

- **CAMERA DEI DEPUTATI**

COMMISSIONI RIUNITE

**I AFFARI COSTITUZIONALI, DELLA PRESIDENZA DEL CONSIGLIO E INTERNI
II GIUSTIZIA**

CONTRIBUTO SCRITTO

sullo schema di decreto legislativo recante adeguamento della normativa nazionale al regolamento (UE) 2024/1689 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile

(Atto del Governo n. 418)

Commissaria Agcom Prof.ssa Elisa Giomi

24 luglio 2026

Indice

1. Oggetto, metodo e valutazione complessiva
2. Sintesi delle condizioni e osservazioni prioritarie
3. Qualità normativa, funzione di supporto e controllo umano (articoli 1-3)
4. Ricerca, collaborazioni e spazi di sperimentazione (articoli 4-5)
5. Formazione obbligatoria e bias prodotti dall'interazione umana (articolo 6)
6. Etichettatura e categorizzazione biometrica (articolo 7)
7. Identificazione biometrica remota in tempo reale (articoli 8-9)
8. Disciplina penale e responsabilità degli enti (articoli 11-15)
9. Tutela processuale civile e responsabilità risarcitoria (articoli 16-20)
10. Governance, regime transitorio e sostenibilità finanziaria (articoli 21-22)
11. Proposta conclusiva di condizioni e osservazioni per il parere
12. Riferimenti normativi e documentali

1. Oggetto, metodo e valutazione complessiva

Il presente contributo esamina lo schema di decreto legislativo di cui all'Atto del Governo n. 418, con particolare attenzione ai profili che incidono sulla qualità della normazione, sui diritti fondamentali, sull'effettività del controllo umano, sull'impiego di sistemi biometrici nell'attività di polizia, sulla determinatezza delle nuove fattispecie penali e sull'accesso alle prove nelle controversie civili. L'analisi assume come parametro il regolamento (UE) 2024/1689 (AI Act), la direttiva (UE) 2016/680, la legge di delegazione 23 settembre 2025, n. 132, la Carta dei diritti fondamentali dell'Unione europea, la Costituzione e la Convenzione europea dei diritti dell'uomo. Sono stati inoltre considerati i contributi già pubblicati nella documentazione delle Commissioni e gli orientamenti delle autorità europee e nazionali competenti.

La valutazione complessiva è favorevole all'obiettivo di costruire un quadro nazionale organico. Lo schema coglie correttamente alcuni snodi essenziali come la funzione meramente strumentale dell'intelligenza artificiale rispetto alla decisione umana, la necessità di una revisione qualificata e tracciabile, la formazione del personale, l'attenzione all'intero ciclo di vita dei sistemi, la registrazione delle operazioni, l'adeguamento dei sistemi già in uso, l'accesso alle prove e la previsione di una presunzione relativa del nesso causale. Questi elementi meritano di essere preservati e resi più esigibili.

I principali punti di attenzione non consistono nella mancanza di principi, bensì nel rapporto non sempre risolto tra principi generali, disposizioni direttamente applicabili dell'AI Act, rinvii alla normativa sulla protezione dei dati e regole nazionali effettivamente innovative. In diversi passaggi lo schema ripete obblighi già vigenti, mentre in altri affida a decreti ministeriali profili che concorrono a determinare l'intensità della sorveglianza, l'affidabilità minima richiesta e le concrete condizioni di esercizio di poteri capaci di incidere su libertà costituzionali. Il risultato rischia di essere, al tempo stesso, ridondante nelle clausole generali e incompleto nei presupposti sostanziali più delicati.

Il criterio guida dovrebbe essere maggiormente marcato. La fonte primaria dovrebbe definire finalità, casi, soggetti, limiti temporali, geografici e personali, condizioni di autorizzazione, conseguenze dell'uso illegittimo, garanzie difensive e criteri essenziali di affidabilità, mentre la fonte secondaria può aggiornare metriche, procedure tecniche e standard di prova, purché entro criteri legislativi sufficientemente determinati e con il coinvolgimento del Garante per la protezione dei dati personali e delle autorità nazionali per l'intelligenza artificiale.

Occorre inoltre distinguere tra rinvii meramente ricognitivi e rinvii con funzione di coordinamento. I primi possono essere soppressi per ridurre l'opacità normativa. I secondi vanno mantenuti quando chiariscono il regime applicabile o introducono una garanzia concreta. In particolare, non sarebbe opportuno eliminare le clausole che vietano il riutilizzo commerciale dei dati operativi o le banche biometriche alimentate mediante scraping non mirato: pur richiamando principi già desumibili dal diritto dell'Unione, esse hanno funzione di certezza applicativa. Potrebbero, semmai, essere rese più precise.

