# Parere sul sistema Sari Real Time - 25 marzo 2021 [9575877]

[doc. web n. 9575877]

**Parere sul sistema Sari Real Time - 25 marzo 2021**

Registro dei provvedimenti
n. 127 del 25 marzo 2021

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, l'avv. Guido Scorza e il dott. Agostino Ghiglia, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito: "RGPD");

VISTO il decreto legislativo 30 giugno 2003, n.196, recante il Codice in materia di protezione dei dati personali, integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101 (di seguito: "Codice");

VISTA la 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;

VISTO il decreto legislativo 18 maggio 2018, n. 51, recante l'Attuazione della direttiva (UE) 2016/680 (di seguito: "Decreto");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali (di seguito: "Regolamento 1/2019");

ESAMINATO il sistema Sari Real Time e la relativa valutazione preventiva di impatto sulla protezione dei dati personali;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali;

Relatore l'avv. Guido Scorza;

**PREMESSO**

Il Ministero dell'Interno-Dipartimento della pubblica sicurezza ha inviato a questa Autorità la descrizione del sistema SARI Real Time, corredata di una bozza di valutazione di impatto, redatta ai sensi dell'art. 23 del Decreto, nella quale sono integrate la descrizione dell'architettura di sistema e le relative istruzioni operative.

Dalla documentazione prodotta risulta che il sistema SARI Real-time – allo stato degli atti non ancora attivo - consente, attraverso una serie di telecamere installate in un'area geografica predeterminata e delimitata, di analizzare in tempo reale i volti dei soggetti ivi ripresi, confrontandoli con una banca dati predefinita per lo specifico servizio (denominata "watch-list"), la cui grandezza è di massimo 10.000 volti.

Ove venga riscontrata, attraverso un algoritmo di riconoscimento facciale, 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.

Il sistema consente, inoltre, di registrare i flussi video delle telecamere “fungendo, in tal senso, quale attività di video sorveglianza.”.

Il sistema è stato progettato e sviluppato come soluzione mobile tale da poter essere installata direttamente presso il sito ove sorge l'esigenza di disporre di una tecnologia di riconoscimento facciale in grado di coadiuvare le Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica, oppure in relazione a specifiche esigenze di Polizia Giudiziaria.

Nella valutazione di impatto vengono richiamate, a vario titolo, diverse disposizioni normative, ritenute conferenti al fine dell’inquadramento e del fondamento giuridico del trattamento in argomento e, segnatamente: alcuni articoli del codice di procedura penale (agli artt. 134 c.4, 234, 266, 431 c.1 lett. b, oltre gli artt. 55, 348, 354 e 370 sull’attività di polizia giudiziaria); il decreto del Ministro dell'Interno del 24 maggio 2017 (Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell’esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari); l'art. 1 del Testo unico delle leggi di pubblica sicurezza (T.U.L.P.S.), approvato con regio decreto 18 giugno 1931, n. 773; la legge 1° aprile 1981, n. 121, sull'ordinamento dell'Amministrazione della pubblica sicurezza; il DPR n. 15 del 15 gennaio 2018, in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato per le finalità di polizia; il d. lgs 51/2018.

**OSSERVA**

1) L’utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione di reati è oggetto di grande attenzione, come indicano, da ultimo, le linee guida del Consiglio d’Europa, che segnalano l’intrusività che esso comporta per il diritto alla vita privata e alla dignità delle persone, unitamente al rischio di ripercussioni negative su altri diritti umani e sulle libertà fondamentali.

Le linee guida richiamano i legislatori e quanti hanno responsabilità di adottare decisioni a stabilire norme specifiche per il trattamento di dati biometrici mediante tecnologie di riconoscimento facciale a fini di contrasto, per garantire che il loro impiego sia strettamente necessario e proporzionato alle finalità e siano prescritte le necessarie garanzie.

Il trattamento di immagini volte ad identificare le persone nel contesto pubblico è quindi di estrema delicatezza ed è perciò necessaria una valutazione d’insieme, per evitare che singole iniziative, sommate tra loro, definendo un nuovo modello di sorveglianza introducano, di fatto, un cambiamento non reversibile nel rapporto tra individuo ed autorità.

Occorre in particolare considerare che il sistema in argomento realizza un trattamento automatizzato su larga scala che può riguardare, tra l’altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di “attenzione” da parte delle forze di Polizia; ancorché la valutazione di impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno, l’identificazione di una persona in un luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato, al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella “watch-list”. Pertanto, si determina una evoluzione della natura stessa dell’attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui.

2) Il sistema SARI Real-Time, in quanto finalizzato all’effettuazione di un trattamento di dati personali per finalità di prevenzione di reati e minacce alla sicurezza pubblica e, anche su delega dell'Autorità Giudiziaria, di indagine, accertamento e perseguimento di reati, rientra nel campo di applicazione del Decreto.

La disciplina speciale per questa tipologia di trattamenti, rispetto a quella generale dettata dal RGPD, evidenzia che tali trattamenti determinano una forte interferenza con la vita privata delle persone interessate che deve trovare giustificazione in una adeguata base normativa.

L’art. 5 del Decreto, in attuazione dell’art. 3 della Direttiva UE 2016/680, dispone che i trattamenti di dati personali da parte degli organi di Polizia devono basarsi su disposizioni di legge o, ove da questa previsto, di regolamento.

Ciò in coerenza con la Convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali, il cui articolo 8 prevede che ogni persona ha diritto al rispetto della propria vita privata e familiare e non può esservi ingerenza di una autorità

pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Anche l'art. 52 della Carta dei Diritti Fondamentali dell'Unione Europea stabilisce che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta – tra i quali il diritto al rispetto della vita privata, ex art. 7 e quello alla protezione dei dati di carattere personale, ex art. 8 - devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà.

