



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy

Non è favorevole il parere del Garante per la protezione dei dati personali sull'utilizzo del sistema Sari Real Time da parte del Ministero dell'interno. Il sistema, oltre ad essere privo di una base giuridica che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, realizzerebbe per come è progettato una forma di sorveglianza indiscriminata/di massa.

Il sistema sottoposto all'esame dell'Autorità e non ancora attivo consente, attraverso una serie di telecamere installate in una determinata area geografica, di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (denominata "watch-list"), che può contenere fino a 10.000 volti.

Qualora, attraverso un algoritmo di riconoscimento facciale venga riscontrata una corrispondenza tra un volto presente nella watch-list ed un volto ripreso da una delle telecamere, il sistema è in grado di generare un alert che richiama l'attenzione degli operatori delle Forze di Polizia. Il sistema, progettato e sviluppato come soluzione mobile, può essere installato direttamente presso il luogo ove sorge l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica, o in relazione a specifiche esigenze di Polizia Giudiziaria. Il sistema consente, inoltre, di registrare le immagini riprese dalle telecamere, svolgendo una funzione di videosorveglianza.

Il Garante, in linea con quanto stabilito dal Consiglio d'Europa, ritiene di estrema delicatezza l'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione dei reati. Va considerato, in particolare, - afferma il Garante - che Sari Real Time realizzerebbe un trattamento automatizzato su larga scala che può riguardare anche persone presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia. Ed anche se nella valutazione di impatto presentata il Ministero spiega che le immagini verrebbero immediatamente cancellate, l'identificazione di una persona sarebbe realizzata attraverso il trattamento dei dati biometrici di tutti coloro che sono presenti nello spazio monitorato, allo scopo di generare modelli confrontabili con quelli dei soggetti inclusi nella "watch-list". Si determinerebbe così una evoluzione della natura stessa dell'attività di sorveglianza, che segnerebbe un passaggio dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale.

È proprio a causa della loro forte interferenza con la vita privata delle persone che la normativa in materia di privacy stabilisce rigorose cautele per i trattamenti di dati biometrici e per particolari categorie di dati (ad esempio, quelli idonei a rivelare opinioni politiche, sindacali, religiose, orientamenti sessuali), i quali devono trovare giustificazione in una adeguata base normativa. Base normativa che non è stata rinvenuta nella documentazione fornita dal Ministero dell'interno.

Secondo il Garante una base normativa adeguata dovrebbe tener conto di tutti i diritti e le libertà coinvolte e definire le situazioni in cui è possibile l'uso di tali sistemi, senza lasciare una discrezionalità ampia a chi lo utilizza. Ciò vale anche per aspetti fondamentali dell'impiego della tecnica di riconoscimento facciale, come i criteri di individuazione dei soggetti che possono essere inseriti nella watchlist, le conseguenze in caso di falsi positivi o la piena adeguatezza del sistema nei confronti di persone appartenenti a minoranze etniche.

Roma, 16 aprile 2021