2. Sintesi delle condizioni e osservazioni prioritarie

Le proposte che seguono sono formulate in modo da poter essere tradotte, con minimi adattamenti, in condizioni o osservazioni del parere parlamentare.

1. **Sopprimere le clausole “senza nuovi obblighi” e nel rispetto delle varie normative vigenti citate.** Eliminare l'articolo 1, comma 3, e l'articolo 3, comma 7, o chiarire che essi escludono soltanto duplicazioni degli obblighi europei, senza comprimere le garanzie nazionali, gli obblighi procedurali e i requisiti organizzativi introdotti dal decreto. Eliminare dallo schema di decreto le varie clausole distribuite nel testo che richiamano in modo ultroneo il rispetto di norme vigenti.
2. **Rendere effettivo il controllo umano.** Definire la revisione umana come controllo sostanziale, svolto da personale competente, dotato dell'autorità e degli strumenti per comprendere, contestare, interrompere o disattendere l'output e tenuto a documentare la motivazione della decisione.
3. **Formazione obbligatoria prima dell'uso.** Consentire l'accesso ai sistemi soltanto a personale che abbia superato una formazione generale e specifica, aggiornata periodicamente e dopo ogni modifica sostanziale del sistema; includere i bias derivanti dalla selezione degli input, dalla formulazione delle interrogazioni, dall'automation bias e dal confirmation bias.
4. **Registro nazionale e monitoraggio indipendente.** Istituire un registro riservato dei sistemi di IA utilizzati dalle Forze di polizia, con inventario, versione, finalità, base giuridica, valutazioni d'impatto, dati di accuratezza, falsi positivi, incidenti e tassi di override umano; prevedere una relazione annuale al Parlamento in forma aggregata.
5. **Restringere l'articolo 7.** Sopprimere l'espressione “ovvero ad ulteriori attività” e tipizzare le sole operazioni tecniche ammesse, escludendo qualsiasi inferenza di caratteristiche sensibili e qualsiasi uso esplorativo non collegato a una finalità investigativa determinata.
6. **Definire nel decreto le garanzie essenziali.** Stabilire direttamente nel decreto i criteri minimi per validazione indipendente, soglie di errore, monitoraggio dei falsi positivi, delimitazione di aree e durata, composizione delle liste di controllo, esclusione di usi indiscriminati e protezione delle riunioni pacifiche.
7. **Evitare che l'output diventi prova autosufficiente.** Stabilire chiaramente che i risultati biometrici e gli altri output di IA sono elementi investigativi da verificare con fonti indipendenti.
8. **Garantire accesso effettivo alle prove.** Integrare l'articolo 17 con ordini di conservazione, categorie documentali ulteriori, accesso ai difensori e consulenti tecnici in regime di riservatezza e una regola secondo cui il segreto commerciale è recessivo rispetto allo svolgimento delle indagini delle forze dell'ordine e all'esercizio del diritto di difesa.
9. **Correggere la presunzione causale.** La norma afferma che la presunzione opera “quando il danno deriva” dalla violazione dell'AI act. Questa formulazione potrebbe essere circolare proprio perché la derivazione è ciò che dovrebbe essere presunto. Forse una formulazione più chiara potrebbe prevedere che quando la violazione di uno o più obblighi del regolamento (UE) 2024/1689 è astrattamente idonea a causare il danno, il nesso di causalità tra la violazione e il danno è presunto, salvo prova contraria.
10. **Condizionare l'operatività alle risorse e all'adeguamento.** È improbabile che si possa attuare efficacemente il presente dispositivo normativo senza lo stanziamento di risorse finanziarie adeguate. In ogni modo, ferma la clausola di invarianza imposta dalla delega, prevedere un piano attuativo entro novanta giorni, la priorità per sistemi biometrici ad alto rischio e il divieto di uso operativo in assenza di formazione, logging, validazione e valutazioni d'impatto.

3. Qualità normativa, funzione di supporto e controllo umano (articoli 1-3)

Clausole generali e rinvii normativi

L'articolo 1, comma 2, e l'articolo 3, comma 1, richiamano diritti fondamentali, proporzionalità, non discriminazione, sorveglianza umana e approccio antropocentrico. Tali richiami hanno una funzione orientativa, ma non sostituiscono presupposti e conseguenze giuridiche specifici. Una disposizione programmatica è utile quando guida l'interpretazione di regole determinate, mentre diventa ridondante quando è affiancata da formule che sembrano neutralizzare la portata innovativa del decreto.