I dati personali oggetto del trattamento in argomento rientrano nelle categorie particolari di dati di cui all'art. 9 del RGPD, sub specie di "dati biometrici intesi a identificare in modo univoco una persona fisica".

Per le circostanze sopra descritte, in relazione all'utilizzo del sistema in occasione di manifestazioni pubbliche, il trattamento in argomento determina il possibile coinvolgimento di ulteriori dati personali di cui all'art. 9 del RGPD, quali quelli idonei a rivelare le opinioni politiche o l'appartenenza sindacale.

L'art. 7 del Decreto stabilisce che il trattamento dei dati particolari di cui all'articolo 9 del RGPD è soggetto a condizioni specifiche, tra le quali quella di dovere essere "specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento".

Orbene, nella documentazione fornita dal Ministero dell'Interno e tra le fonti normative da questo indicate non si rinviene alcuna disposizione specifica che consenta tale tipo di trattamento.

In particolare, il Decreto, ancorché preveda in astratto tali trattamenti, non può considerarsi, di per sé, fonte normativa idonea a legittimarli, in quanto è diretto a specificare le condizioni che ne consentono l'effettuazione, tra le quali individua, appunto, la sussistenza di una norma del diritto dell'Unione o dello Stato nazionale che lo autorizzi specificamente.

L'art. 1 del T.U.L.P.S. prevede i compiti generali in cui si declina l'attività dell'Autorità di pubblica sicurezza ma non contiene alcun riferimento al trattamento in argomento.

Il d.P.R. 15 gennaio 2018, n. 15, recante l'individuazione delle modalità di attuazione dei principi del Codice relativamente al trattamento dei dati effettuato per le finalità di polizia, adottato in attuazione dell'articolo 57 del previgente Codice, prevede e disciplina il trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video (Capo V), sistemi ontologicamente diversi da quelli dei dati biometrici(1).

Gli articoli 134 co.4, 234, 266 e 431 co.1, lett. b, del codice di procedura penale, citati nella valutazione di impatto, riguardano, rispettivamente, la documentazione degli atti per riproduzione audiovisiva, l'acquisizione di scritti o altri documenti mediante fotografia, cinematografia, fonografia ed altri mezzi, l'intercettazione di comunicazioni tra presenti mediante dispositivi elettronici portatili e l'intercettazione di flussi di comunicazioni telematiche. Pertanto, tali disposizioni non costituiscono base giuridica idonea per trattamenti di dati biometrici diretti all'identificazione personale.

Infine, anche gli articoli 55, 348, 354 e 370 del codice di procedura penale, parimenti citati nella valutazione di impatto tra le fonti normative di riferimento, attengono alle funzioni di polizia giudiziaria nell'assicurare le fonti di prova e nel condurre accertamenti su luoghi o persone, di iniziativa o su delega dell'Autorità giudiziaria, ma non prevedono il trattamento dei dati biometrici, onde non costituiscono quella fonte normativa specifica richiesta dall'art. 7 del Decreto.

3) In conclusione, allo stato non sussiste una base giuridica idonea, ai sensi dell'art. 7 del Decreto, a consentire il trattamento dei dati biometrici in argomento, come pure recentemente rilevato dal Garante in un caso per qualche profilo assimilabile (provvedimento n. 54 del 26 febbraio 2020, reperibile sul sito internet dell'Autorità, doc. web n. 9309458).

Al riguardo è da osservare che tale base giuridica, in esito alla ponderazione di tutti i diritti e le libertà coinvolti, dovrà, tra l'altro, rendere adeguatamente prevedibile l'uso di tali sistemi, senza conferire una discrezionalità così ampia che il suo utilizzo dipenda in pratica da coloro che saranno chiamati a disporlo, anziché dalla emananda previsione normativa.

Ciò vale anche per quanto riguarda alcuni aspetti fondamentali dell'impiego della tecnica di riconoscimento facciale in argomento, come, a titolo di mero esempio, i criteri di individuazione dei soggetti che possano essere inseriti nella watch-list o quelli per

determinare i casi in cui può essere utilizzato il sistema. Dovranno essere considerati, altresì, i limiti delle tecniche in argomento, notoriamente basate su stime statistiche della corrispondenza tra gli elementi confrontati e, quindi, intrinsecamente fallibili, stimando le eventuali conseguenze per gli interessati in caso di falsi positivi.

Le precedenti osservazioni assorbono la necessità di esaminare la bozza di valutazione di impatto prodotta da codesta Amministrazione, con riferimento alla quale si osserva tuttavia che appare di particolare rilievo assicurare la accuratezza e la capacità di discrimine, che vanno verificate per accertare che anche nei confronti di appartenenti a minoranze etniche il sistema sia pienamente adeguato.

**TUTTO CIÒ PREMESSO IL GARANTE**

ai sensi dell'art. 24, comma 5 e dell'art. 37, comma 3, lett. c), del Decreto esprime parere non favorevole nei termini di cui in motivazione sul progetto e avverte il titolare che il trattamento dei dati biometrici tramite il sistema Sari Real Time, appare non conforme alla disciplina di cui al Decreto, in mancanza di adeguate e specifiche disposizioni normative legittimanti.

Ai sensi dell'art. 152 del Codice e dell'art. 10 del d. lgs. 1° settembre 2011, n. 150, averso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo in cui il titolare del trattamento ha sede, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso.

*Roma, 25 marzo 2021*

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei

---

(1) Cfr. il considerando 51 del Regolamento (UE) 2016/679: "Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica".