RELAZIONE PER L'AUDIZIONE

Schema di decreto legislativo A.G. n. 418 – impiego dell'intelligenza artificiale nelle attività di polizia

Avv. Francesco Paolo Micozzi

1. Introduzione

Lo schema di decreto legislativo A.G. n. 418 (di seguito indicato anche come "AG418" o "Schema"), adottato in attuazione dell'art. 24 della L. 132/2025, introduce una disciplina specifica dell'impiego di sistemi e modelli di intelligenza artificiale nelle attività delle Forze di polizia. Lo Schema interviene su ricerca, sviluppo, addestramento e sperimentazione dei sistemi, sorveglianza umana, trattamento dei dati personali, identificazione biometrica e responsabilità penale.

Tuttavia, la sua conformità sostanziale ai criteri direttivi della legge-delega non è integrale. Risultano attuati la disciplina specifica dell'IA per l'attività di polizia, la formazione del personale, la nuova fattispecie omissiva e gli strumenti processuali civili. Sono invece solo parzialmente attuati i criteri relativi all'effettività del controllo umano, alla base giuridica dei trattamenti effettuati per l'addestramento, alla composizione e al regime delle banche biometriche, alla tutela delle persone estranee a qualsiasi attività criminosa, alla disponibilità degli elementi necessari all'esercizio del diritto di difesa e al coordinamento con la normativa vigente. Non trova, inoltre, corrispondenza nello Schema il criterio relativo agli strumenti per inibire e rimuovere i contenuti illeciti. Deve inoltre essere chiarito se l'articolo 10, introducendo l'acquisizione preventiva dei template biometrici della generalità delle persone "presenti" al dato luogo o evento, rimanga entro l'oggetto della delega o, eccedendo, introduca un potere di trattamento ulteriore rispetto a quanto necessario per l'adeguamento all'AI Act.

In primo luogo, l'articolo 3 qualifica i sistemi, i modelli e i relativi output come strumenti di supporto alle valutazioni e alle decisioni umane e prevede una revisione umana qualificata. Tali disposizioni non escludono però in termini inequivoci che l'output algoritmico possa determinare sostanzialmente l'esito di un atto, di una misura investigativa o di un'attività operativa incidente sulla persona. Occorre pertanto **introdurre un espresso divieto di adottare decisioni produttive di effetti giuridici negativi, o comunque significativamente incidenti, unicamente o in misura determinante sulla base dell'elaborazione automatizzata**. La revisione umana dovrebbe consistere in una valutazione autonoma, effettiva e documentata, svolta da personale adeguatamente formato e posto nella concreta condizione di verificare, disattendere o interrompere il funzionamento del sistema.

In secondo luogo, le disposizioni degli articoli 3-5 relative a ricerca, sviluppo, addestramento, collaborazioni e spazi di sperimentazione non possono ricondurre automaticamente ogni trattamento di dati effettuato in vista di un futuro impiego di polizia al decreto legislativo n. 51 del 2018. L'individuazione della disciplina applicabile dipende dalla finalità concretamente perseguita, dal titolare del trattamento e dal ruolo effettivo dei soggetti coinvolti. Università, imprese o altri partner che utilizzino i dati per finalità proprie di ricerca, sviluppo commerciale o miglioramento di prodotti non possono essere qualificati come meri responsabili del trattamento. Lo Schema dovrebbe quindi **disciplinare espressamente titolarità, responsabilità, localizzazione dei dati, subfornitura, accessi, riuso, cancellazione e divieto di incorporazione dei dati operativi o biometrici in modelli, pesi, *embedding* o *checkpoint* destinati a impieghi ulteriori**.

Il nucleo maggiormente problematico riguarda l'identificazione biometrica. Lo Schema contempla tre modelli distinti: (a) l'identificazione biometrica remota in tempo reale per finalità preventive, disciplinata dagli articoli 8 e 9; (b) il riconoscimento facciale a posteriori nei luoghi o

negli eventi caratterizzati da esigenze di ordine e sicurezza pubblica, previsto dall'articolo 10; (c) l'identificazione biometrica in tempo reale nell'ambito del procedimento penale, disciplinata dall'articolo 13. Le differenze non attengono soltanto al momento del confronto, ma investono finalità, autorità competente, presupposti applicativi e, soprattutto, composizione della banca dati di riferimento.

La **generazione preventiva e indifferenziata dei template biometrici di persone non sospettate costituisce il principale profilo critico dello Schema**. L'ingerenza nei diritti fondamentali si realizza già al momento dell'acquisizione, della trasformazione del volto in template e della sua memorizzazione, non soltanto al momento del successivo confronto. Tale trattamento deve essere valutato alla luce dei requisiti di stretta necessità, proporzionalità e determinatezza derivanti dalla direttiva (UE) 2016/680, dagli articoli 7, 8 e 52 della Carta dei diritti fondamentali e dalla giurisprudenza europea in materia di dati biometrici.

Deve inoltre essere chiarito se la costituzione preventiva di una banca biometrica di tutti i soggetti che si trovino "sul luogo o all'evento" di cui all'art. 10, rientri nell'oggetto e nei criteri della delega o introduca un autonomo potere di trattamento ulteriore rispetto a quanto necessario per l'adeguamento all'AI Act. La finalità dichiarata dall'articolo 10 potrebbe infatti essere perseguita mediante una soluzione meno invasiva consistente nella conservazione temporanea delle registrazioni video grezze e eventuale generazione selettiva (con riferimento alle persone indiziate) dei template biometrici al verificarsi di uno specifico fatto di reato. Spetta pertanto al Governo dimostrare perché tale alternativa non sia idonea e perché il pre-enrollment biometrico generalizzato sia strettamente necessario.

In conclusione, lo Schema può costituire un'importante base normativa per l'impiego dell'intelligenza artificiale nelle attività di polizia, purché siano introdotti limiti sostanziali, garanzie procedurali e meccanismi di controllo concretamente verificabili. La disciplina dovrebbe assicurare che l'intelligenza artificiale rimanga effettivamente subordinata alla decisione umana; che ogni banca biometrica abbia composizione, finalità, durata e responsabilità chiaramente determinate; che i dati delle persone estranee ai reati non siano acquisiti in modo generalizzato; e che ogni output algoritmico suscettibile di incidere sulla persona possa essere compreso, contestato e sottoposto a un controllo indipendente ed effettivo.

2. Attività e finalità "di polizia"

L'intero Titolo I dello Schema di decreto legislativo si occupa dell'utilizzo dei sistemi di intelligenza artificiale "per l'attività di polizia" in relazione alle specifiche funzioni esercitate in base all'AI Act e alla L. 132/2025 da organi, uffici e comandi delle "Forze di Polizia".

Lo Schema e il d.lgs. 51/2018 adottano la medesima definizione di "Forze di polizia" (tramite richiamo alla norma di cui all'art. 16 della L. 121/1981) e individuano finalità di polizia sostanzialmente coincidenti. Non vi è, invece, coincidenza tra le "Forze di polizia" e la categoria delle "autorità competenti", che nel d.lgs. 51/2018 ricomprende, tra le altre, proprio le Forze di polizia.

Ciò che rileva, tuttavia, è che l'appartenenza del titolare del trattamento dei dati personali a una Forza di polizia non determina automaticamente l'applicazione del d.lgs. 51/2018 posto che ulteriore criterio applicativo delle disposizioni del d.lgs. 51/2018 (che recepisce in Italia la Direttiva UE 2016/680) oltre a quello soggettivo è che il trattamento dei dati personali sia concretamente svolto per una delle finalità tassativamente indicate dall'articolo 1, comma 2, ossia per finalità di "*prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica*".

Conseguentemente, con riguardo alla ricerca delle persone scomparse, occorre chiarire se lo Schema intenda limitare l'impiego dei sistemi ai casi riconducibili alle finalità di contrasto indicate

dall'articolo 3, punto 46), dell'AI Act oppure ricomprendere anche attività di mero soccorso. In quest'ultima ipotesi, il trattamento non sarebbe automaticamente assoggettato al d.lgs. n. 51/2018.