In particolare, l'articolo 1, comma 3, afferma che il titolo non comporta nuovi obblighi rispetto all'AI Act, e l'articolo 3, comma 7, ripete che le attività sono effettuate senza nuovi o ulteriori obblighi. Le formule sono difficili da conciliare con il contenuto dello stesso schema, che introduce corsi di formazione, procedure autorizzative, log quinquennali, notifiche, basi giuridiche, regole di inutilizzabilità e nuove responsabilità. L'AI Act, inoltre, lascia espressamente agli Stati membri la decisione se autorizzare taluni usi biometrici e la disciplina delle relative condizioni e procedure.

Proposta: sopprimere l'articolo 1, comma 3, e l'articolo 3, comma 7. In subordine, sostituirli con la seguente clausola: "Le disposizioni del presente titolo specificano, nell'ambito dei margini riconosciuti dal diritto dell'Unione, le condizioni, le garanzie procedurali e gli obblighi organizzativi applicabili alle Forze di polizia, senza duplicare gli adempimenti direttamente disciplinati dal regolamento IA".

Il richiamo al decreto legislativo n. 51 del 2018 non è invece sempre superfluo. Per i trattamenti svolti dalle autorità competenti a fini di prevenzione e repressione dei reati, la direttiva (UE) 2016/680 e il relativo decreto di recepimento costituiscono il quadro generale di liceità, necessità, proporzionalità, sicurezza e valutazione d'impatto. Il testo può essere alleggerito evitando ripetizioni.

Controllo umano significativo e non rituale

L'articolo 3, comma 4, valorizza la revisione umana qualificata prima dell'impiego dell'output in atti e provvedimenti incidenti sulla sfera giuridica degli interessati. È uno dei punti migliori dello schema, ma la formula "adequate forme di revisione" lascia aperta la possibilità di un controllo meramente formale. L'articolo 14 dell'AI Act richiede che la persona incaricata comprenda capacità e limiti del sistema, sia consapevole della tendenza ad affidarsi automaticamente all'output, possa interpretarlo correttamente e abbia il potere di non usarlo o di interrompere il sistema.

La tutela dovrebbe inoltre coprire non soltanto gli "atti e provvedimenti" formalmente qualificati, ma ogni operazione capace di orientare significativamente un'indagine o una misura: selezione di persone da controllare, assegnazione di priorità, produzione di una lista di candidati, valutazioni di rischio, segnalazioni operative e richieste all'autorità giudiziaria.

Testo suggerito: "La revisione umana è effettiva quando il personale incaricato dispone delle competenze, delle informazioni tecniche e dei poteri necessari per comprendere i limiti del sistema, verificare la pertinenza degli input e della banca dati di riferimento, valutare il margine di errore, disattendere o interrompere l'elaborazione e motivare l'eventuale utilizzazione dell'output. La revisione non può limitarsi alla conferma formale del risultato automatico ed è documentata nei log".

È opportuno aggiungere che l'output non può essere l'unico o il fattore determinante di una decisione sfavorevole. L'articolo 10, comma 9, contiene già una regola analoga per il

riconoscimento facciale; una clausola generale eviterebbe che la garanzia dipenda dalla tecnologia utilizzata.

4. Ricerca, collaborazioni e spazi di sperimentazione (articoli 4-5)

Collaborazioni con soggetti pubblici e privati

L'articolo 4 consente collaborazioni con università, enti di ricerca e soggetti pubblici o privati. La previsione è necessaria perché molte Forze di polizia non dispongono internamente di tutte le competenze tecniche richieste. Tuttavia, la collaborazione crea rischi di dipendenza dal fornitore, accesso a dati operativi, riuso di modelli addestrati su dati pubblici, opacità della catena di subfornitura e difficoltà di audit.

Il comma 2, pur formulato attraverso richiami alla normativa sulla protezione dei dati, non è meramente ridondante: il divieto di condivisione dei dati operativi sensibili e di utilizzazione commerciale dei risultati risponde a un'esigenza sostanziale. La clausola dovrebbe essere rafforzata con obblighi contrattuali minimi.

