



Prof. Mitja Gialuz

Professore ordinario di Diritto processuale penale nell'Università di Genova

CAMERA DEI DEPUTATI – COMMISSIONE GIUSTIZIA

Giovedì 23 luglio 2026 – audizione 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 (418).

Signor Presidente,
Onorevoli Deputate e Deputati,

permettetemi in primo luogo di ringraziarvi per l'invito: sono onorato di contribuire ai lavori di analisi della Commissione su uno schema di decreto legislativo che dà attuazione alla delega contenuta nella l. 132 del 2025 su un tema cruciale, non solo per l'attività di *law enforcement*, ma per la tutela delle libertà fondamentali e dei diritti dei cittadini.

Mi soffermerò in particolare sui profili legati alla disciplina contenuta nel Capo III e dedicata ai Sistemi di intelligenza artificiale utilizzati nelle attività di polizia 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. In particolare, degli artt. 8, 10 e 13.

I. Il bilanciamento tra i valori in gioco

Si tratta del punto chiave della disciplina perché concerne condizioni e limiti di applicabilità nel nostro ordinamento di meccanismi di identificazione biometrica, come il SARI (Sistema Automatico di Riconoscimento Facciale), che ha suscitato in passato una profonda discussione. Sono meccanismi che presentano profili di **particolare delicatezza nelle democrazie contemporanee** e richiedono un attento bilanciamento tra: le esigenze di prevenzione e repressione dei reati; i diritti individuali tra cui va annoverato il diritto alla protezione dei dati personali

(artt. 7 e 8 Carta di Nizza + 8 C.e.d.u.), che viene protetto al massimo livello posto che i dati biometrici sono equiparati a quelli genetici e a quelli relativi alla salute dall'art. 10 della direttiva n. 680/2016; le libertà di associazione, di riunione, di manifestazione del pensiero e, in definitiva, la stessa libertà morale, considerato che un trattamento generalizzato e non proporzionato di tale strumento può determinare il cd. *chilling effect* (Corte edu, 4 luglio 2023, Glukhin c. Russia, che ha condannato la Russia per violazione dell'art. 8 C.e.d.u., considerato che l'uso di una tecnologia di riconoscimento facciale altamente invasiva nel contesto dell'esercizio, da parte del ricorrente, del suo diritto alla libertà di espressione sancito dalla Convenzione è incompatibile con gli ideali e i valori di una società democratica regolata dallo Stato di diritto, che la Convenzione è stata concepita per salvaguardare e promuovere).

Proprio la Corte ha chiarito la necessità di prevedere una base legale di qualità per l'utilizzo di tali strumenti e di rispettare il canone di proporzionalità, in forza del quale, siccome si tratta di misure particolarmente invasive – soprattutto per quanto riguarda la tecnologia di riconoscimento facciale in tempo reale – è necessario un **elevato livello di giustificazione** affinché esse possano essere considerate «necessarie in una società democratica».

II. Considerazioni critiche di ordine sistematico

Preso atto che lo schema di decreto legislativo costituisce un passo avanti nella misura in cui predispone una base legale per i diversi impieghi degli strumenti di identificazione biometrica, la disciplina suscita qualche perplessità sul piano sistematico.

In primis, va detto che i sistemi di identificazione biometrica remota in tempo reale assomigliano a una forma di intercettazione e quindi a un mezzo di ricerca della prova. Si tratta infatti di captazione in diretta di dati biometrici: si suggerisce pertanto, per quel che concerne il riconoscimento collocato in ambito procedimentale, di prevedere un apposito **capo IV bis nel titolo III del libro III**, che potrebbe divenire un **contenitore generale per tutti i mezzi di ricerca della prova basati sull'IA**. Si potrebbe inserire una norma generale (art. 271-bis c.p.p.) in cui fissare i principi generali (quali la proporzionalità, la trasparenza, ecc.) e poi norme speciali relative ai diversi atti. Il primo potrebbe essere proprio un art. 271-ter dedicato alla disciplina del riconoscimento facciale in tempo reale. Potrebbero poi seguire diverse norme dedicate a singoli atti di ricerca basati sull'IA.