Allo stesso modo il trattamento di dati personali eventualmente svolto nella fase di ricerca, sviluppo o addestramento (art. 3, comma 6 dello Schema) può rientrare nel d.lgs. n. 51/2018 anche in assenza di una specifica indagine, purché sia effettuato da un'autorità competente e sia concretamente funzionale a una o più finalità di polizia. La mera destinazione futura del prodotto alla polizia non è invece sufficiente quando il titolare persegua una distinta finalità scientifica, commerciale, amministrativa o di sviluppo generalista. Ancora.

L'articolo 4 dello Schema ammette collaborazioni con partner come università, enti di ricerca e soggetti pubblici o privati e prevede (opportunamente) clausole volte a impedire la condivisione dei dati operativi sensibili e il loro uso commerciale o per finalità estranee alla collaborazione. Resta però necessario stabilire il ruolo effettivo del partner. Se il partner tratta i dati esclusivamente per conto della Forza di polizia, sulla base di istruzioni documentate e senza finalità proprie, può operare come responsabile nell'ambito del regime del d.lgs. 51/2018. Se il partner persegue una propria finalità scientifica, didattica, editoriale o commerciale, non svolge il trattamento per una finalità dell'articolo 1, comma 2, e deve essere individuata un'autonoma base giuridica nel GDPR (la diversità dei regimi riguarda normalmente trattamenti distinti o successivi). Infine, se il partner determina insieme alla Forza di polizia finalità e mezzi, occorre affrontare il problema della contitolarità e della possibile diversità dei regimi applicabili.

3. I tre modelli di identificazione biometrica previsti

Concentrandoci, per il momento, sugli aspetti più rilevanti del Capo I dello Schema di decreto legislativo, è necessario distinguere tra i tre modelli di acquisizione e impiego dei dati biometrici, disciplinati rispettivamente dagli articoli 8, 10 e 13.

Non si tratta di varianti meramente tecniche della stessa operazione, posto che mutano la finalità del trattamento, il momento nel quale avviene l'identificazione, la composizione della banca dati, l'autorità competente e, soprattutto, la posizione delle persone in alcun modo coinvolte in attività criminose.

3.1. Primo modello (art. 8)

L'articolo 8[1] disciplina l'**identificazione biometrica remota in tempo reale**, in luoghi pubblici o aperti al pubblico, per finalità di prevenzione di specifiche minacce, nonché per la ricerca di persone scomparse o vittime di determinati reati.

La disposizione recepisce due delle tre eccezioni al divieto generale stabilito dall'art. 5, co. 1, lettera h), dell'AI Act per l'uso degli strumenti di identificazione biometrica in tempo reale: la **prevenzione di una minaccia** specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone oppure di una minaccia reale e attuale, o reale e prevedibile, di un attacco terroristico; la **ricerca mirata di una persona** scomparsa o di specifiche vittime di sequestro di persona, tratta di esseri umani o sfruttamento sessuale.

Il sistema non può essere utilizzato per identificare indiscriminatamente le persone presenti nell'area sorvegliata ma è diretto alla conferma dell'identità o alla ricerca, anche dinamica e alla geolocalizzazione, di persone specificamente individuate o almeno individuabili in relazione alla minaccia o alla ricerca da eseguire. Si tratta, pertanto, di un modello basato su una lista circoscritta di soggetti i cui dati biometrici rilevati dal flusso video sono confrontati in tempo reale con una banca dati di riferimento contenente i dati delle persone specificamente interessate. La banca dati può essere

[1] 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

ricavata da archivi in uso alle Forze di polizia, da banche dati di altre amministrazioni legalmente accessibili oppure (scraping mirato) da immagini, filmati e altri elementi biometrici acquisiti lecitamente nell'attività di polizia. È espressamente escluso l'impiego di banche dati alimentate mediante scraping non mirato o costituite in violazione della normativa sulla protezione dei dati[2].

L'attivazione segue un procedimento amministrativo-giudiziario di prevenzione. La richiesta proviene dal questore, dai comandanti provinciali dell'Arma dei carabinieri o della Guardia di finanza oppure dai responsabili dei servizi centrali individuati dalla legge ed è rivolta al procuratore della Repubblica presso il tribunale del capoluogo del distretto interessato. L'autorizzazione deve individuare la finalità, le persone ricercate, l'area geografica, la banca dati utilizzata e la durata dell'operazione. Quest'ultima non può eccedere quindici giorni, salva la possibilità di proroghe motivate per successivi periodi della medesima durata.

Nei casi di urgenza l'impiego può essere avviato direttamente su disposizione dell'autorità di polizia competente, previa comunicazione, anche orale, al procuratore della Repubblica. La richiesta deve essere trasmessa entro ventiquattro ore e il procuratore deve pronunciarsi nelle ventiquattro ore successive. La mancata autorizzazione o l'inosservanza delle condizioni stabilite comportano l'interruzione immediata dell'impiego, la cancellazione dei dati, dei risultati e degli output, salvo quanto acquisito legittimamente in base a un diverso titolo, nonché l'inutilizzabilità dei risultati.

La **natura preventiva dello strumento** è ulteriormente confermata dal rinvio all'art. 226, co. 5, delle disposizioni di attuazione del codice di procedura penale. I risultati non sono destinati, in quanto tali, a costituire prova nel procedimento penale, ma assumono essenzialmente una funzione di prevenzione e orientamento investigativo. Come rileva il dossier parlamentare, è questo elemento finalistico, più ancora di quello tecnologico, a distinguere l'art. 8 dall'identificazione in tempo reale disciplinata dall'articolo 13.

All'impiego si applicano inoltre le garanzie comuni dell'articolo 9: preventiva valutazione d'impatto sui diritti fondamentali, registrazione automatica in file di log non modificabili, conservazione quinquennale dei log, notifica successiva al Garante e definizione con decreto ministeriale dei requisiti di accuratezza, sicurezza, monitoraggio e gestione degli errori.

3.2. Secondo modello (art. 10)

L'articolo 10 disciplina una situazione profondamente diversa. Non si tratta di cercare in tempo reale una persona determinata tra coloro che transitano in uno spazio pubblico, ma di costituire preventivamente, in occasione dell'accesso a determinati luoghi o eventi, una banca dati biometrica locale che possa essere interrogata successivamente qualora venga commesso un reato. La disposizione opera nei luoghi o negli eventi rispetto ai quali sussistano esigenze di ordine e sicurezza pubblica e nei quali l'installazione della videosorveglianza sia già consentita da una specifica disposizione di legge. Al momento dell'accesso vengono rilevati dalle immagini del volto e trattati automaticamente i dati biometrici di tutte le persone che entrano. I relativi modelli biometrici sono

[2] Nelle definizioni dello Schema (art. 2, co. 1, lett. l), lo «**scraping non mirato**» è inteso come "*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*". L'art. 5, co. 1, lett. e) dell'AI Act vieta espressamente le pratiche di IA consistenti ne "*l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che* ***creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso***". La presenza dell'inciso "su larga scala" nella definizione nazionale rischia di restringere una pratica vietata a prescindere dalla scala dimensionale dei dati trattati e di creare una zona franca per raccolte ridotte, ripetute, distribuite o frazionate. L'elemento decisivo dovrebbe essere il carattere non mirato dello scraping a prescindere dalla "scala" delle informazioni acquisite, proprio al fine di evitare che determinate pratiche di scraping non mirato e non su larga scala vengano comunque attratte dal divieto dell'AI Act determinando, così, una potenziale inapplicabilità della norma nazionale.

memorizzati localmente e associati ai dati anagrafici e, ove esistente, all'identificativo del posto assegnato, acquisiti mediante la scansione elettronica del titolo di accesso.

Il riconoscimento facciale viene **attivato soltanto dopo la commissione di un reato**, allo scopo di identificare una persona già indiziata sulla base di elementi oggettivi e verificabili. Tuttavia, la banca dati che rende possibile il confronto è stata costituita prima del reato mediante **l'acquisizione generalizzata dei template biometrici** di tutti coloro che hanno avuto accesso al luogo o all'evento.

Il sistema realizza, pertanto, un meccanismo bifasico. Nella prima fase, anteriore a qualsiasi reato, viene effettuato il cosiddetto pre-enrollment biometrico delle persone che accedono al luogo o all'evento (il sistema crea e conserva i modelli biometrici, ma non attiva ancora il confronto finalizzato all'identificazione). Nella seconda fase, che può iniziare soltanto dopo la commissione di un reato, anche tentato, il sistema estrae il dato biometrico dalle immagini della persona ritenuta responsabile e lo confronta con la banca dati degli accessi al fine di attribuirle un'identità ed eventualmente collegarla al titolo di ingresso e al posto occupato.