Integrazioni suggerite: prevedere: a) divieto di riutilizzo dei dati, dei modelli derivati, delle rappresentazioni vettoriali e delle conoscenze ricavate per finalità diverse; b) divieto di addestramento ulteriore di modelli commerciali; c) obbligo di cancellazione o restituzione verificabile; d) tracciamento degli accessi e dei subfornitori; e) diritto delle amministrazioni a svolgere audit tecnici e di sicurezza; f) disponibilità della documentazione necessaria a verificare prestazioni, errori e modifiche di versione; g) portabilità e continuità operativa per evitare il lock-in; h) divieto di accesso remoto del fornitore ai dati operativi, salvo interventi eccezionali, autorizzati e integralmente registrati.

La titolarità pubblica dei modelli addestrati su dati operativi sensibili, prevista dal comma 3, è positiva ma non sufficiente. La proprietà formale non garantisce la controllabilità se l'amministrazione non dispone di documentazione, strumenti di audit, chiavi, ambienti di esecuzione e diritti di manutenzione.

5. Formazione obbligatoria e bias prodotti dall'interazione umana (articolo 6)

L'articolo 6 è uno degli elementi più concreti dello schema. L'alfabetizzazione in materia di IA non può tuttavia ridursi all'offerta di corsi ma deve diventare un requisito di abilitazione all'uso. L'articolo 4 dell'AI Act impone a fornitori e deployer di adottare misure per assicurare un livello sufficiente di alfabetizzazione del personale, tenendo conto delle conoscenze tecniche, dell'esperienza, dell'istruzione, della formazione e del contesto d'uso. Per sistemi utilizzati nella coercizione pubblica, la verifica delle competenze dovrebbe essere documentata.

Il testo considera i bias e gli errori dei sistemi, ma non esplicita i bias prodotti dall'interazione dell'operatore. Si tratta di un profilo distinto: selezione incompleta o orientata degli input; formulazione suggestiva delle interrogazioni; scelta della soglia dopo aver visto i risultati; uso di immagini di qualità inadeguata; confirmation bias; automation bias; interpretazione del primo candidato come identificazione certa; mancata considerazione delle condizioni demografiche e ambientali; reiterazione di interrogazioni fino a ottenere un risultato conforme all'ipotesi investigativa.

La letteratura tecnica dimostra che i tassi di falso positivo e falso negativo dipendono dall'algoritmo, dalla qualità delle immagini, dalla soglia, dalla dimensione e composizione della banca di confronto e dal gruppo demografico. Le valutazioni NIST sottolineano che i falsi positivi possono variare tra gruppi e sistemi e che il contesto operativo è decisivo.

Testo suggerito: “L’accesso e l’utilizzo dei sistemi di IA sono consentiti esclusivamente al personale che abbia completato con esito positivo un percorso formativo generale e specifico per il sistema e la funzione esercitata. La formazione è aggiornata almeno annualmente e in occasione di modifiche sostanziali del sistema, dei dati, delle soglie o delle finalità. Essa comprende, oltre ai bias dei dati e del modello, i rischi derivanti dalla selezione e qualità degli input, dalla formulazione delle interrogazioni, dal confirmation bias, dall’automation bias, dall’interpretazione dei punteggi e dall’uso reiterato o esplorativo del sistema”.

La formazione dovrebbe riguardare tutti gli utilizzatori, anche occasionali, nonché i responsabili che autorizzano o valutano l’impiego, il personale addetto agli acquisti e alla validazione e coloro che effettuano la revisione umana. Per i sistemi ad alto rischio, l’abilitazione dovrebbe essere revocabile e subordinata a esercitazioni periodiche su falsi positivi, arresto del sistema.

6. Etichettatura e categorizzazione biometrica (articolo 7)

L’articolo 7 intende delimitare l’eccezione al divieto di categorizzazione biometrica previsto dall’articolo 5, paragrafo 1, lettera g), dell’AI Act. È corretta la previsione che le attività non siano finalizzate a inferire caratteristiche sensibili e che non costituiscano l’unico fondamento di decisioni con effetti giuridici. È invece troppo ampia la lettera b), nella parte in cui consente “ulteriori attività” purché conformi alla normativa vigente e perseguano finalità di polizia.

Una clausola aperta è particolarmente rischiosa in una disposizione che delimita una pratica vietata. La legalità dell’acquisizione iniziale del dato non rende automaticamente proporzionata ogni successiva operazione di etichettatura, filtraggio o categorizzazione.

