L'articolo 45 introduce, nell'ambito della formazione professionale, specifici percorsi di alfabetizzazione e formazione sull'utilizzo dei sistemi di intelligenza artificiale (IA), rivolti sia ai professionisti iscritti ad ordini e collegi, sia, in determinati casi, ai professionisti appartenenti alle professioni non organizzate in ordini o collegi. La disposizione individua, inoltre, i contenuti minimi dei percorsi formativi, disciplina le modalità di adeguamento dei regolamenti professionali e reca una specifica previsione per le professioni sanitarie.

L'articolo 45, comma 1, dello schema di decreto legislativo stabilisce un obbligo fondamentale per gli ordini professionali, i quali sono tenuti a integrare nei propri percorsi di formazione professionale iniziale e di formazione continua specifici programmi di alfabetizzazione e addestramento all'uso dei sistemi di intelligenza artificiale. Questa disposizione non si limita a una semplice indicazione programmatica, ma impone una trasformazione strutturale del bagaglio di competenze dei professionisti iscritti ad albi, rendendo la conoscenza tecnologica una parte integrante del loro percorso di aggiornamento obbligatorio.

Il comma 1 dà attuazione alla delega conferita al Governo dalla legge 23 settembre 2025, n. 132 (cosiddetta "Legge IA"), che all'articolo 24, comma 2, lettera f), prevedeva esplicitamente l'introduzione di percorsi formativi per professionisti e operatori di settore sull'uso dell'intelligenza artificiale. La norma si pone inoltre in costante dialogo con il Regolamento (UE) 2024/1689 (AI Act), il quale all'articolo 4 introduce il concetto di alfabetizzazione in materia di IA (AI literacy) come misura necessaria per garantire che chiunque si occupi del funzionamento o dell'utilizzo di tali sistemi possieda una consapevolezza tecnica e critica adeguata.

In termini di finalità, l'intervento legislativo mira a garantire che l'integrazione di



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

questi strumenti nelle professioni intellettuali avvenga nel rispetto della prospettiva antropocentrica definita dall'articolo 1, comma 1, della citata legge n. 132 del 2025, la quale stabilisce che l'IA debba sempre essere utilizzata in modo corretto, trasparente e responsabile, ponendo l'essere umano al centro dello sviluppo tecnologico.

Tale formazione obbligatoria diventa dunque lo strumento primario per prevenire fenomeni di responsabilità derivanti da un uso non diligente o improvvido della tecnologia, come le cosiddette allucinazioni algoritmiche, assicurando che il **professionista mantenga sempre il controllo e la supervisione umana sul risultato finale della prestazione.**

Il comma 2 dell'articolo 45 del suddetto decreto legislativo specifica gli elementi contenutistici e didattici che devono necessariamente caratterizzare i percorsi di alfabetizzazione e formazione professionale sull'intelligenza artificiale (IA) introdotti dal comma precedente.

La norma delinea un programma formativo articolato su tre pilastri fondamentali, volti a garantire che il professionista non solo apprenda l'uso tecnico dello strumento, ma ne comprenda anche le implicazioni legali ed etiche all'interno del proprio specifico settore di riferimento.

Il primo pilastro riguarda i profili tecnici, imponendo che la formazione copra il funzionamento dei sistemi di IA, con particolare attenzione alle tecniche di interrogazione e istruzione (comunemente note come *prompt engineering*), fondamentali per ottenere risultati accurati. Oltre alle potenzialità, il percorso formativo deve esplicitare chiaramente i limiti di tali tecnologie, assicurando che il professionista sia consapevole dei margini di errore e delle possibili criticità operative legate all'impiego di specifici algoritmi nel proprio ambito lavorativo (**lett. a).**

In secondo luogo, la disposizione stabilisce **l'obbligo di approfondire i profili giuridici relativi alla disciplina dei sistemi di intelligenza artificiale**. Il riferimento normativo centrale in questo ambito è il Regolamento (UE) 2024/1689 (noto come *AI Act*), approvato dal Parlamento europeo e dal Consiglio il 13 giugno 2024, che rappresenta la cornice regolatoria armonizzata a livello comunitario. La formazione deve dunque aggiornare i professionisti sia su questo regolamento europeo sia sulle correlate disposizioni nazionali di attuazione, garantendo la piena conformità legale delle attività professionali assistite dall'IA (**lett. b).**

Infine, il terzo pilastro si focalizza sui profili deontologici, trattando in modo discorsivo le responsabilità che il professionista assume quando decide di avvalersi di sistemi algoritmici.

