

Roma, 12 marzo 2026 – Nelle scorse settimane, il Parlamento ha approvato definitivamente la legge di conversione del decreto Milleproroghe, adottando anche un emendamento che estende fino al **31 dicembre 2027** la moratoria sull'installazione e sull'utilizzo di sistemi di **riconoscimento facciale nei luoghi pubblici o aperti al pubblico**.

L'impegno della **Rete Diritti Umani Digitali** è stato fondamentale nel raggiungimento di questo obiettivo, che garantirà maggiori tutele dei diritti alla privacy, alla libertà di espressione e alla non discriminazione. Diritti posti particolarmente a rischio dall'utilizzo di sistemi di riconoscimento facciale e sorveglianza biometrica, che per loro natura sono caratterizzati da forte pervasività ed errori sistemici.

Grazie alla misura adottata dal Parlamento, su proposta dell'On. Magi di +Europa, l'installazione e l'utilizzo di impianti di videosorveglianza che impiegano sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici, resterà sospesa fino all'adozione di una disciplina legislativa organica della materia, che dovrà essere adottata nel nome del principio di proporzionalità sancito dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea.

In concreto, grazie alla moratoria:

- **soggetti privati**, come il proprietario di un cinema o di un supermercato, **non potranno installare sistemi di videosorveglianza basati sul riconoscimento biometrico** nei luoghi accessibili al pubblico;
- le tecnologie in esame potranno essere installate e impiegate dalle **autorità competenti a fini di prevenzione e repressione** dei reati o di esecuzione di sanzioni penali, **solo in presenza del parere favorevole del Garante**. Il parere non sarà, invece, necessario, in caso di utilizzo **da parte dell'autorità giudiziaria** nell'esercizio delle funzioni giurisdizionali (vedi indagini polizia giudiziaria).

Senza questo intervento normativo, la moratoria in oggetto sarebbe scaduta il **31 dicembre 2025**, eliminando importanti tutele rispetto all'implementazione e all'utilizzo di tali sistemi e lasciando la disciplina della materia solo al quadro generale del GDPR e alla normativa ordinaria in materia di protezione dei dati personali. Una situazione che avrebbe rappresentato **un significativo passo indietro nelle garanzie**, soprattutto in una fase di evoluzione della normativa, e che pertanto aveva suscitato forte preoccupazione nella **Rete per i Diritti Umani Digitali**, la coalizione di organizzazioni della società civile impegnate sul tema dell'impatto delle nuove tecnologie – e in particolare dell'intelligenza artificiale – sui diritti umani, composta da **The Good Lobby, Amnesty International Italia, Privacy Network, Strali, Period Think Tank e Hermes Center**.

É opportuno chiarire che la questione riguarda la sola **identificazione biometrica a posteriori** su materiale video già registrato — che è, allo stato attuale, l'unica forma utilizzabile in Italia. Il **riconoscimento biometrico in tempo reale**, invece, rientra tra le pratiche soggette a un divieto europeo entrato in vigore il **2 febbraio**, con alcune eccezioni limitate per le forze di polizia. La normativa europea stabilisce tuttavia che, proprio per garantire adeguate tutele nell'uso di strumenti così invasivi, tali eccezioni possano essere applicate solo previa adozione di una **legge nazionale** che istituisca un sistema di autorizzazione e individui le autorità competenti a concederla. Poiché l'Italia non ha ancora predisposto questo quadro normativo, non dovrebbero essere operativi sistemi di riconoscimento biometrico in tempo reale neppure da parte delle forze dell'ordine.

Rimane, però, molto difficile ottenere informazioni sugli usi attuali del riconoscimento biometrico da parte delle forze di polizia — sia in tempo reale che a posteriori — e quindi verificare il rispetto del divieto, a causa dell'elevato livello di opacità e del ricorso al **segreto di Stato**, più volte opposto alle richieste di accesso civico generalizzato presentate dalla Rete.

In particolare, per quanto riguarda l'**identificazione biometrica a posteriori, interessata dalla moratoria**, il quadro europeo non è ancora pienamente operativo e alcune disposizioni dell'**AI Act** non sono ancora entrate in funzione. Ad ogni modo, va sottolineato che è lo stesso GDPR a contenere garanzie volte a limitare possibili abusi di potere: in caso di trattamento di dati biometrici, infatti, richiede una valutazione d'impatto sui diritti fondamentali e l'eventuale coinvolgimento di un'autorità competente, come il Garante o l'autorità giudiziaria. Tuttavia, in assenza di una disciplina specifica come quella prevista dalla moratoria, non si sarebbe raggiunto lo stesso livello di tutela.

“La Rete per i Diritti Umani Digitali ha costantemente ribadito la propria posizione a favore di un divieto totale dell'utilizzo dei sistemi di riconoscimento biometrico, sia in tempo reale sia a posteriori, ritenendo che tali tecnologie presentino gravi criticità in termini di fallibilità e opacità e possano, di conseguenza, generare ingiustizie, violazioni dei diritti fondamentali e abilitare pratiche di sorveglianza indiscriminata. Continueremo a mobilitarci per ottenere un divieto assoluto dell'utilizzo di sistemi di riconoscimento biometrico, ma nel frattempo accogliamo con favore l'estensione della moratoria fino al 2027, in considerazione della sua capacità di garantire un livello minimo di tutela dei diritti fondamentali” – afferma **Laura Ferrari, The Good Lobby, in rappresentanza della Rete**.

-