Proposta: sostituire la lettera b) con un elenco chiuso: “siano necessarie alla verifica della qualità tecnica del dato, alla deduplicazione, alla comparazione con dati riferiti a persone specificamente ricercate o alla ricerca mirata nell’ambito di un’attività di polizia determinata e documentata”. Eliminare l’espressione generica “ovvero ad ulteriori attività”.

È opportuno aggiungere il divieto di utilizzare proxy o combinazioni di caratteristiche per inferire indirettamente razza, origine etnica, opinioni politiche, appartenenza sindacale, convinzioni religiose, vita sessuale, orientamento sessuale o altre categorie protette.

7. Identificazione biometrica remota in tempo reale (articoli 8-9)

I casi ammessi dovrebbero essere riprodotti in modo tassativo

L’AI Act vieta in via generale l’identificazione biometrica remota “in tempo reale” in spazi accessibili al pubblico a fini di attività di contrasto, ammettendo eccezioni tassative: ricerca mirata di determinate vittime o persone scomparse; prevenzione di una minaccia specifica, sostanziale e imminente alla vita o all’incolumità fisica, o di una minaccia reale e attuale o reale e prevedibile di attacco terroristico; localizzazione o identificazione di sospettati di specifici reati. L’uso deve servire soltanto a confermare l’identità della persona specificamente interessata ed essere limitato nel tempo, nello spazio e nella portata personale.

L’articolo 8, comma 1, rinvia alle disposizioni europee, ma la formula “per le finalità di prevenzione” non rende immediatamente percepibile il carattere eccezionale della misura. Poiché il decreto costituisce la base nazionale che rende possibile un impiego altrimenti vietato, i casi devono essere riportati per esteso e non ampliati mediante concetti generali di ordine o sicurezza pubblica.

Proposta: riprodurre nell'articolo 8 i presupposti dell'articolo 5 dell'AI Act e aggiungere che la mera prevenzione generale, il controllo di aree considerate sensibili, la gestione ordinaria dell'ordine pubblico e la partecipazione a manifestazioni non costituiscono presupposti autonomi.

Banche dati di riferimento e persone non interessate

Il comma 3 vieta banche alimentate mediante scraping non mirato. La previsione non dovrebbe essere soppressa come meramente ultronea: rende operativa, nel contesto nazionale, una delle pratiche vietate dall'AI Act e facilita il controllo sulla provenienza dei dati. Deve essere integrata con requisiti di chiusura e qualità della watchlist.

Integrazione: la banca di riferimento deve contenere soltanto i dati della persona o delle persone indicate nell'autorizzazione; per ciascun dato devono essere registrati fonte, data, qualità, base giuridica e verifica di attualità; non sono consentite liste esplorative, categorie di persone o banche generaliste. I dati biometrici delle persone non corrispondenti devono essere eliminati immediatamente e non possono alimentare ulteriori archivi.

Libertà di riunione, espressione e partecipazione politica

Il considerando 32 dell'AI Act riconosce che la sorveglianza biometrica in tempo reale può generare una sensazione di controllo costante e dissuadere l'esercizio della libertà di riunione e di altri diritti fondamentali. La Corte europea dei diritti dell'uomo, nel caso *Glukhin c. Russia*, ha ravvisato la violazione degli articoli 8 e 10 CEDU nell'impiego della tecnologia di riconoscimento facciale contro un partecipante a una manifestazione pacifica.

La legge nazionale dovrebbe impedire che il luogo o il contesto di una manifestazione divengano, da soli, il motivo dell'attivazione. Qualora una persona specificamente ricercata possa trovarsi in un evento protetto dalle libertà politiche, sindacali, religiose o associative, occorrono motivazione rafforzata, delimitazione tecnica che escluda l'identificazione dei partecipanti e relazione successiva al Garante.

Clausola suggerita: "La partecipazione, l'organizzazione o la presenza in riunioni, manifestazioni, iniziative politiche, sindacali, religiose o associative non possono costituire, da sole o prevalentemente, presupposto dell'attivazione, criterio di inclusione nella banca di riferimento o informazione utilizzabile per finalità ulteriori".

Accuratezza, falsi positivi e validazione indipendente

Il comma 5 rinvia a un decreto ministeriale i requisiti minimi di affidabilità e accuratezza. È corretto non cristallizzare nella legge numeri destinati a diventare rapidamente obsoleti; tuttavia la fonte primaria deve indicare le metriche e le condizioni essenziali. "Accuratezza" non è un valore unico. Per il riconoscimento facciale devono essere considerate almeno: false match rate, false non-match rate, soglia operativa, qualità delle immagini, condizioni di luce e angolazione, tempo trascorso, prestazioni per gruppi demografici, tasso di candidati multipli e tasso di override umano.