Questo include la definizione degli obblighi informativi verso il paziente, un



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

aspetto cruciale per mantenere il rapporto fiduciario, e il rispetto assoluto del principio antropocentrico. Tale principio è esplicitamente richiamato dal già richiamato articolo 1, comma 1, della legge 23 settembre 2025, n. 132, che stabilisce che lo sviluppo e l'applicazione dell'IA devono essere sempre orientati alla tutela della dignità umana e alla garanzia che l'essere umano mantenga il controllo e la decisione finale sulla prestazione professionale (lett. c).

Il comma 3 dell'articolo 45 definisce i criteri quantitativi e le modalità attuative dei percorsi formativi sull'intelligenza artificiale per i professionisti, stabilendo che tali corsi debbano prevedere un monte ore minimo per ogni periodo di valutazione della formazione continua, in linea con quanto già previsto dalle specifiche disposizioni di settore per ciascuna categoria professionale. Questa norma garantisce che l'alfabetizzazione tecnologica non sia lasciata alla discrezionalità dei singoli, ma diventi un obbligo misurabile e integrato nei sistemi di crediti formativi esistenti. Il legislatore specifica, inoltre, che i contenuti dettagliati, le metodologie di erogazione e la periodicità di questi aggiornamenti devono essere stabiliti seguendo le procedure descritte nel comma 5 dello stesso articolo, mantenendo però l'obbligo tassativo di rispettare i requisiti minimi di competenza tecnica, giuridica e deontologica delineati nei primi due commi della disposizione.

Il comma 5 stabilisce compiti specifici per le forme aggregative delle associazioni: in particolare, queste realtà sono tenute a rendere facilmente conoscibili i percorsi formativi proposti e, aspetto fondamentale, le modalità di accertamento dell'effettivo assolvimento dell'obbligo di aggiornamento da parte dei professionisti iscritti.

Il comma 6 dell'articolo 45 introduce una disciplina speciale per le professioni sanitarie, stabilendo che l'integrazione dei percorsi formativi sull'intelligenza artificiale (IA) debba avvenire all'interno del sistema dell'educazione continua in medicina (ECM). A differenza di altre categorie professionali, per le quali l'adeguamento dei programmi è rimesso direttamente ai rispettivi consigli nazionali o organismi di regolazione, per l'ambito sanitario la norma prevede che l'inclusione di tali percorsi sia disposta attraverso un accordo da sancire in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano. Tale accordo deve essere adottato entro il termine di sei mesi dall'entrata in vigore del decreto e ha il compito di definire le modalità con cui i



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

professionisti della salute acquisiranno le competenze necessarie per utilizzare i sistemi algoritmici in modo sicuro e responsabile.

Il comma 6 opera un rinvio interno ai commi 2 e 3 del medesimo articolo 45, imponendo che l'accordo in Conferenza Stato-Regioni garantisca il rispetto di precisi requisiti minimi di contenuto e di durata.

Il comma si coordina inoltre con quanto previsto dall'articolo 47 dello schema, il quale dettaglia ulteriormente il ruolo della Commissione nazionale per la formazione continua nel definire la quota specifica di crediti ECM triennali da destinare a questa materia, e dell'AGENAS per quanto concerne la formazione manageriale in sanità. In questo quadro, il comma 6 dell'articolo 45 funge da cerniera procedurale, assicurando che l'alfabetizzazione in materia di IA, richiesta anche dall'articolo 4 del Regolamento (UE) 2024/1689, venga declinata tenendo conto delle specificità del settore sanitario e delle competenze regionali in materia di salute.

Il riferimento alle professioni sanitarie riguarda le professioni assoggettate al sistema di educazione continua in medicina (ECM), (tra cui medici chirurghi e odontoiatri), disciplinato dagli articoli 16-bis e seguenti del decreto legislativo 30 dicembre 1992, n. 502, nonché dalla normativa di settore relativa alle singole professioni sanitarie.

Articolo 46 (Norme in materia di equo compenso)

L'articolo 46 dello schema di decreto legislativo disciplina l'impatto dell'intelligenza artificiale sulla determinazione dei compensi professionali.

