



CONTRIBUTO SCRITTO

elementi di conoscenza e di valutazione

nell'ambito dell'esame dello **schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile**

da parte delle

Commissioni riunite I Affari costituzionali e II Giustizia della Camera dei deputati

Il decreto in oggetto, composto da **22 articoli**, è adottato ai sensi dell'articolo 24, comma 1, comma 2, lett. h), comma 3 e comma 5 della legge 23 settembre 2025, n. 132, per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689, del Parlamento europeo e del Consiglio, del 13 giugno 2024 ("Regolamento IA" o "AI Act").

Il testo è organizzato in **tre titoli**: il Titolo I, dedicato all'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia; il Titolo II, relativo alle disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale e alle disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi; il Titolo III, riguardante le disposizioni finali.

Il provvedimento muove dalla considerazione che l'intelligenza artificiale può **rafforzare la prevenzione e il contrasto dei fenomeni criminosi**, ma solo entro un **perimetro rigoroso** definito dal rispetto di determinate regole:

1) **Uso mirato e proporzionato dell'IA.** L'impiego dei sistemi di IA nell'attività di polizia è configurato dal decreto come uno strumento di supporto alle funzioni di prevenzione, accertamento e repressione dei reati, il cui utilizzo deve essere strettamente necessario rispetto alle finalità perseguite e conforme alla tutela dei diritti fondamentali e alle libertà previste dalla Costituzione. In tale prospettiva, il ricorso ai sistemi di IA non assume un carattere generalizzato, ma viene circoscritto a casi tassativi nei quali il ricorso alla menzionata tecnologia risulti effettivamente idoneo a migliorare l'efficacia dell'azione amministrativa e investigativa.

2) **Divieto di sorveglianza massiva.** Un principio cardine del provvedimento è rappresentato dall'esclusione di forme di sorveglianza indiscriminata della popolazione mediante sistemi di intelligenza artificiale. Il decreto si pone in linea con il Regolamento IA nel vietare pratiche suscettibili di determinare un monitoraggio generalizzato degli individui o una raccolta sistematica e non selettiva di dati biometrici o comportamentali. La disciplina mira così a prevenire utilizzi dell'IA che possano tradursi in forme di controllo pervasivo della collettività, assicurando che ogni attività di identificazione sia sempre ricondotta a presupposti normativi specifici e a finalità determinate.



3) **Autorizzazione giudiziaria per l'identificazione biometrica in tempo reale.** Il decreto conferma il carattere eccezionale del ricorso ai sistemi di identificazione biometrica remota in tempo reale, subordinandone l'utilizzo alla preventiva autorizzazione dell'autorità giudiziaria. Tale scelta risponde all'esigenza di assicurare un controllo preventivo indipendente sull'impiego di una tecnologia potenzialmente molto invasiva, garantendo che essa possa essere utilizzata esclusivamente nei casi previsti dalla legge.

4) **Costante revisione umana qualificata delle decisioni algoritmiche.** Il decreto ribadisce il principio secondo cui i sistemi di IA costituiscono strumenti di supporto alle attività delle autorità di pubblica sicurezza e non possono sostituire la valutazione e la responsabilità decisionale dell'operatore umano. Le decisioni che incidono sui diritti e sulle libertà delle persone devono pertanto essere sempre assunte o validate da personale adeguatamente formato, in grado di comprendere il funzionamento dei sistemi utilizzati, valutarne criticamente gli esiti, individuare eventuali anomalie o bias algoritmici e intervenire, ove necessario, modificando o disattendendo le indicazioni fornite dall'algoritmo. Il presidio umano rappresenta, pertanto, una garanzia essenziale di legalità, trasparenza e responsabilità nell'impiego dei sistemi di IA, coerentemente con il principio di supervisione umana consacrato anche dall'AI Act.

In questo senso, le linee direttrici sopra richiamate sono volte a garantire, complessivamente, la **sicurezza ma anche i diritti, escludendo la possibilità di un controllo generalizzato della popolazione** e favorendo esclusivamente l'utilizzo da parte delle Forze di polizia di **strumenti tecnologicamente avanzati, solo come supporto mirato all'azione umana che preserva la sua centralità.**

Come anticipato, sono previste **regole rigorose per l'identificazione biometrica in tempo reale**, il cui utilizzo è ammesso solo in casi eccezionali. Il ricorso a tali sistemi è consentito esclusivamente nei casi previsti dalla legge, subordinatamente alla preventiva autorizzazione dell'Autorità giudiziaria e per un arco temporale limitato.

Parallelamente, il decreto vieta la costituzione di banche dati biometriche alimentate mediante raccolte massive e indiscriminate di dati reperiti dal web o attraverso altre fonti.

Coerentemente con tale impostazione, il decreto attribuisce particolare rilievo alla formazione specialistica **degli operatori delle Forze di polizia** chiamati a utilizzare i sistemi di IA. La formazione rappresenta, pertanto, un elemento essenziale per assicurare un utilizzo consapevole, corretto e conforme ai principi di legalità, imparzialità e buon andamento dell'azione amministrativa, preservando la responsabilità decisionale dell'operatore umano.

Con riferimento, poi, alla **responsabilità penale (alterazione e omissioni di misure di sicurezza)**, il decreto prevede un **nuovo articolo nel Codice penale, il 437-bis** che sanziona l'omessa adozione delle misure di sicurezza nei sistemi di IA ad alto rischio e la loro alterazione illecita quando ne derivi un pericolo concreto per la vita, l'incolumità pubblica o la sicurezza dello Stato. Stabilisce, altresì, che la responsabilità può estendersi anche all'ente e che la punibilità è ancorata al pericolo concreto e, per la forma colposa, alla colpa grave.