Principio legislativo suggerito: "Il sistema non può essere impiegato operativamente se non è stato validato da un soggetto indipendente dal fornitore e dall'unità utilizzatrice, in condizioni rappresentative dello specifico contesto d'uso, e se non sono stabilite soglie di errore compatibili con la gravità delle conseguenze. Il decreto attuativo definisce metriche e valori, il metodo di prova, la frequenza dei test e i criteri di sospensione; i risultati sono comunicati al Garante e alle autorità nazionali per l'IA".

Il monitoraggio deve misurare i falsi positivi reali e non soltanto le prestazioni di laboratorio. È opportuno registrare quante segnalazioni siano state confermate, scartate, contestate o abbiano

determinato controlli su persone estranee, con disaggregazione adeguata e senza creare nuovi rischi di **discriminazione**.

8. Disciplina penale e responsabilità degli enti (articoli 11-15)

Utilizzo processuale degli output biometrici

Clausola generale suggerita: “Il risultato di un sistema di IA costituisce elemento investigativo da verificare mediante fonti indipendenti. Non può costituire l’unico o determinante fondamento di una misura limitativa, di una richiesta cautelare, di un’imputazione o di una decisione sulla responsabilità. L’autorità procedente documenta la verifica effettuata e rende disponibili alla difesa, quando cessano le esigenze di segretezza, autorizzazione, log, versione del sistema, soglia, banca di riferimento e documentazione sulle prestazioni pertinenti”.

L’accesso difensivo non richiede necessariamente la pubblicazione integrale del codice sorgente. Può essere assicurato mediante ostensione mirata, accesso a consulenti vincolati alla riservatezza, test indipendenti e documentazione tecnica sufficiente a contestare errore, soglia, database e funzionamento. Il segreto commerciale non può limitare l’accesso alle informazioni e rendere l’output incontestabile.

9. Tutela processuale civile e responsabilità risarcitoria (articoli 16-20)

Accesso e conservazione delle prove

L’articolo 17 risponde a una reale asimmetria informativa: il danneggiato spesso non conosce il sistema utilizzato, la versione, i dati, i log, le soglie e l’intervento umano. È positiva la possibilità di ordinare l’esibizione sulla base di fatti che rendano verosimile la domanda e la previsione di conseguenze probatorie per l’inadempimento.

La disciplina dovrebbe contemplare espressamente la conservazione preventiva delle prove. Log e versioni possono essere sovrascritti, i sistemi aggiornati e le configurazioni mutate. Il giudice deve poter ordinare, anche prima dell’esibizione, il congelamento della versione, dei log, dei parametri, dei dati pertinenti e della documentazione di post-market monitoring.

Osservazione proposta: In qualsiasi momento, il giudice dovrebbe poter ordinare la conservazione degli elementi di prova, della versione del sistema e dell’ambiente necessario alla loro verifica, con misure proporzionate e successivo contraddittorio.

L’elenco del comma 2 dovrebbe comprendere anche: istruzioni d’uso; dichiarazione di conformità; registrazione nella banca dati europea o nazionale; versione e cronologia delle modifiche; dati di validazione pertinenti; incidenti e reclami; output completo e punteggi; input; criteri di selezione della banca; interventi umani; contratti e ripartizione delle responsabilità; audit e monitoraggio successivo all’immissione sul mercato.

La richiesta non dovrebbe essere respinta perché l’attore non è in grado di nominare un documento del quale ignora l’esistenza. È sufficiente una descrizione per categorie, purché collegata al sistema e al danno. Spetta al giudice delimitare l’ordine secondo necessità e proporzionalità.

Segreti commerciali e diritto di difesa

Il comma 4 tutela i segreti commerciali mediante le misure dell’articolo 121-ter del codice della proprietà industriale. La tutela è necessaria, ma non può trasformarsi in un diniego sostanziale

della prova. Il principio corretto deve prevedere la prevalenza delle esigenze investigative e difensive sui segreti industriali e commerciali, lasciando al giudice l'onere di garantire comunque un accesso effettivo e lì dove necessario misure di riservatezza meno restrittive della totale sottrazione.