Il comma 1 stabilisce che l'impiego di sistemi di intelligenza artificiale da parte di un professionista può dare luogo a una modulazione dell'equo compenso, ai sensi della legge 21 aprile 2023, n. 49. Tale variazione deve basarsi su parametri specifici che tengano conto della classificazione di rischio del sistema tecnologico utilizzato, seguendo i criteri definiti dal Regolamento (UE) 2024/1689.

La legge 21 aprile 2023, n. 49 reca una disciplina organica volta a garantire la dignità e la proporzionalità della remunerazione dei professionisti intellettuali, definendo l'equo compenso come un corrispettivo necessariamente proporzionato alla quantità e alla qualità del lavoro svolto, nonché al contenuto e alle caratteristiche specifiche della prestazione professionale. La normativa stabilisce un legame inscindibile tra l'equità del compenso e la conformità ai parametri ministeriali di riferimento, individuati per le altre professioni ordinistiche dai ministeri vigilanti.

L'ambito di applicazione della legge è circoscritto ai rapporti professionali regolati da convenzioni in cui il committente è rappresentato da soggetti dotati di un forte potere contrattuale, come le imprese bancarie e assicurative, le loro controllate e



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

mandatarie, nonché le grandi imprese che superano determinati requisiti dimensionali legati al numero di dipendenti e al fatturato. La tutela viene estesa anche alle prestazioni rese in favore della Pubblica Amministrazione e delle società a partecipazione pubblica, mentre restano esclusi specifici ambiti come le società veicolo di cartolarizzazione e gli agenti della riscossione. Un elemento cardine della riforma è la presunzione legale secondo cui gli accordi vincolanti per il professionista si considerano unilateralmente predisposti dalle imprese contraenti, salva prova contraria, gravando così su queste ultime l'onere della correttezza negoziale.

Il meccanismo di protezione si fonda sulla nullità delle clausole che prevedono un compenso inferiore ai minimi tabellari o che attribuiscono al cliente vantaggi sproporzionati, come la facoltà di modifica unilaterale del contratto, l'imposizione di prestazioni aggiuntive gratuite o la pattuizione di termini di pagamento superiori ai sessanta giorni. Tale nullità, definita "di protezione", opera esclusivamente a vantaggio del professionista e può essere rilevata d'ufficio dal giudice, senza inficiare la validità dell'intero contratto. In caso di accertata violazione, il professionista ha il diritto di adire l'autorità giudiziaria per ottenere la rideterminazione del compenso e un eventuale indennizzo fino al doppio della differenza dovuta, ferma restando la possibilità per gli ordini di rilasciare pareri di congruità con efficacia di titolo esecutivo qualora non opposti entro quaranta giorni.

Il regolamento (UE) 2024/1689 (AI Act) introduce una disciplina armonizzata dell'intelligenza artificiale nell'Unione europea fondata su un approccio basato sul rischio, che distingue tra pratiche vietate, sistemi ad alto rischio, sistemi soggetti a obblighi di trasparenza e sistemi a rischio limitato o minimo. Il regolamento disciplina gli obblighi dei diversi operatori della filiera dell'IA, prevede requisiti specifici per i sistemi ad alto rischio e per i modelli di IA per finalità generali e istituisce meccanismi di vigilanza, controllo e promozione dell'innovazione.

Il comma 2 stabilisce un preciso cronoprogramma per l'adeguamento economico delle prestazioni professionali all'era dell'intelligenza artificiale (IA), fissando il termine di dodici mesi dall'entrata in vigore della norma per l'integrazione della normativa vigente. Questo intervallo temporale è concesso affinché le autorità competenti possano aggiornare i criteri di calcolo dei compensi, riflettendo le trasformazioni introdotte dall'impiego dei sistemi algoritmici nell'attività d'opera intellettuale. Il legislatore dispone, infatti, che debbano essere integrati i decreti ministeriali già previsti da tre pilastri normativi fondamentali della disciplina professionale italiana. Nello specifico, la disposizione richiama l'articolo 9 del decreto-legge 24 gennaio 2012, n. 1, che rappresenta la norma generale sui parametri per la liquidazione dei compensi delle professioni regolamentate nel sistema ordinistico; nonché l'articolo 13,

FNOMCeO Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri

Via Ferdinando di Savoia, 1 – 00196 Roma – Tel. 06 36 20 31 Fax 06 32 22 794 – e-mail: presidenza@fnomceo.it – C.F. 02340010582



FNOMCeO

Federazione Nazionale degli Ordini
dei Medici Chirurghi e degli Odontoiatri

comma 6, della legge 31 dicembre 2012, n. 247.