Forse si potrebbe collocare qui anche un art. 271-*quater* dedicato al riconoscimento *ex post* oppure tale istituto potrebbe essere collocato nel libro V, accanto alla disciplina dell'identificazione affidata alla polizia (art. 349 c.p.p.) o all'individuazione affidata al PM (art. 361 c.p.p.). A seconda delle ipotesi, l'identificazione biometrica *ex post* appare riconducibile all'una o all'altra categoria.

Quanto infine al riconoscimento attualmente disciplinato dall'art. 8 dello schema, pare che la sede più ragionevole potrebbe essere un nuovo art. 226-bis disp. att., posto che la disciplina di tale meccanismo è palesemente modellata su quella delle intercettazioni preventive.

Per quel che riguarda invece le norme non processuali, come l'art. 9, appare ragionevole mantenerle in una sede diversa dal codice di rito e quindi potrebbero trovare collocazione nel decreto.

III. Rilievi critici sulle singole disposizioni e proposte di emendamento

1. Art. 8, che disciplina i 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).

Al di là del refuso contenuto nel primo comma ove si richiama l'art. 14 mentre è l'art. 13 che introduce il 359-ter c.p.p., il punto critico mi pare la competenza per l'autorizzazione del Procuratore della Repubblica.

Dal punto di vista delle fonti e della giurisprudenza europea, prevedere il **controllo preventivo di un giudice non è una soluzione obbligata, ma comunque preferibile**. Le attività gravemente intrusive nei diritti fondamentali dei singoli, specialmente con riferimento agli **artt. 7 e 8 della Carta**, richiedono un controllo preventivo svolto da un'autorità (giudiziaria, o amministrativa indipendente, peraltro a prescindere che si tratti di accertamento di reati o di sicurezza pubblica) che **"disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per garantire una conciliazione dei diversi interessi e diritti in gioco"** (ex multis, C-746/18, *Prokuratuur*). In tale occasione si era escluso che il p.m. potesse svolgere tale ruolo, in quanto coinvolto attivamente nelle indagini e non equidistante. Pur non essendo questo il caso del Procuratore della Repubblica nella disciplina *de qua*, il giudice mi pare sia un organo meglio attrezzato per compiere delicate operazioni di contemperamento dei diritti individuali e delle istanze di sicurezza. Va aggiunto che il Procuratore della Repubblica interverrebbe sulla richiesta dei medesimi soggetti (i vertici delle Forze dell'Ordine) ai quali deve a sua volta chiedere il personale per svolgere le indagini. Questa considerazione indebolisce senza dubbio l'imparzialità del Procuratore.

Gli argomenti di cui sopra varrebbero anche in relazione alle **intercettazioni preventive**: in una prospettiva *de iure condendo*, sarebbe opportuno, per le stesse ragioni dianzi espresse, attribuire al giudice il compito di autorizzare le intercettazioni preventive.

Proposte di emendamento:

- collocare la disposizione nell'art. 226 bis disp. att.;
- attribuire la competenza funzionale a un giudice. Problema: quale giudice? Attualmente, non abbiamo un giudice dei diritti per le intrusioni preventive. Forse oggi avendo tipologie di intrusione diverse e avendo guadagnato un livello diverso quei diritti, merita ragionare su un giudice dei diritti preventivo. Potrebbe essere il **presidente della sezione GIP** o il **presidente del Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione ovvero di ricerca**.

Forse la seconda scelta consente scelte organizzative più sartoriali e non mi pare confliggere con il principio del giudice naturale. Poi verrà indicato nella tabella del tribunale il giudice, che verosimilmente sarà il presidente della sezione GIP.

2. Art. 13, che inserisce nel codice di rito penale l'art. 359-ter rubricato *Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale*.