Il riconoscimento facciale può essere attivato soltanto per identificare persone già indiziate sulla base di documentazione video-fotografica e di elementi oggettivi e verificabili. Lo Schema intende evidentemente ricondurre questa ipotesi all'eccezione prevista dall'articolo 26, paragrafo 10, dell'AI Act per l'«identificazione iniziale di un potenziale sospetto» fondata su fatti oggettivi e verificabili direttamente connessi al reato. In tale ipotesi il regolamento europeo non richiede la preventiva autorizzazione giudiziaria o amministrativa prevista, invece, per gli ulteriori impieghi dell'identificazione biometrica a posteriori.

La corrispondenza non è tuttavia formulata in termini del tutto inequivoci. Lo Schema parla di «persone già indiziate», mentre l'AI Act esenta dall'autorizzazione soltanto l'identificazione iniziale di un potenziale sospetto. La disposizione dovrebbe quindi chiarire che il regime privo di autorizzazione individuale è limitato a questa prima identificazione. Qualora il sistema fosse impiegato per la ricerca di una persona già identificata o per operazioni ulteriori rispetto all'identificazione iniziale, tornerebbe applicabile l'articolo 26, paragrafo 10, dell'AI Act, che richiede un'autorizzazione preventiva oppure, nei casi consentiti, un'autorizzazione richiesta senza indebito ritardo e comunque entro quarantotto ore.

La maggiore criticità dell'art. 10 è riconducibile al fatto che non ci si limita ad analizzare una registrazione video già legittimamente acquisita, ma viene **preventivamente costituita una banca dati biometrica della generalità dei soggetti che abbiano fatto "accesso a luoghi o ad eventi" rispetto ai quali siano state ritenute sussistenti esigenze di "ordine e sicurezza pubblica"** (concetto ampio che ricomprende l'insieme delle attività preventive e repressive rivolte alla prevenzione dei reati, alla protezione delle istituzioni, dei cittadini e dei beni e alla conservazione delle condizioni fondamentali dell'ordinata e civile convivenza nazionale). Se, ad esempio, l'accesso ad un evento fosse subordinato a identificazione nominativa, non vi potrebbe essere mai necessità di una successiva identificazione biometrica.

Se anche possiamo ritenere l'impiego di tale banca dati biometrica sufficientemente circoscritto, non altrettanto può affermarsi con il momento costitutivo della stessa banca dati, alla conservazione della stessa e alla possibile estrazione, comunicazione o riversamento dei dati e dei risultati in altre banche dati soggette a termini di conservazione più lunghi, così come disciplinati dal DPR 15/2018. Questi aspetti saranno affrontati più avanti.

3.3. Terzo modello (art. 13)

L'articolo 13 introduce invece nel codice di procedura penale il nuovo articolo 359-ter e disciplina l'identificazione biometrica remota in tempo reale nell'ambito di un procedimento penale (potremmo definirlo il modello processuale e investigativo). Il sistema può essere impiegato per confermare l'identità oppure per ricercare e localizzare una persona nei cui confronti sussistano

sufficienti indizi della commissione di uno dei reati elencati nell'allegato II dell'AI Act, purché il reato sia punito con una pena detentiva il cui massimo non sia inferiore a quattro anni. Può inoltre essere utilizzato per localizzare un latitante destinatario di una misura cautelare coercitiva o di un ordine di esecuzione non sospeso che dispone la carcerazione per uno dei medesimi delitti. Nell'ambito di un procedimento penale è infine consentita la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale.

Anche questo è un modello "mirato", costruito intorno ai dati biometrici di persone specificamente individuate o individuabili. Il confronto deve avvenire con una banca dati adeguata alla singola finalità, alimentata con dati nella disponibilità della polizia giudiziaria o dell'autorità giudiziaria oppure con immagini, filmati e altri elementi biometrici legalmente acquisiti nell'indagine.

A causa del suo possibile impiego nel procedimento penale, l'autorizzazione spetta al giudice per le indagini preliminari su istanza del pubblico ministero. Il decreto deve essere motivato e delimitare l'area geografica, le persone ricercate e la durata, non superiore a quindici giorni, prorogabile con ulteriori decreti motivati per periodi successivi della stessa durata. Devono essere previamente compiute le valutazioni di necessità e proporzionalità richieste dall'articolo 5, paragrafo 2, dell'AI Act. In caso di urgenza il pubblico ministero può disporre direttamente l'attivazione con decreto motivato, da comunicare al giudice entro ventiquattro ore (e il giudice dovrebbe convalidarlo entro le successive quarantotto ore). Se l'urgenza non consente di attendere neppure il provvedimento del pubblico ministero, possono procedere direttamente gli ufficiali di polizia giudiziaria, i quali devono trasmettere la richiesta al pubblico ministero entro dodici ore. Il pubblico ministero deve richiedere la convalida entro ventiquattro ore dall'avvio e il giudice decide nelle quarantotto ore successive.

Quando il sistema sia stato utilizzato fuori dei casi consentiti o senza il rispetto delle condizioni autorizzatorie, opera una specifica sanzione di inutilizzabilità e i dati, i risultati e gli output devono essere cancellati (salvo che costituiscano corpo del reato). Anche a questo impiego si applicano le garanzie dell'articolo 9 concernenti valutazione d'impatto sui diritti fondamentali, registrazione, conservazione dei log e notifica al Garante.

3.4. I tre diversi modelli

La differenza fra gli articoli 8 e 13 non riguarda quindi la tecnologia utilizzata (che in entrambi i casi è quella dell'identificazione biometrica remota in tempo reale) ma il contesto di operatività. Mentre l'art. 8 opera sul terreno preventivo e della ricerca di persone, l'art. 13 opera entro i confini del procedimento penale. Per queste ipotesi l'art. 9 dispone garanzie comuni ad entrambe le ipotesi, compresa la valutazione d'impatto sui diritti fondamentali (FRIA) prevista dall'articolo 27 dell'AI Act. L'articolo 10, invece, rimane estraneo a tale disciplina dell'art. 9, posto che si prevede una valutazione d'impatto sulla protezione dei dati (DPIA[3]) e la consultazione preventiva del Garante, ma non è richiamata espressamente la valutazione d'impatto sui diritti fondamentali dell'AI Act.

La distinzione può essere sintetizzata in questi termini:

[3] Per i sistemi di identificazione biometrica remota in tempo reale degli artt. 8 e 13, l'art. 9 richiama la valutazione d'impatto sui diritti fondamentali prevista dall'art. 27 dell'AI Act mentre l'art. 10, co. 5, menziona invece soltanto la DPIA e la consultazione preventiva del Garante. L'omissione non dovrebbe esonerare dalla FRIA anche nelle ipotesi di cui all'art. 10, posto che il confronto uno-a-molti a posteriori è normalmente un sistema di identificazione biometrica ad alto rischio e l'utilizzatore è un'autorità pubblica. La FRIA deve comprendere libertà di riunione, espressione e associazione, non discriminazione, presunzione d'innocenza, libertà personale, diritto di difesa, ricorso effettivo ed effetto dissuasivo della sorveglianza. Una valutazione unica per sistemi "analoghi" non può ignorare le differenze tra un concerto, una manifestazione politica, un luogo di culto e un'infrastruttura critica.

- negli articoli 8 e 13 la banca di riferimento contiene, almeno in linea di principio, i dati delle persone specificamente ricercate, mentre il sistema analizza in tempo reale una pluralità indeterminata di persone presenti nello spazio sorvegliato;
- nell'articolo 10, invece, la banca dati contiene preventivamente i template biometrici della generalità delle persone che accedono al luogo o all'evento, affinché possa essere effettuato, dopo l' eventuale commissione di un reato, il confronto con la persona da identificare;
- mentre l'art. 8 si colloca nelle attività di prevenzione e protezione, e l'art. 13 prevede l'uso dell'IA all'interno del singolo procedimento penale, l'art. 10 disegna, infine, un'infrastruttura biometrica temporanea e destinata a un eventuale utilizzo investigativo successivo.