Articolo 48 (Formazione in materia di intelligenza artificiale nell'ambito della formazione continua in medicina -ECM- e della formazione manageriale in sanità)

L'articolo 48 stabilisce che nell'ambito della educazione continua in medicina (ECM) devono essere previsti percorsi di alfabetizzazione e formazione all'uso dei sistemi di intelligenza artificiale indirizzati ai professionisti sanitari (comma 1).

Il comma 2 specifica l'articolazione di tali percorsi, i quali includono:

- a) profili tecnici riguardanti il funzionamento, comprese le tecniche di interrogazione e istruzione, le potenzialità e i limiti dei sistemi di intelligenza artificiale adoperati nel settore professionale di riferimento;
- b) profili giuridici riguardanti la disciplina dei sistemi di intelligenza artificiale, con riferimento al regolamento IA e alle disposizioni attuative nazionali;
- c) profili deontologici riguardanti le responsabilità del professionista nell'uso dei sistemi di intelligenza artificiale, gli obblighi informativi nei confronti del cliente e il rispetto del principio antropocentrico previsto dall'articolo 1, comma 1, della legge IA.

Il comma 3 prevede la definizione, entro sei mesi dall'entrata in vigore del decreto legislativo in esame, da parte della Commissione nazionale per formazione continua, prevista dall'articolo 16-ter del D.Lgs. n. 502 del 1992, di una specifica percentuale dell'obbligo formativo individuale triennale indirizzata ai percorsi formativi delineati dal comma 1, nell'ambito del programma di educazione continua in medicina, previsto dall'articolo 16-bis del citato D.Lgs. n. 502 del 1992.

Il comma 4, infine, attribuisce all'AGENAS (Agenzia nazionale per i servizi sanitari regionali) il compito di individuare, entro sei mesi dall'entrata in vigore dello schema di decreto legislativo in commento, programmi formativi specifici in materia di alfabetizzazione e utilizzo dei sistemi di intelligenza artificiale previsti dal precedente comma 2, da collocare nell'ambito dei corsi di formazione manageriali disciplinati dall'articolo 16-quinquies del citato D.Lgs. n. 502 del 1992. In conclusione, al fine di consentire un esame più approfondito della materia si allega il provvedimento indicato in oggetto (All. n. 1).

Cordiali saluti

IL PRESIDENTE

Filippo Anelli

All.n.1

MF/CDL

Documento informatico firmato digitalmente ai sensi del D.Lgs. n. 445/2000 e del D.Lgs. 82/2005

FILIPPO

01.10.2026
14:44:29

FNOMCeO Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri

DECRETO LEGISLATIVO 9 settembre 2026, n. 160

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

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

Vigente al: 30-9-2026

Titolo I

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

Capo I

Disposizioni generali

IL PRESIDENTE DELLA REPUBBLICA

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

Vista la legge 23 agosto 1988, n. 400 recante «Disciplina dell'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 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;

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 responsabilit  amministrativa delle persone giuridiche, delle societ  e delle associazioni anche prive di personalit  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, nonch  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 autorit  competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonch  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 modalit  di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalit  di polizia, da organi, uffici e comandi di polizia»;

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

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

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

Acquisiti i pareri delle competenti Commissioni parlamentari della

Camera dei deputati e del Senato della Repubblica;

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

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

Emana
il seguente decreto legislativo:

Art. 1

Oggetto e finalita'

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

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

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

Art. 2

Definizioni

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

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

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

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

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

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

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

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

h) «dati operativi sensibili»: i dati relativi ad attivita' di prevenzione, accertamento, indagine o perseguimento di reati,

indicati dall'articolo 3, punto 38), del regolamento (UE) 2024/1689;

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

l) «scraping non mirato»: l'estrazione e la raccolta automatizzata e indiscriminata, su larga scala, mediante l'utilizzo di un sistema di intelligenza artificiale, di immagini facciali dalla rete internet o da filmati di telecamere a circuito chiuso, allo scopo di creare o ampliare banche dati di riconoscimento facciale;

m) «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;

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

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

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

q) «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, 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, e all'articolo 3 del regolamento (UE) 2024/1689.