Come già anticipato, la norma appare fuori posto: l'attività non è equiparabile a un accertamento tecnico. A me pare sia piuttosto assimilabile a un'intercettazione, nella misura in cui vi è una sorveglianza in tempo reale che consente di acquisire dei dati biometrici.

Una grave criticità **riguarda però la disciplina d'urgenza** contemplata dal comma 7, ove si affida la competenza al PM e, “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”. Mi pare che tale disposizione possa essere conforme al Regolamento (che prevede un'eccezione all'art. 5 par. 3), ma che sia a **rischio di illegittimità costituzionale per violazione dell'art. 3 Cost.**: la disciplina sulle intercettazioni non prevede (e non potrebbe prevedere, data la riserva di giurisdizione di cui all'art. 15 Cost.), neppure per i casi di urgenza, poteri autonomi della p.g. Visto che l'intrusività dello strumento è **quanto meno equiparabile**, sembra che lo stesso divieto debba imporsi nel caso di specie.

Si consideri che anche la disciplina d'urgenza per l'acquisizione di tabulati prevede intervento del pm con successiva convalida del giudice: art. 132, c. 3-*bis*¹. Ne conseguirebbe il paradosso per cui, per un atto meno intrusivo, si esclude la facoltà di attivarsi della polizia, mentre lo si consentirebbe per un atto molto più intrusivo per il singolo e per la collettività quale è il riconoscimento biometrico *real time*.

3. Art. 10, contenente disposizioni in materia di sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall'intelligenza artificiale, per il contrasto dei reati

Si tratta senz'altro della norma più problematica.

a. Il primo profilo riguarda la **mancata previsione del procedimento autorizzatorio ordinario**. L'art. 26, par. 10, del Regolamento stabilisce che l'uso dei sistemi di identificazione biometrica a posteriori richiede, come regola generale, un'autorizzazione preventiva - o comunque entro 48 ore - da parte di “un'autorità giudiziaria o amministrativa terza, la cui decisione sia vincolante e soggetta a controllo giurisdizionale” (*«fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la*

¹ Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini ovvero alle ricerche di un latitante, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato.

ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, ex ante o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema»). L'art. 10 dello schema decreto non reca una disciplina di questa procedura autorizzatoria, né in via preventiva né in via successiva. Ciò posto, per esigenze di adeguamento all'atto eurounitario, sarebbe necessario **inserire una previsione che vada ad ovviare questo difetto**.

Proposta di emendamento: introdurre un nuovo articolo in un nuovo capo IV-bis all'interno del libro III, titolo III del c.p.p. (v. meglio *infra*), che stabilisca che

“nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il pubblico ministero chiede in via preventiva, o senza indebito ritardo ed entro 48 ore, un'autorizzazione da parte del giudice per le indagini preliminari, il quale decide con decreto motivato”.

La proposta di attribuire la competenza ad autorizzare l'impiego dello strumento di riconoscimento facciale in capo al **giudice per le indagini preliminari in questo caso è necessitato dalla giurisprudenza della Corte di Lussemburgo**, la quale, al cospetto delle attività gravemente intrusive dei diritti fondamentali, specie rispetto agli artt. 7 e 8 della Carta, tende a richiedere un **controllo preventivo svolto da un giudice o da un'autorità amministrativa indipendente**. Si tratta di organi che dovrebbero possedere tutte le attribuzioni e le garanzie per assicurare il corretto bilanciamento tra gli interessi legati alle esigenze delle indagini penali e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali dei soggetti i cui dati sono coinvolti nell'accesso². Centrale per la Corte è il rispetto del criterio dell'indipendenza, il quale si compone di due fondamentali condizioni: 1) l'autorità deputata al controllo non deve essere coinvolta nella conduzione delle indagini in questione (e, quindi, non potrebbe essere il pubblico ministero); 2) deve trovarsi in una posizione di neutralità rispetto alle parti del procedimento penale³.

b. L'ipotesi normata dall'art. 10, comma 2 dello schema di d.lgs. si fonda evidentemente sull'**eccezione** rispetto alla **necessità dell'autorizzazione preventiva** stabilita dall'art. 26, par. 10, reg. Mi pare che sia scritto male perché non riprende testualmente tale eccezione e finisce in tal modo per disciplinare un'ipotesi diversa e per creare confusione.

