Il Riformista
20-GIU-2026
da pag. 5 / foglio 1

Sorveglianza di massa: c'è il rischio di un "grande fratello" in divisa

■ **Giorgio Altieri**

Lo schema di decreto legislativo uscito dal Consiglio dei Ministri del 10 giugno 2026, se verrà approvato in via definitiva, introdurrà il riconoscimento biometrico in tempo reale nelle indagini penali.

Si spalancano le porte a un controllo sistematico della popolazione.

Un provvedimento presentato come necessaria attuazione dell'AI Act europeo (Reg. UE 2024/1689) e della legge delega 132/2025, rivela al suo interno, quasi in sordina, una norma altamente critica nel rapporto tra Stato e cittadini: il nuovo articolo 359-ter del codice di procedura penale.

Nell'ambito delle indagini penali, introduce la facoltà per il pubblico ministero di richiedere al giudice per le indagini preliminari l'autorizzazione all'identificazione e localizzazione di persone tramite sistemi di IA per il riconoscimento biometrico remoto in tempo reale. In altri termini: telecamere puntate su spazi pubblici, algoritmi che leggono i volti, banche dati che archiviano e confrontano.

Nel procedimento penale, il giudice per le indagini preliminari sarebbe competente all'autorizzazione per l'impiego in tempo reale del riconoscimento biometrico in relazione a reati di particolare gravità: latitanti, vittime di sottrazione, tratta o sfruttamento sessuale. Sul versante preventivo, è invece il pubblico ministero a fungere da presidio autorizzativo, con un abbassamento della soglia di garanzia giurisdizionale che non può passare inosservata.

Il governo ha cercato di circondare la misura di salvaguardie: l'autorizzazione sarebbe temporanea e delimitata, massimo quindici giorni con eventuali proroghe motivate. Le richieste dovranno dettagliare finalità, durata, area territoriale, persone interessate, banche dati e tecnologie impiegate. I dati biometrici raccolti dovranno essere cancellati automaticamente dopo sette giorni.

Chi ha dimestichezza con il diritto penale sa come gli "strumenti di eccezione" si trasformino, nel tempo, in prassi ordinaria.

Il punto nodale non è chi viene identificato ai fini delle indagini. È chi viene scansionato nel mezzo. Il punto sensibile riguarda la collettività dei volti attraversati dal sistema: l'interferenza costituzionale colpisce anche chi riceve solo un istante di attenzione algoritmica, perché il controllo biometrico trasforma la presenza pubblica in dato da esaminare.

Chiunque transiti in un'area soggetta a sorveglianza biometrica attiva ha il proprio volto acquisito, confrontato, temporaneamente memorizzato, anche se non ha commesso nulla.

Sette giorni per la cancellazione dei dati biometrici è un lasso di tempo più che sufficiente per costruire profili di mobilità, associazioni tra persone, abitudini e frequentazioni. I dati biometrici, per loro natura, non sono neutrali: rivelano identità, stato di salute, etnia, espressioni emotive.

L'articolo 15 della Costituzione tutela la libertà e la segretezza di ogni forma di comunicazione: i dati biometrici, trasmessi silenziosamente dai nostri corpi ai server delle forze dell'ordine, meritano analoga protezione. L'articolo 2, poi, tutela i diritti inviolabili della persona e non conosce eccezioni "temporanee".

Lo stesso AI Act tratta il riconoscimento biometrico in tempo reale in spazi pubblici come uno strumento ad altissimo rischio, soggetto a divieto generale con deroghe tassative e molto stringenti.

Un sistema più accettabile dovrebbe prevedere: il divieto assoluto di raccolta biometrica in occasione di manifestazioni, assemblee e attività di esercizio di diritti costituzionali; la cancellazione in tempo reale dei dati delle persone non corrispondenti al soggetto ricercato (non dopo sette giorni); audit periodici del Garante per la protezione dei dati personali con poteri effettivi di intervento anche sulle Autorità di pubblica sicurezza.