Nel contesto su delineato volto a disciplinare i sistemi di IA impiegati per le attività di polizia, risultano di particolare interesse per l'Agenzia per la cybersicurezza nazionale **tre aspetti.**



Il **primo** è la previsione all'articolo 5 di una disciplina finalizzata ad assicurare che anche le Forze di polizia possano **avvalersi delle opportunità offerte dagli spazi di sperimentazione normativa** con riferimento allo sviluppo, alla realizzazione e alla prova dei **sistemi di IA**, in particolare ad alto rischio, **destinati** esattamente alle **attività di polizia**.

Giova ricordare che attraverso l'istituzione di tali spazi si intende provvedere alla **creazione di un ambiente controllato** di sperimentazione e prova dei sistemi di IA nella fase di sviluppo e pre-utilizzo al fine di garantirne la conformità al regolamento IA. **L'attività di sperimentazione**, nonostante sia endemicamente caratterizzata dalla possibilità di derogare temporaneamente a puntuali obblighi normativi, **deve** comunque svolgersi, anche quando finalizzata alle attività di polizia, **nel pieno rispetto delle condizioni cumulativamente previste dall'articolo 59, par. 1, del regolamento IA, e, più ampiamente, dei diritti fondamentali e della normativa multilivello in materia di protezione dei dati personali**.

Tanto premesso, la disposizione assicura, altresì, il **raccordo tra le Forze di polizia e l'ACN e l'AgID**, in qualità di Autorità nazionali per l'intelligenza artificiale co-mandatari per quanto attiene all'**istituzione e alla gestione congiunta di spazi di sperimentazione normativa**, ai sensi dell'articolo 20, comma 1, lett. c), della legge n. 132/2025. In tal senso, si rinvia a un **regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'Interno**, la definizione delle **modalità di coordinamento** tra lo spazio di sperimentazione nazionale istituito ai sensi dell'art. 57 del regolamento IA e la sperimentazione relativa alle attività di polizia.

Il coordinamento risulta fondamentale, oltre che per garantire una **coerenza o omogeneità delle attività sperimentali** svolte dalla diverse amministrazioni in relazione ai rispettivi ambiti di competenza, a consentire alle Autorità nazionali per l'intelligenza artificiale di **far convergere i risultati di tutte le sperimentazioni** all'interno della **relazione annuale** che dovrà essere trasmessa all'**ufficio europeo per l'IA** a decorrere dall'anno successivo all'istituzione dello spazio di sperimentazione nazionale, conformemente a quanto previsto dall'articolo 57, par. 16, del regolamento IA, e dall'**articolo 31** del decreto delegato in materia di poteri delle autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione (AG n. 421).

Il **secondo** profilo di più diretto interesse di questa Agenzia è la previsione all'articolo 9 del citato provvedimento di un **decreto del Ministro dell'Interno** adottato di concerto con i Ministri della giustizia, della difesa e dell'economia e delle finanze, **sentiti** il Garante per la Protezione dei Dati Personali e le **Autorità nazionali per l'IA**, quindi anche l'ACN, volto a stabilire specifiche disposizioni **sull'impiego dei sistemi di IA ad alto rischio 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, nonché per la **ricerca** di una persona scomparsa o persone specifiche, vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale, come previsto dall'articolo 8 del decreto in oggetto.

Tra i diversi aspetti che saranno disciplinati all'interno del menzionato DPCM, il coinvolgimento di ACN risulta particolarmente necessario in relazione alla **definizione dei requisiti tecnici minimi di affidabilità e accuratezza** di tali sistemi di IA, potendo valorizzare il know-how che sarà acquisito da questa Agenzia in qualità di **autorità generale di vigilanza del mercato** ai sensi dell'art. 70 del



regolamento IA. Ciò avverrà, conformemente al **quadro di governance nazionale** delineato dall'articolo 5 del già citato decreto delegato in materia di poteri delle Autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione, in raccordo con il **Garante per la Protezione dei Dati Personali** in qualità di autorità di vigilanza del mercato competente sulla **specificità verticalità** rappresentata dai sistemi di IA ad alto rischio impiegati nelle **attività di contrasto**, gestione delle frontiere, giustizia e democrazia, ai sensi dell'articolo 74, paragrafo 8, del citato regolamento europeo.

Il **terzo** aspetto concerne la **formazione del personale di polizia**, che rappresenta la **precondizione** per l'utilizzo corretto e consapevole dei sistemi di IA nell'espletamento delle attività sopra menzionate. L'articolo 6 del decreto in oggetto include espressamente tra i **risultati formativi minimi** da conseguire la **consapevolezza dei rischi di cybersicurezza connessi all'utilizzo dei sistemi di IA**, anche con riferimento alle **indicazioni dell'ACN**. La disposizione assume particolare rilievo poiché conferma la **cybersicurezza dei sistemi di intelligenza artificiale quale presupposto essenziale** per il loro impiego affidabile, come previsto dall'articolo 3, comma 6, della legge n. 132/2025. Ciò assume una **rilevanza rafforzata in contesti particolarmente sensibili come quello delle attività di polizia**, nei quali eventuali vulnerabilità informatiche, alterazioni dei dati, attacchi ostili o compromissioni degli algoritmi potrebbero incidere direttamente sull'efficacia dell'azione investigativa e sulla tutela dei diritti fondamentali. Tale previsione risulta coerente con il ruolo attribuito all'ACN dall'articolo 20, comma 1, lettera b), della legge n. 132/2025, che affida alla citata Agenzia il compito di **promuovere lo sviluppo dell'IA relativamente ai profili di cybersicurezza**.