Il Regolamento ammette infatti una deroga all'obbligo di autorizzazione soltanto per «l'*identificazione iniziale* di un **potenziale sospetto** sulla base di fatti oggettivi e verificabili direttamente connessi al reato». L'ipotesi tipica è quella del reato appena consumato in un luogo pubblico ripreso da telecamere, le forze di polizia dispongono di un volto ma non sanno a chi appartenga e il sistema di riconoscimento facciale serve a dare un nome a quell'identità ancora ignota. È un uso puntuale, limitato a quel momento iniziale e a quella specifica lacuna conoscitiva.

² V. Corte giust. UE, 30 aprile 2024, *La Quadrature du Net* e a., C-470/21, punto 125.

³ Cfr. Corte giust. UE, 5 aprile 2022, C-140/20, *G.D.*, punto 108; Corte giust. UE, 2 marzo 2021, C-746/18, *H.K. (Prokuratuur)*, punto 54.

L'art. 10, comma 2, disciplina **invece una situazione diversa e più avanzata sul piano investigativo**: il sistema viene attivato quando esiste già un indiziato, precedentemente individuato sulla base di documentazione video-fotografica e di altri elementi oggettivi e verificabili. Si pensi al caso in cui la polizia abbia già identificato, attraverso testimonianze, intercettazioni o altri elementi, Mevio come presunto autore di una rapina; l'art. 10 consente allora di attivare il riconoscimento facciale per verificare la presenza di Tizio nei luoghi e nei momenti rilevanti. Il sospettato non è ignoto ma è già noto, e il sistema interviene a rafforzare o a confermare un'accusa già formulata su altra base. Si tratta di **un uso ulteriore e aggiuntivo rispetto all'ipotesi minima che la deroga del Regolamento intende coprire**. La deroga **non pare pertanto invocabile per escludere il generale obbligo di autorizzazione**.

c. Particolarmente delicato mi pare **l'art. 10, comma 3**, che disciplina un **meccanismo bi-fasico**:

a. raccolta e memorizzazione dei dati biometrici di chiunque acceda a luoghi o eventi in relazione ai quali si registrano esigenze di **ordine e sicurezza pubblica**, come stadi, stazioni, piazze durante manifestazioni o concerti. I tratti biometrici acquisiti sono conservati per **sette giorni in un archivio locale**

b. utilizzo di dati biometrici ex post nell'ipotesi di commissione di un fatto di reato ai sensi del comma 2. In questa ipotesi si potranno attivare le tecnologie di riconoscimento facciale con il trattamento automatizzato dei dati biometrici estratti dalle immagini del volto per accertare qualsiasi reato.

Sembra che la norma ponga qualche problema sotto diversi profili.

Anzitutto, sotto il profilo della costituzione di un archivio di volti, orari e luoghi costruito in via anticipatoria su una platea indifferenziata di cittadini che non sono sospettati di alcunché possa porre dei problemi, sulla base di **presupposti molto generici**: **“In caso di accesso a luoghi o ad eventi rispetto ai quali sussistono esigenze di ordine e sicurezza pubblica**.

Ciò è problematico con riguardo al regolamento, che nel **considerando 95** vieta esplicitamente la *“sorveglianza indiscriminata”*; nonché con riferimento al **canone di proporzionalità** fissato dagli artt. 7 e 8 Carta di Nizza.

Il riferimento comune a “luoghi o ad eventi” rischia di creare problemi: per il luogo il rischio è di introdurre una sorveglianza generalizzata e permanente.