4. La "banca dati di riferimento"

Una ulteriore difficoltà interpretativa deriva dall'impiego, in diverse disposizioni dello Schema, della medesima espressione – «banca dati di riferimento» o «base di dati di riferimento» – per indicare archivi che hanno composizione, funzione e impatto sui diritti fondamentali profondamente differenti.

Negli articoli 8 e 13, relativi all'identificazione biometrica remota in tempo reale, la banca dati di riferimento dovrebbe contenere i dati biometrici delle persone specificamente ricercate: persone collegate a una minaccia concreta, persone scomparse, vittime di determinati reati, indiziati o latitanti. Le immagini delle persone presenti nello spazio sorvegliato vengono analizzate in tempo reale e confrontate con questa lista di soggetti predeterminati.

Verrebbe da chiedersi: se, ad esempio, il template biometrico della persona da ricercare non fosse mai stato precedentemente acquisito ed inserito in una banca dati biometrica (come, ad esempio, AFIS) perché, in ipotesi, non se ne siano verificate le condizioni, questo template biometrico sarà creato ed inserito a posteriori nella banca dati (magari tentando di acquisire il template da immagini del soggetto)? In quale banca dati sarà inserito questo template al fine di consentire al sistema AI di effettuare il match da strumenti di acquisizione audiovisiva in tempo reale? Il comma 3 dell'art. 8 prevede che la "banca dati di riferimento", può essere "*derivata da dati contenuti in banche dati in uso alle Forze di polizia o tenute da altre pubbliche amministrazioni e accessibili alle predette Forze, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle attività di polizia*". La disposizione processuale contenuta nel nuovo articolo 359-ter c.p.p. usa una formula analoga per immagini, filmati o elementi biometrici acquisiti legalmente nell'ambito delle indagini. Pertanto, il testo sembra autorizzare la seguente sequenza di operazioni: immagine legittimamente acquisita; estrazione del template; inserimento in una banca operativa di confronto; ricerca biometrica in tempo reale.

In termini tecnici, in un sistema di riconoscimento biometrico abbiamo, da un lato l'immagine rilevata dal sistema che costituisce il dato da sottoporre a verifica – il cosiddetto "**probe**" – e dall'altro la banca dati biometrica dalla quale il sistema IA attinge per il confronto (la "**gallery**"). Il trattamento potrebbe ben coinvolgere altre persone che transitassero nell'area di ripresa, ma essendo la "gallery" di confronto stabile, il sistema dovrebbe essere in grado di riconoscere unicamente i soggetti dei quali siano stati precedentemente acquisiti e poi conservati i template biometrici.

La creazione del template, però, è un autonomo trattamento di dati biometrici. Non basta che la fotografia sia stata lecitamente acquisita: occorre che anche la sua trasformazione in template e il suo impiego per l'identificazione siano strettamente necessari, proporzionati e assistiti da garanzie adeguate. L'articolo 10 della direttiva 2016/680 impone proprio queste condizioni per il trattamento biometrico da parte delle autorità competenti.

In quale banca dati viene inserito il dato biometrico? È proprio qui che lo Schema è lacunoso. Non individua una banca dati determinata. Parla genericamente di «una banca dati di riferimento adeguata per ciascuna delle finalità». Questa potrebbe essere una banca dati già esistente; una selezione logica ricavata da più archivi; una gallery temporanea creata per la singola operazione di polizia; un archivio materialmente collocato nel sistema di IA o nell'infrastruttura del fornitore; una banca operativa alimentata trasferendo copie dei template estratti da immagini e filmati. L'espressione «**può essere derivata**» sembra ammettere la costituzione di una nuova raccolta, almeno sul piano logico e funzionale. Ma lo non si dice chi materialmente crea e gestisce questa raccolta; dove sia conservata; se il template debba essere cancellato alla conclusione della ricerca; se debba essere cancellata anche la copia eventualmente conservata nel sistema del fornitore; se possa essere trasferito in AFIS o in altre banche dati; se possa essere riutilizzato per altre indagini e così via.

Consideriamo, oltretutto, che il termine massimo di quindici giorni (art. 8, comma 5) riguarda l'autorizzazione all'uso del sistema e non la conservazione del template nella banca dati. L'articolo 9, comma 3, rinvia invece ai termini del DPR 15/2018. Si apre quindi il rischio che una gallery nata per un'operazione di quindici giorni venga trattata come una banca dati di polizia ordinaria e conservata per periodi assai più lunghi.

Nell'articolo 10, invece, la stessa espressione «base dati di riferimento» indica qualcosa di sostanzialmente opposto. Essa è costituita mediante l'acquisizione preventiva delle immagini del volto e l'estrazione dei template biometrici di tutte le persone che accedono al luogo o all'evento. Soltanto dopo l'eventuale commissione di un reato verrebbe estratto il dato biometrico della persona da identificare e confrontato con la banca della generalità degli accessi formata inizialmente.

Si verifica quindi una vera e propria inversione della struttura del confronto:

- negli articoli 8 e 13 la banca di riferimento contiene i soggetti ricercati e il sistema analizza il flusso delle persone presenti per individuare un'eventuale corrispondenza;
- nell'articolo 10 la banca di riferimento contiene la generalità delle persone che hanno avuto accesso al luogo o all'evento e il dato della persona ricercata viene confrontato, a posteriori, con tale insieme.

L'alternanza tra le espressioni «banca dati di riferimento», utilizzata negli articoli 8 e 13, e «base di dati di riferimento», utilizzata nell'articolo 10 potrebbe non rappresentare una differenza meramente lessicale. Si tratta, come abbiamo visto, di architetture oggettivamente differenti. Nel primo caso una lista mirata di ricerca, nel secondo un archivio biometrico generalizzato e temporaneo dei soggetti "presenti" nel luogo o all'evento (in massima parte composta da persone non sospettate di alcun illecito).

Sarebbe opportuno che lo Schema chiarisse se le due espressioni individuino categorie giuridiche diverse. Qualora siano sinonimi, la terminologia dovrebbe essere uniformata a quella del regolamento europeo. Qualora, al contrario, indichino oggetti distinti, sarà necessario definirli espressamente e prevedere per la base di dati dell'articolo 10 un regime rafforzato di segregazione, limitazione delle finalità, divieto di trasferimento o duplicazione, divieto di confluenza in altre banche dati e cancellazione effettiva dei template, delle copie, degli indici e dei dati derivati. La diversa denominazione non può comunque determinare l'elusione delle garanzie applicabili ai sistemi di identificazione biometrica remota.

5. Focus sull'acquisizione biometrica dell'articolo 10

L'art. 10, co. 3, primo periodo, non si limita a consentire il confronto facciale dopo un reato ma dispone il trattamento automatizzato dei dati biometrici estratti dalle immagini del volto[4] di tutte le persone che accedono ai luoghi o partecipino eventi, con memorizzazione locale del template biometrico e, tramite scansione dei titoli di accesso, la registrazione dei corrispondenti dati anagrafici e del posto assegnato. La costituzione della banca dati di template biometrici avviene prima che alcun reato sia commesso, e tali template biometrici sono riferiti alla generalità dei partecipanti, e suscettibili di essere associati ai dati anagrafici e al posto occupato. Una volta formato tale database biometrico viene reso interrogabile per future ed eventuali finalità di polizia.

5.1. Il quadro giurisprudenziale europeo

L'ingerenza si produce nel momento in cui **il volto di ogni partecipante viene rilevato, ne viene estratta una rappresentazione biometrica, questa viene collegata – ove disponibili – a identità e posto occupato e il risultato è reso interrogabile**. La trasformazione del volto in template è trattamento di dati biometrici (rientranti nelle categorie particolari di dati personali che meritano una tutela rafforzata), ammesso dall'articolo 7 del d.lgs. n. 51 del 2018 solo in caso di stretta necessità, e la memorizzazione in sé costituisce interferenza con gli articoli 7 e 8 della Carta secondo la giurisprudenza consolidata sulla conservazione dei dati (da Digital Rights Ireland, C-293/12 e C-594/12, a La Quadrature du Net, C-511/18).

Il riferimento più direttamente fondato sulla direttiva 2016/680 è la sentenza C-205/21 (Spetsializiran nakazatelen sad)[5], in cui la Corte di giustizia europea ha ritenuto incompatibile con il requisito della «stretta necessità» una disciplina che consentiva l'acquisizione sistematica di dati biometrici e genetici di ogni persona accusata, senza una valutazione individuale. Si tratta di un'applicazione analogica, ma di particolare forza posto che l'articolo 10 dello Schema è ancora più delicato, perché estende la raccolta a persone che – a differenza dalla fattispecie esaminata dalla Corte di giustizia europea – non sono neppure sospettate di essere coinvolte in attività criminose.