Capo II

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

Art. 3

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

1. La ricerca, la sperimentazione, lo sviluppo, l'addestramento, l'adozione, l'applicazione, la convalida e l'utilizzo di sistemi e modelli di intelligenza artificiale per le 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, 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 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.

Art. 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, dell'articolo 64 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e della normativa di settore applicabile. I medesimi rapporti individuano altresì, nel rispetto del decreto legislativo n. 51 del 2018, i ruoli svolti dai soggetti coinvolti nel trattamento dei dati personali, specificando quando gli stessi operano quali titolari, contitolari o responsabili del trattamento e disciplinando i relativi obblighi e responsabilità, anche con riferimento alle misure di sicurezza e alla documentazione delle operazioni di trattamento. E' in ogni caso assicurata la titolarità in capo alle Forze di polizia dei modelli addestrati su dati operativi sensibili.

Art. 5

Sviluppo, realizzazione e prova di determinati sistemi di IA per 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, nonché del decreto legislativo 18 maggio 2018, n. 51, per il trattamento di dati personali, inclusi i dati relativi a reati e le categorie particolari di dati di cui all'articolo 3, punto 37), dello stesso regolamento IA, effettuato dalle Forze di polizia nell'ambito di spazi di sperimentazione normativa per l'intelligenza artificiale, quando tale trattamento 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, 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, 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.

Art. 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, 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, e al decreto legislativo 18 maggio 2018, n. 51;

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 prevenzione o di protezione e per il riconoscimento facciale a posteriori a fini di contrasto dei reati

Art. 7

Etichettatura, filtraggio e categorizzazione di dati biometrici nell'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, sono consentiti a condizione che:

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

b) siano funzionali ad 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, e 96, dello stesso regolamento, ed è svolto nel rispetto di quanto previsto dal decreto legislativo 18 maggio 2018, n. 51.

Art. 8

Sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale per 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 e' ammesso per le finalita' di prevenzione di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto ii), del regolamento IA. I sistemi di cui al primo periodo possono essere utilizzati, 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'articolo 5, paragrafo 1, primo comma, lettera h), punto i), del regolamento IA.

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

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

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

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

6. Nei casi d'urgenza, quando vi e' fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave e irreparabile per le

finalita' di cui al comma 1, l'utilizzo del sistema di IA puo' essere avviato, su disposizione del questore, dei comandanti o dei responsabili indicati al comma 4, dall'organo di polizia procedente, previa comunicazione, anche in forma orale, al procuratore della Repubblica, e a condizione che sia limitato a quanto strettamente necessario, in ogni caso con delimitazione dell'area interessata e indicazione delle persone ricercate.

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

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

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

Art. 9

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

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

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

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

4. Dopo l'utilizzo dei sistemi di cui al comma 1, il titolare del trattamento effettua notifica al Garante, in conformita' a quanto previsto dall'articolo 5, paragrafo 4, del regolamento IA. La notifica, effettuata previo nulla osta dell'autorita' giudiziaria competente che puo' differirlo per un periodo non superiore a tre mesi, rinnovabile per una sola volta, in presenza di specifiche esigenze di segretezza, contiene le informazioni essenziali sull'autorizzazione rilasciata e sul risultato conseguito con

l'utilizzo del sistema, e non include dati operativi sensibili. Nel caso di piu' attivazioni del sistema di IA per l'identificazione biometrica remota in tempo reale nello stesso contesto operativo ovvero di piu' utilizzi omogenei del predetto sistema, la notifica di cui al presente comma puo' essere effettuata in modo periodico e cumulativo, secondo i termini previsti dal decreto di cui al comma 5, ferma restando la necessita' del nulla osta preventivo dell'autorita' giudiziaria nei termini di cui al secondo periodo.

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

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

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

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

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

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

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

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

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

Art. 10

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

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

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

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

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

4. Sulla base dei criteri di cui al comma 12, lettera a), l'utilizzo dei sistemi di videosorveglianza previsti dal comma 1, nei casi ivi contemplati, comporta il trattamento automatizzato, delle immagini del volto delle persone che accedono a luoghi o a eventi per i quali sussistono particolari esigenze di ordine e sicurezza pubblica, senza elaborazione dei relativi dati biometrici. Le immagini sono memorizzate, a livello locale, nella base dati di riferimento di cui al comma 12, lettera b). Nella medesima base dati sono 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 e' il Ministero dell'interno - Dipartimento della pubblica sicurezza.

