

UTILIZZO DELL'A.I. NEL RICONOSCIMENTO FACCIALE PER FINI DI POLIZIA PROSPETTIVE E PROBLEMATICHE GIURIDICHE

Il decreto legislativo approvato dal governo il 4 agosto 2026, in base a legge delega del Parlamento 132/ 2025 per l'utilizzo dell'intelligenza artificiale da parte delle forze dell'ordine, disciplina la complessa materia del riconoscimento facciale.

In particolare, tale procedura avviene tramite software che analizzano l'immagine di un volto e la traducono in una serie di numeri che variano in base a caratteristiche fisiche come la distanza fra gli occhi, la forma della mandibola o la posizione degli zigomi, da raffrontare con immagini aventi requisiti simili precedentemente archiviate.

Naturalmente, come sempre avviene quando si parla di questo tipo di attività di polizia occorre distinguere fra attività preventiva ed attività giudiziaria (ossia ante delictum e post delictum).

I precedenti utilizzi di questo tipo di tecnologia in termini di prevenzione possono essere annoverati fin dal 2015, quando la struttura presso il sito di Rho Fiera (MI) destinato ad ospitare per sei mesi l'esposizione internazionale del cibo denominata Expo, venne resa con apposito decreto del governo sito strategico e munita appunto di un sistema di videosorveglianza TVCC collegato a database delle Forze dell'Ordine contenenti le foto di sospetti terroristi a livello internazionale.

Successivamente, superato quasi il prolungato allarme terrorismo nel nostro Paese derivante dalla minaccia dell'Isis al mondo occidentale, le pressanti esigenze di tutela della sicurezza pubblica - tema importante per la collettività a fronte della recrudescenza di fenomeni criminali quali aggressioni, reati predatori ed incidenti violenti in occasioni di manifestazioni pubbliche - ma anche in considerazione della gestione di grandi eventi che il nostro Paese ha ospitato di recente, quali il Giubileo della speranza nel 2025, il vertice dei primi ministri della Ue e quello per la soluzione della crisi tra Palestina ed Israele nel 2026, hanno indotto il governo ad emanare tutta una serie di provvedimenti d'urgenza in materia, poi convertiti in legge, sia pur con alcune modifiche da parte del Parlamento.

Rimane comunque di primaria importanza la normativa di cui ci accingiamo a parlare, dato che affronta in termini generali il tema dell'utilizzo di tecnologie autonome per finalità di controllo, i cui principi fondamentali sono stati già fissati a livello europeo dall'AI Act del 2024, recepito in Italia appunto con la legge delega del 2025 citata in precedenza.

Va detto innanzitutto che, a livello sperimentale, già dal 2016 in Italia il Garante per la privacy ha autorizzato l'installazione presso l'impianto di videosorveglianza dello stadio Olimpico di Roma della tecnologia sviluppata dalla società Reco 3.26 che acquisisce il volto dello spettatore ai tornelli di ingresso e lo associa al nominativo del biglietto in funzione di verifica di eventuale Daspo a carico. Tuttavia la gestione di tutta la procedura avviene esclusivamente sotto il controllo della polizia, con cancellazione automatica inoltre delle immagini, salvo specifiche esigenze investigative, entro i successivi 7 giorni.

Le modalità di riconoscimento delle immagini sono simili a quelle del noto SARI (Sistema Automatico Riconoscimento Immagini) utilizzato dalla Polizia di Stato sia per finalità preventive mediante SARI Real Time per l'esame dei volti tramite telecamere stradali, sia per finalità investigative, al pari di altre importanti banche dati interforze ormai esistenti da tempo quali AFIS per le impronte digitali e IBIS per i rilievi balistici, oltre alla famosa banca dati nazionale del DNA, gestita d'intesa tra i Ministeri dell'Interno e della Giustizia, contenente il profilo genetico dei soggetti arrestati o detenuti esclusivamente per gravi reati predatori o contro la persona.

Tuttavia il vero punto critico, sotto il profilo giuridico, dell'applicazione della tecnologia del riconoscimento che il decreto legislativo del 4 agosto ha inteso sanare, risiede in particolare nell'applicazione degli articoli 8 e 10 del citato AI Act elaborato dall'Unione Europea.

L'articolo 8 infatti riguarda l'identificazione in tempo reale in luoghi pubblici o aperti al pubblico che è ammessa esclusivamente per:

- Prevenire una minaccia grave e specifica, quale un attacco terroristico, per la vita e l'incolumità delle persone
- Rintracciare persone scomparse o vittime di tratta di essere umani o sfruttamento sessuale
-

L'articolo 10 dell'AI Act disciplina invece la governance e la gestione dei dati imponendo sia l'utilizzo di dataset di addestramento (convalida e prova di qualità: training, validation e testing) per evitare i cosiddetti bias che possono generare il problema dei "falsi positivi" nel caso di comparazione fra immagini raccolte dal vivo e quelle archiviate, sia di criteri asettici di raccolta delle immagini nei database (quindi solo quelle certificate ossia provenienti da siti web istituzionali o ufficiali e non ad esempio liberamente attinte dal web o dai social) al fine di garantire correttezza e trasparenza a tutto il sistema.

Uno studio del 2019 sugli algoritmi ha rilevato errori 10 volte più frequenti nel riconoscimento facciale per i volti asiatici ed africani, soprattutto se da lontano e in movimento, mentre per i caucasici sono esatti nel 99% dei casi, ma solo nel 34% per le donne di colore.

Per quanto riguarda invece il riconoscimento facciale dopo la commissione di un reato (post delictum) il medesimo dovrà essere comunicato dagli ufficiali di P.G. precedenti entro 24 ore al P.M. il quale lo potrà autorizzare entro le successive 24 ore.

Si può quindi sostenere in sintesi che il sistema complessivo in base alle disposizioni emesse dal governo a seguito di un lungo lavoro di studio per armonizzare la complessa materia, si basa su di un regime di visione da parte delle forze dell'ordine - ufficiali ed agenti di P.S e di P.G. - delle immagini in luogo pubblico o aperto al pubblico anche massiva per finalità preventive (con distruzione successiva delle medesime dopo 7 giorni) mentre per il riconoscimento facciale vero e proprio, basato cioè su dati biometrici, sia comunque necessaria l'autorizzazione della A.G. competente, sia pur entro i termini temporali citati.'

E' naturalmente in questo senso necessaria anche una specifica formazione da parte delle forze dell'ordine per utilizzare questo tipo di tecnologia.

Appare superfluo quindi aggiungere come ormai la vera partita, anche in termini di tutela della tanto invocata sicurezza, si giochi tutta sulla ricerca di un punto di equilibrio fra le enormi possibilità offerte dalla tecnologia e il principio del rispetto della privacy delle persone, che può essere limitato solo a fronte di comprovate ragioni, riconosciute da un'autorità terza come quella giudiziaria e secondo criteri eticamente condivisibili.

Filippo Guglielmino Dirig. Gen. a.r. della Polizia di Stato