L'orientamento è stato da ultimo confermato e rafforzato dalla sentenza C-371/24[6], Comdribus, del 19 marzo 2026. La Corte ha stabilito che neppure nei confronti di una persona sospettata di reato

---

[4] L'art. 10 circoscrive espressamente la propria disciplina ai sistemi di videosorveglianza dotati di tecnologie di riconoscimento facciale a posteriori. Tale perimetro risulta più ristretto rispetto alla nozione di «identificazione biometrica» adottata dal regolamento (UE) 2024/1689, la quale comprende il riconoscimento automatizzato di caratteristiche fisiche, fisiologiche, comportamentali o psicologiche diretto a stabilire l'identità di una persona mediante il confronto con dati biometrici contenuti in una banca dati di riferimento. Come chiarito dal considerando 15 dell'AI Act, tali caratteristiche possono comprendere, oltre al volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura e la postura, purché siano oggetto di un trattamento tecnico idoneo a consentire l'identificazione della persona.

[5] "*L'articolo 10 della direttiva 2016/680, in combinato disposto con l'articolo 4, paragrafo 1, lettere da a) a c), nonché con l'articolo 8, paragrafi 1 e 2, di tale direttiva, deve essere interpretato nel senso che esso osta a una normativa nazionale che prevede la raccolta sistematica di dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, ai fini della loro registrazione, senza prevedere l'obbligo, per l'autorità competente, di verificare e di dimostrare, da un lato, che tale raccolta è strettamente necessaria per il raggiungimento dei concreti obiettivi perseguiti e, dall'altro, che tali obiettivi non possono essere raggiunti mediante misure che costituiscono un'ingerenza meno grave nei diritti e nelle libertà della persona interessata*".

[6] "*L'articolo 10 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, letto in combinato disposto con l'articolo 4, paragrafo 1, lettere da a) a c), e con l'articolo 8 di tale direttiva, deve essere interpretato nel senso che esso osta a una normativa nazionale che prevede la raccolta sistematica dei dati biometrici di qualsiasi persona nei cui confronti sussistano una o più ragioni plausibili di sospettare che abbia commesso o tentato di commettere un reato, a meno che sia dimostrato, da un lato, che il diritto nazionale definisce le finalità specifiche e concrete perseguite da tale raccolta in modo adeguato e sufficientemente preciso e, dall'altro, che l'autorità competente è tenuta, in ciascun caso*

la raccolta di dati biometrici – nella specie, rilievi segnaletici dattiloscopici e fotografici – può essere sistematica. Occorrono una valutazione individuale, il carattere strettamente necessario e una motivazione specifica caso per caso, con conseguenze anche sulla sanzionabilità del rifiuto. L'argomento *a fortiori* è immediato: **se l'acquisizione biometrica non può essere automatica neppure per i sospettati, la creazione preventiva di *template* riferiti a persone prive di qualsiasi collegamento con un reato è a maggior ragione problematica**. Merita rilievo la circostanza che la vicenda all'origine del rinvio riguardava il fermo di una persona per l'organizzazione di una manifestazione non preavvisata. Qui il collegamento tra acquisizione biometrica e libertà di riunione non è ipotesi di scuola, ma il caso concreto da cui muove la più recente giurisprudenza europea.

Convergono nella stessa direzione la giurisprudenza della Corte EDU in S. and Marper c. Regno Unito (GC, 4 dicembre 2008), sul carattere non neutro della conservazione di identificatori biometrici e sul rischio di assimilare persone non condannate a una popolazione sospetta, e in Glukhin c. Russia (4 luglio 2023), sull'intrusività del riconoscimento facciale e sul suo effetto dissuasivo rispetto alla partecipazione a manifestazioni.

Sebbene la sentenza della Corte di giustizia europea del 16 luglio 2020, nota anche come "Schrems II" (C-311/18) non riguardi specificamente il trattamento di dati biometrici, i principi da essa affermati sono applicabili alla disciplina in esame. La Corte di giustizia ha precisato che una normativa che consenta ingerenze nei diritti garantiti dagli articoli 7 e 8 della Carta deve delimitare in modo chiaro e preciso il potere di trattamento, circoscriverlo allo stretto necessario e predisporre garanzie effettive contro abusi, accessi illegittimi e utilizzazioni ulteriori, tanto più quando il trattamento è automatizzato; devono inoltre esistere mezzi di ricorso effettivi. La generazione preventiva di template biometrici riferiti alla generalità delle persone che accedono a un luogo o a un evento, indipendentemente da qualsiasi collegamento con un reato, presenta i caratteri di un'acquisizione generalizzata e indifferenziata. La sola previsione di un termine di conservazione di sette giorni[7] non esaurisce il giudizio di proporzionalità, poiché l'ingerenza si realizza già con la

---

specifico, a valutare se detta raccolta sia strettamente necessaria alla realizzazione di tali finalità, cosicché una siffatta raccolta non riveste un carattere sistematico.

L'articolo 10 della direttiva 2016/680, letto in combinato disposto con l'articolo 4, paragrafo 4, nonché con l'articolo 54 di tale direttiva, e alla luce dell'articolo 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta a una normativa nazionale che non prevede l'obbligo, per l'autorità competente, di motivare adeguatamente, in ciascun caso specifico, il carattere «strettamente necessario», ai sensi di tale articolo 10, della raccolta dei dati biometrici di qualsiasi persona nei cui confronti sussistano una o più ragioni plausibili di sospettare che abbia commesso o tentato di commettere un reato".

[7] Il comma 6 dell'articolo 10 stabilisce che i dati personali trattati mediante il sistema siano conservati nella banca dati di riferimento per sette giorni dalla raccolta e siano successivamente cancellati in modo automatico. Il comma 8 fa tuttavia salvi i termini generali previsti dall'articolo 10 del DPR 15/2018 per i dati trattati per finalità di polizia. Il coordinamento tra le due disposizioni risulta problematico, perché una lettura estensiva del comma 8 potrebbe consentire di sottrarre al termine di sette giorni tutti o parte dei dati presenti nella banca biometrica, trasferendoli o riclassificandoli in una delle categorie disciplinate dal DPR 15/2018.

Il rischio emerge in modo particolare rispetto alla lettera i) dell'art. 10, co. 3, del DPR 15/2018, che consente di conservare per quindici anni dall'ultimo trattamento i dati relativi ad attività di indagine o di polizia giudiziaria che non abbiano dato luogo a un procedimento penale. Se fosse sufficiente qualificare genericamente la raccolta biometrica come attività investigativa, la banca dati costituita ai sensi dell'articolo 10 potrebbe essere conservata per quindici anni anziché per sette giorni. Inoltre, poiché il termine decorre dall'«ultimo trattamento», successive operazioni di consultazione, aggiornamento o trasferimento potrebbero determinare uno spostamento del dies a quo. Una simile interpretazione priverebbe di effettività il termine speciale del comma 6 e trasformerebbe una banca biometrica temporanea, comprendente prevalentemente persone estranee al reato, in un archivio di polizia di lunga durata.

Una lettura sistematica impone invece di distinguere la banca biometrica complessiva dai singoli dati che, entro il termine di sette giorni, risultino concretamente pertinenti a una determinata indagine. Il termine speciale deve applicarsi all'intero insieme dei dati acquisiti o generati dal sistema per il confronto a posteriori: immagini utilizzate a tale scopo, template biometrici, vettori o rappresentazioni numeriche, dati anagrafici associati, identificativi dei posti, metadati, risultati intermedi, output, duplicati e copie presenti nei diversi ambienti di trattamento. La cancellazione non dovrebbe poter essere elusa mediante il trasferimento dei dati in un diverso archivio, la loro duplicazione o la loro riclassificazione formale.

trasformazione dell'immagine del volto in un identificatore biometrico interrogabile e con la sua eventuale associazione a dati anagrafici e di localizzazione. Occorre pertanto dimostrare perché tale acquisizione preventiva sia strettamente necessaria e perché la finalità non possa essere raggiunta mediante la conservazione temporanea dei filmati e la generazione mirata dei template soltanto dopo il verificarsi di uno specifico fatto di reato.