Clausola suggerita: “L'esistenza di un segreto commerciale o di altra informazione riservata non può, da sola, giustificare il diniego degli elementi necessari all'effettivo esercizio del diritto di azione e di difesa. Il giudice assicura l'accesso almeno ai difensori e ai consulenti tecnici vincolati alla riservatezza, può disporre udienze riservate, versioni oscurate e ambienti sicuri e limita la divulgazione a quanto strettamente necessario”.

Presunzione del nesso causale

L'articolo 18 dispone che, “quando il danno deriva” dalla violazione di obblighi dell'AI Act, il nesso di causalità tra violazione e danno è presunto. La formulazione è circolare: per accedere alla presunzione sembrerebbe necessario dimostrare proprio la derivazione che la norma intende presumere.

La soluzione non dovrebbe tuttavia fondarsi sulla mera “astratta idoneità”, che rischia di attivare la presunzione per ogni violazione formalmente collegabile. È preferibile una soglia di ragionevole probabilità, coerente con il tipo di obbligo e con il danno verificatosi.

Riformulazione proposta: “Quando l'attore prova la violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689, il nesso di causalità tra danno e violazione è presunto, salvo prova contraria”.

Si potrebbe sostenere che chiunque cagiona un danno mediante l'impiego di un sistema di intelligenza artificiale è tenuto al risarcimento quando il danneggiato provi la violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689, specificamente diretti a prevenire il rischio concretizzatosi. In tali casi, il nesso di causalità tra la violazione e il danno evento si presume, salvo che l'operatore provi di avere adottato tutte le misure idonee a evitare il danno ovvero che il danno sia derivato da causa a lui non imputabile.

Si potrebbe anche aggiungere che la presunzione non opera quando il convenuto rende disponibili tempestivamente elementi sufficienti a ricostruire il funzionamento e dimostra che la violazione non ha avuto influenza causale. Viceversa, la mancata conservazione o esibizione dei log rafforza la presunzione.

10. Governance, regime transitorio e sostenibilità finanziaria (articoli 21-22)

Un inventario nazionale dei sistemi

Lo schema distribuisce competenze tra Forze di polizia, Ministero dell'interno, autorità giudiziaria, Garante, AgID e ACN, ma non prevede un inventario unitario dei sistemi utilizzati né un meccanismo nazionale per confrontare prestazioni, falsi positivi, incidenti e pratiche operative. Le registrazioni europee possono essere soggette a limitazioni per finalità di contrasto e non sostituiscono un registro nazionale riservato utile alla responsabilità amministrativa e al controllo parlamentare.

Proposta: istituire presso un soggetto pubblico già esistente un registro nazionale riservato dei sistemi di IA utilizzati nelle attività di polizia. Per ciascun sistema: amministrazione, finalità, base giuridica, fornitore, versione, classificazione, stato operativo, dati trattati, valutazioni d'impatto, validazione, soglie, incidenti, falsi positivi, reclami, audit, data di sospensione o dismissione. Il Garante, AgID e ACN accedono per le rispettive competenze.

Il Ministero dell'interno dovrebbe produrre annualmente una relazione pubblica aggregata sul numero e sulle categorie di sistemi, sugli usi biometrici, sugli esiti, sui falsi positivi, sulle sospensioni, sulle violazioni e sulla formazione. Le informazioni operative sensibili possono essere contenute in un allegato riservato. L'AI Act già valorizza la rendicontazione annuale degli usi di identificazione biometrica in tempo reale.

Clausola di invarianza finanziaria

La clausola di invarianza è coerente con l'articolo 24, comma 6, della legge delega. Ciò non rende però irrilevante la sostenibilità. Formazione specialistica, validazione indipendente, log non modificabili, monitoraggio dei bias, registri, notifiche, audit e gestione degli incidenti richiedono personale e infrastrutture.

Il rischio concreto è che gli obblighi restino nominali o che le risorse siano sottratte ad altre funzioni operative. Il decreto dovrebbe imporre una programmazione attuativa e affermare che nessun sistema può essere messo o mantenuto in esercizio se l'amministrazione non dispone delle risorse minime per rispettare le garanzie.

Osservazione suggerita: richiedere al Governo una relazione su costi, personale formato, sistemi inventariati, infrastrutture di logging, validazioni e criticità, con indicazione delle risorse già disponibili e delle priorità. In assenza dei presupposti organizzativi, l'attivazione dovrebbe essere rinviata.

11. Proposta conclusiva di condizioni e osservazioni per il parere

Alla luce delle considerazioni svolte, si propone di esprimere un parere parlamentare favorevole tenendo conto delle seguenti osservazioni.