In secondo luogo, la norma presenta profili problematici con riguardo al codice: questa è una **forma di individuazione**, che deve essere effettuata dal PM e non dalla pg.

In terzo luogo, emergono criticità con riguardo all'art. 52 Carta di Nizza e della **direttiva n. 680 del 2016**, che **prevede il principio di minimizzazione dei dati di cui all'art. 4, par. 1, lett. c)**. A me pare che quest'ultima richieda la **predeterminazione dei reati**. Utili coordinate provengono dalla pronuncia della Corte relativa all'accesso a dati contenuti nello *smartphone* (C-548/21, *CG-Landeck*), attività regolata dalla direttiva 2016/680/UE: da un lato, *“ritenere che solo la lotta contro i reati gravi possa giustificare l'accesso a dati contenuti in un telefono cellulare limiterebbe i poteri di indagine delle autorità competenti, ai sensi della direttiva 2016/680, nei confronti dei reati in generale”*;

dall'altro, **alla luce dell'art. 52 della Carta**, che impone che la limitazione dei diritti fondamentali tutelati dalla stessa Carta sia “prevista dalla legge”, “*spetta al legislatore nazionale definire in modo sufficientemente preciso gli elementi, in particolare la natura o le categorie dei reati di cui trattasi, da prendere in considerazione*”.

Proposta di emendamento: In linea generale, ingerenze “gravi” nei diritti fondamentali dovrebbero essere giustificate dal contrasto di forme “gravi” di criminalità (*ex multis*, C-511/18, C-512/18, C-520/18, *La Quadrature du Net I*)⁴. Per trovare un giusto equilibrio con le esigenze di sicurezza e accertamento, potrebbe suggerirsi la tecnica già in uso nell'art. 266 c.p.p., con la **previsione di una soglia edittale e di un elenco di reati per i quali si intende comunque consentire il ricorso al mezzo di ricerca della prova** (ad esempio, nel nostro caso, reati commessi con violenza sulle cose o sulle persone).

4. Mancanza della sorveglianza umana rafforzata

Nella previsione dell'art. 10 dello schema manca una **sorveglianza umana rafforzata** mediante una procedura di **verifica obbligatoria del risultato prodotto dal sistema a opera di almeno due operatori indipendenti**, in linea con il **considerando n. 73 del reg. IA**. Il considerando così recita: «*tenuto conto delle conseguenze significative per le persone in caso di una corrispondenza non corretta da parte di determinati sistemi di identificazione biometrica, è opportuno prevedere un requisito rafforzato di sorveglianza umana per tali sistemi, in modo che il deployer non possa adottare alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato **separatamente da almeno due persone fisiche**. Tali persone potrebbero provenire da una o più entità e comprendere la persona che gestisce o utilizza il sistema. Tale requisito non dovrebbe comportare oneri o ritardi inutili e potrebbe essere sufficiente che le verifiche separate da parte delle diverse persone siano automaticamente registrate nei log generati dal sistema. Date le specificità dei settori delle attività di contrasto, della migrazione, del controllo delle frontiere e dell'asilo, tale requisito non dovrebbe applicarsi se il diritto dell'Unione o nazionale ritenga sproporzionata la sua applicazione*».

In dottrina (Ernestina Sacchetto, *Tecnologie di riconoscimento facciale e procedimento penale*, Torino, 2025, p. 193), si è **enfaticizzata l'importanza di tale doppio controllo**, dal momento che «assume una valenza cruciale non solo per ridurre al minimo gli errori sistemici, ma anche per attenuare l'impatto di potenziali bias algoritmici o di condizionamenti cognitivi che potrebbero influenzare il giudizio di un singolo operatore».

Genova, 23 luglio 2026

Mitja Gialuz

⁴ Per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, conformemente al principio di proporzionalità, solo la lotta alle forme gravi di criminalità e la prevenzione di minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta.

Ms