5.2. Pratiche vietate e la "prossimità"

La disposizione dell'AI Act, già menzionata, vieta i sistemi che creano o ampliano banche dati di riconoscimento facciale mediante *scraping* non mirato (a meno che non si intenda che è "mirato" se fa riferimento ad un unico luogo fisico o a un singolo evento) di immagini facciali provenienti da internet o da riprese di telecamere a circuito chiuso. La costruzione preventiva di una banca di template riferiti alla generalità degli utenti presenta una significativa prossimità funzionale con tale pratica, perché comporta l'estrazione automatica e indifferenziata dei volti da riprese video, e solleva un dubbio interpretativo che lo schema non risolve. Occorre chiarire se l'estrazione automatizzata di immagini facciali dalle riprese effettuate ai varchi, nell'ambito di un sistema appositamente installato, debba essere qualificata come scraping non mirato di riprese CCTV (in ogni caso, la definizione nazionale, con l'aggiunta del requisito della «larga scala», non può restringere una pratica vietata da un regolamento direttamente applicabile).

Il parametro più direttamente pertinente è il considerando 95 dell'AI Act, che richiede che **l'identificazione biometrica a posteriori sia sempre proporzionata, legittima e strettamente necessaria**, e quindi mirata quanto alle persone da identificare, al luogo e all'ambito temporale, fondata su un insieme chiuso di filmati acquisiti legalmente, e mai utilizzata, nel contesto delle attività di contrasto, in modo da condurre a una "sorveglianza indiscriminata". Nello stesso senso, l'art. 26, co. 10, vieta espressamente l'uso non mirato, privo di collegamento con uno specifico reato, procedimento penale, minaccia o ricerca di persona scomparsa. **La generazione preventiva dei *template* previsto dall'art. 10 opera in direzione opposta a ciascuno di questi requisiti: non è mirata (quanto alle persone), precede il fatto di reato e non si fonda su un insieme chiuso di filmati (ma su un flusso continuo di acquisizioni ai varchi)**.

Il considerando si chiude con un'avvertenza che colpisce frontalmente l'architettura dell'articolo 10: "***le condizioni per l'identificazione biometrica remota a posteriori non dovrebbero, in ogni caso, fornire una base per eludere le condizioni del divieto e le rigorose eccezioni per l'identificazione biometrica remota «in tempo reale»***". L'articolo 10, comma 1, dichiara espressamente di costruire il sistema «*con un intervallo di tempo tale da non configurare una identificazione biometrica remota in tempo reale ai sensi del regolamento IA*». In sostanza è la norma stessa a disegnare il proprio funzionamento sul confine temporale che il considerando vieta di utilizzare come scappatoia. Il Governo deve chiarire perché un sistema di acquisizione biometrica continua ai varchi, con confronto soltanto differito, non integri l'elusione che il considerando 95 intende prevenire.

Il rinvio del comma 8 dovrebbe operare soltanto rispetto agli elementi selettivamente estratti dalla banca perché oggettivamente collegati a uno specifico reato o a una determinata attività investigativa. La conservazione ulteriore richiede, pertanto, una finalità di polizia concreta e attuale, la verifica della necessità e pertinenza del singolo dato e un atto che documenti le ragioni dell'acquisizione nel fascicolo o nell'archivio investigativo. Potrebbero essere conservati, ad esempio, il dato relativo alla corrispondenza individuata, le immagini pertinenti e gli elementi necessari alla verifica del risultato; non potrebbe invece essere conservata l'intera banca biometrica delle persone presenti nel luogo o nell'evento per la sola eventualità che possa risultare utile in futuro.

Il comma 6 deve quindi essere inteso come *lex specialis* rispetto ai termini generali del DPR 15/2018: allo scadere dei sette giorni la regola è la cancellazione integrale, mentre la conservazione ulteriore rappresenta un'eccezione circoscritta ai dati individualmente selezionati e acquisiti nell'ambito di una specifica indagine. Dovrebbe essere espressamente vietata qualsiasi forma di conservazione o riclassificazione generalizzata diretta esclusivamente a prolungare la disponibilità della banca dati.

La finalità dichiarata – identificare a posteriori la persona già indiziata – appare perseguibile mediante una plausibile alternativa meno invasiva come, ad esempio, la conservazione temporanea delle sole registrazioni video grezze e la generazione mirata dei template soltanto dopo il verificarsi di uno specifico fatto di reato, dalle sole immagini pertinenti al fatto e riferite alle persone indiziate. Ai sensi dell'articolo 52, paragrafo 1, della Carta, spetta al Governo dimostrare perché tale soluzione non sarebbe sufficiente e perché la generazione preventiva e indifferenziata dei template sia strettamente necessaria. **La comodità operativa del confronto futuro non è un parametro di necessità**.

5.3. Il profilo assembleare

La formula «luoghi o eventi rispetto ai quali sussistono esigenze di ordine e sicurezza pubblica» non esclude manifestazioni, riunioni o iniziative politiche svolte in luoghi o eventi con accesso controllato. Cortei e manifestazioni di strada privi di varchi o titoli di accesso non sembrano invece automaticamente riconducibili al meccanismo di pre-enrollment descritto dal comma 3, che presuppone varchi, scansione dei titoli di accesso e, ove esistente, un posto assegnato.

Il profilo assembleare non si esaurisce tuttavia nel comma 3. I commi 1 e 2 consentono l'integrazione del riconoscimento facciale a posteriori su qualsiasi sistema di videosorveglianza legittimamente installato, quindi anche su piazze, strade e spazi aperti dove le manifestazioni si svolgono. Per tali contesti, privi del meccanismo di pre-enrollment, la base di dati di riferimento per il confronto non è definita, il che riconduce all'indeterminatezza. Ne risultano due scenari distinti, entrambi rilevanti per gli articoli 11 e 12 della Carta dei diritti fondamentali dell'UE e 17 e 21 della Costituzione: la **schedatura biometrica all'ingresso** degli eventi ad accesso controllato, con il suo effetto dissuasivo sulla partecipazione, e **l'identificazione a posteriori dei partecipanti a manifestazioni in spazi aperti tramite la videosorveglianza ordinaria integrata con componenti di intelligenza artificiale**.

Si dovrebbe, eventualmente, prevedere, come detto, che il trattamento automatizzato dei dati biometrici sia consentito esclusivamente dopo la commissione di un fatto di reato, mediante estrazione selettiva dei template dalle sole immagini pertinenti al fatto e riferite alle persone indiziate ai sensi del comma 2. Dovrebbe essere vietata la creazione preventiva di template biometrici delle persone che accedono ai luoghi o agli eventi, nonché l'associazione tra dati biometrici, dati anagrafici e titoli di accesso riferiti a persone diverse da quelle indiziate.

5.4. L'effetto dissuasivo

L'acquisizione dei template biometrici della generalità delle persone che accedono a un luogo o a un evento non incide soltanto sulla protezione dei dati personali ma può modificare preventivamente il comportamento delle persone e, attraverso tale modificazione, **restringere indirettamente l'esercizio delle libertà fondamentali**.

Il fenomeno è generalmente descritto come ***chilling effect*** o effetto dissuasivo. La consapevolezza, o anche il solo ragionevole timore, di essere identificati e registrati può indurre le persone – pur estranee o in alcun modo intenzionate a commettere attività illecite – a rinunciare a comportamenti perfettamente leciti. Si pensi, ad esempio, spinto dalla curiosità di partecipare ad una manifestazione Pride eviti di farlo nel timore di future ed eventuali ritorsioni o, comunque, discriminazioni di qualunque tipo. Non è necessario che i dati siano effettivamente utilizzati contro l'interessato, posto che **l'effetto può derivare dal semplice timore della possibilità di un'utilizzazione futura**, dall'incertezza sulle successive destinazioni dei dati o dalla difficoltà di verificare che la cancellazione sia realmente avvenuta.

La raccolta biometrica presenta un'efficacia dissuasiva potenzialmente maggiore rispetto alla normale videosorveglianza[8]. Una registrazione video documenta la presenza di una persona, ma non necessariamente ne stabilisce automaticamente l'identità. Il template biometrico trasforma invece il volto in un identificatore suscettibile di essere confrontato con altre banche dati e utilizzato per ricostruire presenze, spostamenti e relazioni. Il partecipante non si percepisce più soltanto come ripreso da una telecamera, ma come identificabile e collegabile in modo automatizzato all'evento, in qualsiasi tempo.