Osservazioni

1. Sopprimere o riformulare l'articolo 1, comma 3, e l'articolo 3, comma 7, in modo da non neutralizzare gli obblighi organizzativi e le garanzie nazionali introdotte dal decreto.
2. Integrare l'articolo 3 con una definizione di controllo umano significativo, con il divieto di controllo meramente formale e con una regola generale secondo cui l'output dei sistemi di intelligenza artificiale non può costituire l'unico o determinante fondamento di decisioni sfavorevoli.
3. Rendere obbligatoria, verificata e periodica la formazione di ogni persona autorizzata a usare, supervisionare, acquistare o validare sistemi di IA, includendo bias di input, interrogazione, conferma e automazione.
4. Eliminare dall'articolo 7 la clausola aperta relativa a "ulteriori attività" e sostituirla con un elenco chiuso di operazioni tecniche strettamente necessarie.
5. Per l'articolo 8, riprodurre i casi tassativi dell'articolo 5 dell'AI Act, restringere durata e area, documentare l'urgenza e proteggere espressamente riunioni e manifestazioni pacifiche.
6. Integrare l'articolo 9 con doppia valutazione d'impatto ove applicabile, log completi e non modificabili, validazione indipendente, metriche contestuali di accuratezza e monitoraggio effettivo dei falsi positivi.

7. Integrare l'articolo 17 con un ordine di conservazione delle prove e garanzie di accesso effettivo nonostante i segreti commerciali; riformulare l'articolo 18 secondo la ragionevole idoneità causale della violazione.
8. Istituire un registro nazionale riservato dei sistemi di IA di polizia e una relazione annuale pubblica; subordinare l'uso dei sistemi di intelligenza artificiale alla disponibilità effettiva di formazione, validazione, logging e risorse organizzative.

Conclusione

Lo schema ha il merito e l'ambizione di affrontare temi complessi in modo organico, efficace per le Forze di Polizia e nel rispetto dei diritti fondamentali. Perché l'intervento sia stabile, occorre che le garanzie più importanti siano contenute direttamente nella fonte primaria e che l'uso biometrico rimanga eccezionale, mirato, autorizzato e tecnicamente contestabile. La tecnologia può supportare l'attività di polizia ma non deve trasformare un risultato algoritmico probabilistico in una prova certa, né una possibilità tecnica in una sorveglianza ordinaria. Le Forze di Polizia dovrebbero avere una formazione avanzata prima di gestire i sistemi di intelligenza artificiale.

12. Riferimenti normativi e documentali

I riferimenti sono riportati in forma essenziale. I collegamenti rinviano a fonti ufficiali o istituzionali consultate per la redazione.

- [1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (AI Act) — in particolare considerando 32, 34, 36 e 95; articoli 4, 5, 12, 14, 15, 26, 27 e 59.
- [2] Direttiva (UE) 2016/680 relativa ai trattamenti delle autorità competenti — in particolare principi di necessità e proporzionalità e valutazione d'impatto.
- [3] Legge 23 settembre 2025, n. 132 — Disposizioni e deleghe al Governo in materia di intelligenza artificiale — in particolare articolo 24.
- [4] Camera dei deputati — Atto del Governo n. 418 e documentazione acquisita — pagina ufficiale dell'esame parlamentare.
- [5] Garante per la protezione dei dati personali — Parere del 2 agosto 2024 sul disegno di legge in materia di IA — sull'autorizzazione biometrica, il ruolo del Garante e gli spazi di sperimentazione.
- [6] Corte europea dei diritti dell'uomo — Glukhin c. Russia, 4 luglio 2023 — riconoscimento facciale, vita privata e libertà di espressione in una manifestazione pacifica.
- [7] NIST — Face Recognition Technology Evaluation: Demographic Effects — prestazioni, falsi positivi e differenziali demografici.
- [8] EDPB-EDPS, Joint Opinion 5/2021 sulla proposta di AI Act — rischi elevati dell'identificazione biometrica remota in spazi pubblici.
- [9] Corte costituzionale, sentenza n. 175 del 2022 — determinatezza dei criteri di delega in materia penale.
- [10] Parlamento europeo — approvazione del Digital Omnibus sull'IA, 16 giugno 2026 — stato del procedimento di modifica dell'AI Act.
- [11] EUR-Lex — testo finale del Digital Omnibus sull'IA, documento PE 30/2026 REV 1 — testo datato 8 luglio 2026.
- [12] Direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi — coordinamento con la responsabilità da prodotto.