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

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

8. Gli accessi e le operazioni di trattamento sui sistemi di cui al presente articolo devono essere effettuati esclusivamente dalle

persone autorizzate e registrati automaticamente in appositi file di log, non modificabili, conformemente a quanto previsto dall'articolo 12, paragrafo 3, del regolamento IA. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili per finalita' di verifica della liceita' del trattamento, di controllo interno e nell'ambito di un procedimento penale.

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

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

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

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

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

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

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

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

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

14. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri per la finanza pubblica.

Titolo II

DISPOSIZIONI PENALI, SOSTANZIALI E PROCESSUALI, IN MATERIA DI REALIZZAZIONE E IMPIEGO ILLECITI DEI SISTEMI DI INTELLIGENZA ARTIFICIALE E DISPOSIZIONI PROCESSUALI CIVILI IN MATERIA DI RISARCIMENTO DEI DANNI CAGIONATI DALL'UTILIZZO DEI MEDESIMI SISTEMI

Capo I

Disposizioni sanzionatorie e in materia di procedimento penale

Art. 11

Definizioni

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

Art. 12

Modifiche al codice penale

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

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

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

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

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

Art. 13

Modifiche al codice di procedura penale

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

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

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

memorizzati in una banca dati di riferimento.

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

4. Con le stesse modalita' di cui ai commi 1, 2 e 3 puo' essere autorizzata la ricerca mirata, nell'ambito di un procedimento penale, di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani.

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

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

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

8. I risultati forniti dai sistemi di intelligenza artificiale

non possono essere utilizzati qualora gli stessi siano stati impiegati fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dai commi 6 e 7. In questi casi, tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato.».

Art. 14

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

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

Art. 15

Modifiche al decreto legislativo 8 giugno 2001, n. 231

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

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

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

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

Capo II

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

Art. 16

Ambito di applicazione e foro del consumatore

1. Le disposizioni di cui all'articolo 17 si applicano 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 piu' 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, e della normativa nazionale di recepimento della direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024.

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

Art. 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;

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

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

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

3. L'ordine di esibizione e' 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 proprieta' industriale, di cui al decreto legislativo 10 febbraio 2005, n. 30.

5. Se la parte, senza giustificato motivo, non adempie, anche parzialmente, all'ordine di esibizione, il giudice puo' desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile. 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.

Art. 18

Presunzione del nesso di causalita'

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

Art. 19

Rilevanza della conformita' al regolamento (UE) 2024/1689

1. Fermo quanto previsto dalla normativa nazionale di recepimento della direttiva (UE) 2024/2853, la conformita' 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, non esclude di per se' la responsabilita' del convenuto.

Art. 20

Azione diretta nei confronti dell'impresa di assicurazione

1. Chi intende promuovere l'azione di cui all'articolo 16 puo' chiedere preventivamente al soggetto a cui ritiene che sia imputabile

il danno se e' assistito da un contratto di assicurazione della responsabilita' civile relativo al danno medesimo. La richiesta di cui al primo periodo non costituisce condizione di procedibilita' della domanda. Il soggetto nei cui confronti e' formulata la richiesta comunica entro trenta giorni dalla sua ricezione, l'esistenza di un contratto di assicurazione della responsabilita' 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 puo' desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile.

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

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

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 e' litisconsorte necessario il soggetto individuato quale responsabile del danno.

6. L'azione diretta di cui al comma 2 e' 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

Art. 21

Disposizioni transitorie sull'utilizzo dei sistemi di intelligenza artificiale per l'attivita' 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 finalita' di polizia ovvero sono gia' in uso nell'attivita' 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 e' prevista direttamente ovvero dipende dal regolamento IA, si osservano i termini di entrata in vigore e di compiuta attuazione dello stesso regolamento.

Art. 22

Clausola di invarianza finanziaria

1. Le amministrazioni interessate provvedono alle attivita' 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.

Il presente decreto, munito del sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addi' 9 settembre 2026

MATTARELLA

Meloni, Presidente del Consiglio
dei ministri

Foti, Ministro per gli affari
europei, il PNRR e le politiche di
coesione

Piantedosi, Ministro dell'interno

Nordio, Ministro della giustizia

Tajani, Ministro degli affari
esteri e della cooperazione
internazionale

Crosetto, Ministro della difesa

Giorgetti, Ministro dell'economia e
delle finanze

Visto, il Guardasigilli: Nordio