La scansione biometrica può trasformare l'accesso a un evento in una scelta condizionata, in cui la persona, per partecipare, per esercitare il suo diritto, deve accettare di entrare in una banca biometrica, sia pure temporanea. Sia pur limitata a sette giorni. Questa condizione può essere particolarmente gravosa quando la partecipazione costituisce esercizio di una libertà costituzionale (si pensi, ad esempio, a congressi o iniziative politiche; riunioni sindacali; manifestazioni religiose; eventi organizzati da associazioni impegnate su temi socialmente controversi; iniziative riguardanti orientamento sessuale, identità di genere, salute, migrazione o appartenenza etnica; incontri di movimenti ambientalisti, pacifisti o di opposizione politica; eventi culturali nei quali la partecipazione esprime, anche implicitamente, convinzioni personali). Si tratta di eventi o situazioni dai quali una determinata informazione può essere associata (in modo più o meno permanente) ad una determinata persona fisica. Quali garanzie vi sono sul fatto che l'associazione tra "aver partecipato a una data manifestazione politica" e una persona determinata, non salti fuori successivamente, quando magari il Paese dovesse essere guidato dallo schieramento politico opposto? Ricordiamo che il tema dei "dati sensibili" si è sviluppato, in Europa, attorno agli anni '50, quando i forni crematori e i lager nazisti erano chiusi da pochi anni e la memoria delle "cause" che determinavano l'internamento erano politiche, religiose, legate alle preferenze sessuali e via discorrendo.

L'effetto dissuasivo non si distribuisce uniformemente. Le persone che ritengono di non avere nulla da temere potrebbero continuare a partecipare; altre, invece, potrebbero percepire un rischio più elevato. Ciò può riguardare appartenenti a minoranze; migranti e persone con una posizione amministrativa precaria; lavoratori che temano conseguenze professionali; dipendenti pubblici o appartenenti a organizzazioni gerarchiche; attivisti, giornalisti e informatori; persone già sottoposte a controlli di polizia, anche senza condanne; soggetti che temano discriminazioni familiari, sociali o economiche.

Le voci più vulnerabili o dissenzienti rischiano così di essere progressivamente espulse dallo spazio pubblico. Il risultato può essere paradossale posto che una misura presentata come neutrale produce una selezione sociale e politica dei partecipanti senza che sia adottato alcun formale provvedimento limitativo.

L'articolo 10 presenta un ulteriore significato simbolico. I dati biometrici vengono acquisiti prima che sia stato commesso il reato e quando ancora non esiste alcun indiziato. Tutti i partecipanti

[8] È anche vero che lo Schema non introduce un divieto generale di trucco, abbigliamento o accessori volti a ridurre l'efficacia di un algoritmo biometrico di riconoscimento facciale. L'AI Act non impone alle persone di rendersi biometricamente leggibili. Residua l'articolo 5 della legge n. 152 del 1975, che vieta in luogo pubblico o aperto al pubblico, senza giustificato motivo, caschi o altri mezzi atti a rendere difficoltoso il riconoscimento, con disciplina più rigorosa durante le manifestazioni. Tuttavia, l'applicazione a questo caso dipende da caratteristiche e contesto. Ostacolare uno specifico modello e rendere la persona difficilmente riconoscibile da un essere umano non sono necessariamente la stessa cosa. Una lettura estensiva *in malam partem* sarebbe problematica e contraria. Si veda anche UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests, 2024, in cui espressamente si dice: "*Participants' tactics intended to preserve their anonymity, such as measures for encryption or wearing masks can be important to ensure the enjoyment of the right to peaceful assembly and should not be regarded as inherently suspicious or as a justification for the use of surveillance tactics*" (le modalità adottate dai partecipanti per preservare il proprio anonimato, quali il ricorso a strumenti di cifratura o l'uso di maschere, possono essere importanti per garantire l'esercizio del diritto di riunione pacifica e non dovrebbero essere considerate intrinsecamente sospette né idonee, di per sé, a giustificare il ricorso a tecniche di sorveglianza).

vengono inseriti nell'archivio perché uno di loro potrebbe, in futuro, diventare la persona da identificare. Si determina così un mutamento del rapporto tra cittadino e autorità in cui la presenza a un evento non è più soltanto esercizio di una libertà, ma diventa preventivamente un dato di polizia. La persona pacifica viene trattata tecnicamente nello stesso modo del futuro sospettato, almeno nella fase di acquisizione e memorizzazione. La normalizzazione di questa pratica può gradualmente rendere socialmente accettabile l'idea che l'accesso a uno spazio collettivo comporti necessariamente la rinuncia all'anonimato. Il rischio non è soltanto la sorveglianza del singolo evento, ma la costruzione di una cultura della sorveglianza nella quale essere identificati diventa il prezzo ordinario della partecipazione sociale.

La raccolta biometrica può diminuire la fiducia tanto nelle istituzioni quanto negli organizzatori privati degli eventi. Il cittadino può non essere in grado di sapere chi abbia materialmente accesso ai template biometrici; se i dati siano stati realmente cancellati dopo sette giorni; se siano state prodotte copie; se i risultati siano confluiti in archivi di polizia; se la presenza possa essere successivamente ricostruita; se il sistema abbia prodotto corrispondenze errate; se i dati possano essere utilizzati per finalità diverse.

La sola incertezza può essere sufficiente a produrre autocensura. La garanzia formale della cancellazione dopo sette giorni non elimina necessariamente l'effetto dissuasivo, soprattutto se la legge non vieta espressamente l'estrazione e il trasferimento dei dati in altri archivi prima della scadenza.

L'ingerenza può propagarsi dalla protezione dei dati personali a un insieme più ampio di diritti quali libertà personale e sviluppo della personalità, ai sensi degli articoli 2 e 13 della Costituzione; libertà di riunione, ai sensi dell'articolo 17 della Costituzione; libertà religiosa, ai sensi dell'articolo 19; libertà di manifestazione del pensiero, ai sensi dell'articolo 21; libertà di associazione, partecipazione politica e libertà sindacale, ai sensi degli articoli 18, 39 e 49; vita privata, protezione dei dati, libertà di espressione e libertà di riunione e associazione, ai sensi degli articoli 7, 8, 11 e 12 della Carta dei diritti fondamentali dell'Unione europea; diritti garantiti dagli articoli 8, 10 e 11 CEDU.

Il problema non consiste soltanto nel chiedere se il riconoscimento venga attivato dopo un reato. Occorre chiedere se sia costituzionalmente proporzionato acquisire preventivamente i template biometrici di tutti i partecipanti per rendere possibile quella futura ricerca. La valutazione di proporzionalità dovrebbe comprendere anche gli effetti collettivi e comportamentali della misura quante persone rinunceranno a partecipare a un evento politico, sindacale, religioso o associativo sapendo che il loro volto sarà trasformato in un template biometrico, collegato alla loro identità e conservato in una banca dati gestita dalle autorità di pubblica sicurezza?

5.5. Necessità di coordinamento con l'articolo 9 del DL 139 del 2021

Il vigente articolo 9, comma 9, sospende fino all'entrata in vigore di una disciplina legislativa della materia, e comunque non oltre il 31 dicembre 2027, installazione e uso in luoghi pubblici o aperti al pubblico di videosorveglianza con riconoscimento facciale da parte di autorità pubbliche o privati. Il comma 12 esclude però dalla sospensione i trattamenti delle autorità competenti per prevenzione e repressione dei reati, subordinandoli, salvo le funzioni giudiziarie, al parere favorevole del Garante.

Lo Schema produce quindi un cambiamento rilevante ma non una liberalizzazione generale. Per la polizia **passa da una moratoria con eccezione fondata sul parere favorevole del Garante a una disciplina positiva e permanente (**pre-enrollment biometrico degli accessi, uso a posteriori dopo un reato, banca locale, collegamento con dati anagrafici e posto, sette giorni, titolarità ministeriale e possibile finanziamento o manutenzione privata). Al tempo stesso **introduce limiti più dettagliati, ma sostituisce l'espresso "parere favorevole" con DPIA e consultazione preventiva**

e consente una valutazione unica per sistemi analoghi. Sotto questo profilo la garanzia può risultare attenuata.

Lo Schema non abroga né coordina espressamente il DL 139/2021. Poiché la moratoria cessa all'entrata in vigore di una "disciplina legislativa della materia", vi è il rischio che una disciplina riferita alle Forze di polizia venga interpretata come termine della sospensione anche per sistemi privati, benché lo schema non regoli il loro uso autonomo. Deve essere chiarito che l'entrata in vigore dell'articolo 10 fa cessare la sospensione soltanto per i trattamenti espressamente disciplinati dal decreto e non autorizza sistemi privati di riconoscimento facciale. Per ogni altro trattamento pubblico o privato restano fermi il comma 9 e la scadenza del 31 dicembre 2027, salvo una distinta disciplina legislativa.

Le disposizioni del presente articolo costituiscono disciplina legislativa esclusivamente per i trattamenti effettuati dal Ministero dell'interno - Dipartimento della pubblica sicurezza nei casi e alle condizioni qui previsti. Esse non autorizzano l'accesso o l'utilizzo dei dati biometrici da parte dei soggetti privati di cui al comma 12 e non determinano la cessazione della sospensione prevista dall'articolo 9, comma 9, del decreto-legge n. 139 del 2021 per trattamenti diversi.

5.6. Soggetti privati e accesso ai dati biometrici dell'articolo 10

L'articolo 10, comma 12, consente a gestori dei luoghi, organizzatori, promotori o soggetti che dispongono delle strutture di provvedere all'installazione e alla manutenzione. Il sistema è però concesso in comodato gratuito alla questura, che ne acquisisce la "completa ed esclusiva disponibilità"; il titolare del trattamento è il Ministero dell'interno e il comma 7 limita accessi e operazioni alle persone autorizzate.

Queste **disposizioni non attribuiscono ai privati un autonomo diritto di consultare, estrarre o utilizzare la banca biometrica**. L'accesso deve essere riservato alle Forze di polizia per le finalità e nei casi dell'articolo 10. Il gestore può trattare ordinariamente dati di biglietteria sulla base del proprio titolo, ma non può per ciò solo accedere al collegamento fra identità, posto e template biometrico.

Resta però una lacuna, posto che "persone autorizzate" non significa necessariamente personale di polizia e la manutenzione può richiedere privilegi tecnici. Occorre stabilire che i privati non accedano ai dati in chiaro; ogni intervento eccezionale deve avvenire quale responsabile o soggetto autorizzato, su istruzioni documentate del Ministero, con privilegio minimo, durata limitata, supervisione della questura, log immutabili, divieto di accesso remoto ordinario, copia, estrazione, riuso o addestramento e cancellazione dei dati tecnici temporanei. L'architettura dovrebbe separare fisicamente o crittograficamente i dati di biglietteria dalla banca biometrica.

6. Ulteriori rischi tecnici

La costituzione di una banca dati biometrica da parte delle Forze di polizia presenta rischi particolarmente elevati, sia per la natura dei dati trattati sia per la capacità dei sistemi di stabilire collegamenti tra persone, luoghi, eventi e attività investigative.

Diversamente da una password, caratteristiche quali il volto o le impronte digitali non sono normalmente sostituibili in caso di compromissione. La **sottrazione dei relativi template** può quindi produrre conseguenze durevoli, agevolando correlazioni tra archivi diversi, attacchi di impersonificazione o di presentazione e ulteriori forme di sorveglianza. Il rischio aumenta con la centralizzazione delle informazioni, la moltiplicazione delle copie, l'interoperabilità con altri sistemi e il prolungamento dei tempi di conservazione.

Un primo profilo critico concerne **l'affidabilità del confronto biometrico**. Un falso positivo può associare una persona estranea a qualsiasi condotta illecita a un determinato luogo o evento, con

possibili conseguenze investigative e reputazionali. L'indicazione di un tasso medio di accuratezza non è sufficiente, poiché le prestazioni possono variare in relazione al gruppo demografico, alle condizioni di illuminazione, all'angolazione del volto, alla distanza, al dispositivo di acquisizione, alla qualità del campione e al tempo trascorso tra le immagini confrontate. Nelle ricerche uno-a-molti, inoltre, anche un tasso di errore apparentemente ridotto può generare un numero significativo di corrispondenze inesatte quando il confronto riguarda una popolazione numerosa. È pertanto necessario che ogni risultato sia sottoposto a verifica umana qualificata e sia considerato come un'indicazione da corroborare, non come una prova autosufficiente dell'identità.

L'affidabilità deve essere valutata anche nel tempo. Gli aggiornamenti del modello, la modifica delle soglie di corrispondenza e il progressivo deterioramento delle prestazioni possono determinare risultati differenti a partire dagli stessi dati. Ogni operazione dovrebbe quindi essere tecnicamente ricostruibile mediante la conservazione selettiva della versione del modello, dei parametri e della soglia utilizzati, del campione sottoposto a confronto, dell'insieme di riferimento, del punteggio prodotto e dei log delle operazioni. Senza tali elementi non sarebbe possibile verificare il funzionamento del sistema, ripetere il confronto o accertare l'incidenza di errori, bias e modifiche intervenute successivamente.

Alla perdita di riservatezza si aggiungono i **rischi per l'integrità della banca dati e del sistema**. Il data poisoning può contaminare i dati di addestramento, aggiornamento o riferimento, mentre immagini manipolate, template artefatti e tecniche avversariali possono alterare il confronto o provocare corrispondenze erronee. Qualora il sistema biometrico sia integrato con componenti generative o agentiche che acquisiscono documenti o istruzioni da fonti esterne, deve essere considerato anche il rischio di prompt injection. La sicurezza richiede pertanto la verifica della provenienza e dell'integrità dei dati, la firma e il versionamento dei modelli, l'isolamento delle fonti non affidabili, test avversariali periodici, la separazione degli ambienti e dei privilegi e la possibilità di ricostruire ogni fase del trattamento.

La banca dati deve inoltre essere **protetta tanto dalle intrusioni esterne quanto dagli accessi abusivi interni**. Sono necessarie la cifratura dei dati sia durante la trasmissione sia durante la conservazione, la segregazione logica degli archivi, una gestione rigorosa e separata delle chiavi crittografiche, l'autenticazione forte, l'applicazione del principio del minimo privilegio e un controllo rafforzato sugli amministratori di sistema. Gli accessi e le operazioni devono essere registrati in log non modificabili o comunque idonei a rendere rilevabili le alterazioni. Occorre, inoltre, mantenere un inventario completo delle repliche, delle esportazioni e delle copie di sicurezza, affinché la cancellazione alla scadenza del termine previsto sia effettiva e sincronizzata in tutti gli ambienti di trattamento.

La sicurezza tecnica è infine strettamente collegata alle **garanzie del contraddittorio e del giusto processo di cui all'articolo 111 della Costituzione**. Un risultato biometrico non è effettivamente contestabile se la difesa non può conoscere, almeno mediante modalità di accesso protetto, il dato originario, la composizione dell'insieme di confronto, la soglia applicata, la versione del modello, il punteggio prodotto e i log necessari alla verifica. Le esigenze di sicurezza e la tutela del segreto commerciale possono giustificare limitazioni e cautele nell'accesso, ma non possono rendere l'output tecnicamente incontestabile. L'impiego processuale di risultati non riproducibili o privi degli elementi indispensabili alla verifica dovrebbe pertanto essere escluso, salvo che sia assicurato un mezzo equivalente ed effettivo di contestazione.

La conservazione degli elementi necessari al contraddittorio deve, tuttavia, essere coordinata con i principi di minimizzazione e limitazione della conservazione. Quando un risultato sia concretamente utilizzato in un'indagine o in un procedimento, possono essere selettivamente preservati i dati indispensabili a verificarlo e contestarlo. Ciò non giustifica la conservazione dell'intera banca biometrica sulla base della mera possibilità che possa risultare utile in futuro. La sicurezza del sistema richiede, in definitiva, non soltanto misure contro gli accessi abusivi e le

alterazioni, ma anche una rigorosa delimitazione dei dati raccolti, delle persone autorizzate, delle finalità perseguite e della durata effettiva della conservazione.

Cagliari-Roma, 22 luglio 2026

Avv. Francesco Paolo Micozzi