UTILIZZO DEL RICONOSCIMENTO FACCIALE

PER FINI DI POLIZIA IN ITALIA

Utilizzo pratico, legalità del sistema, impatti sui diritti fondamentali, rischi di abuso

UN'INDAGINE A CURA DI:

PRIVACY NETWORK

STRALI
strategic litigation

STRALI
strategic litigation

PRIVACY NETWORK

Report a cura di: Riccardo Apa, Maria Vittoria Capra,
Alice Giannini, Lorenzo Sottile
Impaginato da: Serena Brighenti e Anna Florian
Aggiornato al: 17.04.2026

Progetto "Building Accountability for Law Enforcement Facial Recognition (SARI) in Italy"

Funded by European Artificial Intelligence & Society Fund

INDICE

PRIVACY NETWORK & STRALI HANNO INDAGATO L'UTILIZZO DI *SARI ENTERPRISE*, IL SISTEMA DI RICONOSCIMENTO FACCIALE IMPIEGATO DALLE FORZE DELL'ORDINE IN ITALIA.

Perché abbiamo indagato

Negli anni abbiamo assistito ad una diffusione massiva delle tecnologie di riconoscimento facciale nel settore privato e nel settore pubblico. Tuttavia, il dibattito pubblico è stato praticamente assente. Le informazioni disponibili sono poche e molto vaghe.

Questo tipo di tecnologia ha un impatto sui diritti e le libertà fondamentali di ognunə di noi (uguaglianza, libertà di manifestazione del pensiero, libertà di riunione, ecc.) tale da ridisegnare il rapporto fra cittadini ed autorità.

Sono numerosi gli esempi nel mondo di tecnologie di riconoscimento facciale utilizzate in maniera distorta, più come strumento di sorveglianza e repressione politica, che come mezzo per garantire la sicurezza dei cittadini.

Negli Stati Uniti,[1] già nel 2016, metà della popolazione era presente nei database di riconoscimento facciale della polizia, anche senza aver mai commesso reati.

Altri esempi di utilizzo politico del riconoscimento facciale sono stati registrati in Russia, a cui dobbiamo la prima sentenza della Corte Europea dei Diritti dell'Uomo (CEDU) su questo tema, in Ungheria, in Iran, in Cina e in molti altri Paesi.

Perché l'utilizzo del riconoscimento facciale non sfoci in abuso, sono necessarie regole chiare e una comprensione adeguata e diffusa da parte dei cittadini. Solo così possiamo sviluppare un'opinione fondata su dati oggettivi ed informazioni precise ed affidabili.

[1] www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up

All'interno di una società che vuole rimanere democratica, l'impiego di uno strumento di questo tipo deve necessariamente passare attraverso il vaglio di un dibattito aperto ed informato.

Questo lavoro nasce quindi dall'esigenza di comprendere lo strumento e fornire dati oggettivi al pubblico, in modo che chiunque possa verificare se il riconoscimento facciale sia un efficace strumento di indagine oppure un mezzo di sorveglianza.

OBIETTIVI DELL'INDAGINE

(i) Ricostruire le modalità pratiche di utilizzo del sistema

(ii) Valutarne l'affidabilità ed efficacia come strumento di indagine

(iii) Valutarne la legalità rispetto alla normativa in tema di diritti fondamentali, sulla protezione dei dati personali e di utilizzabilità in un processo penale

(iv) Comparare l'utilizzo con casi simili in altri Stati europei

COME ABBIAMO INDAGATO

L'indagine è stata svolta tramite richieste di accesso civico generalizzato (anche chiamate FOIA, Freedom of Information Act).

La richiesta di accesso civico generalizzato, introdotta nel d.lgs 33/2013, permette a qualsiasi cittadino di ottenere dati e documenti in possesso della pubblica amministrazione. L'obiettivo della norma è favorire una maggiore trasparenza delle istituzioni e garantire alla società civile e ai giornalisti il ruolo di controllo sulle attività governative.

Il principio di trasparenza nell'operato della pubblica amministrazione ha radici molto antiche. È un'idea universalmente condivisa che il controllo diffuso da parte dei cittadini favorisce la democrazia. Già nel 1908, Turati immaginava le strutture della Pubblica amministrazione come una "casa di vetro". O con le parole del Ministro per la semplificazione e la pubblica amministrazione:

> [...] occorre tener conto della particolare rilevanza, ai fini della promozione di un dibattito pubblico informato, delle domande di accesso provenienti da giornalisti e organi di stampa o da organizzazioni non governative, cioè da soggetti riconducibili alla categoria dei "social watchdogs" cui fa riferimento anche la giurisprudenza della Corte europea dei diritti dell'uomo (da ultimo, caso Magyar c. Ungheria, 8 novembre 2016, §165).

StraLi e Privacy Network operano proprio in queste vesti per facilitare il dibattito pubblico.

Tutte le istanze della pubblica amministrazione devono essere studiate.
È un dovere e un diritto dei cittadini verificare che la pubblica amministrazione agisca nell'interesse pubblico.

Fra queste, **le forze dell'ordine meritano un'attenzione speciale perché sono le uniche legittimate a usare la forza**. Esiste il rischio concreto che l'idea di sicurezza venga strumentalizzata per colpire il dissenso politico, etichettando come violente tutte le forme di critica, spesso in assenza di prove tangibili.

Quando ciò accade, la polizia smette di perseguire i reati comuni a beneficio della collettività per concentrarsi sulla repressione di atti di natura politica. Trasformandosi, di fatto in un corpo di protezione esclusiva dei detentori del potere economico e politico

Questa deriva rappresenta uno dei maggiori pericoli per le democrazie moderne: la trasformazione dello Stato di diritto in una "democrazia illiberale", dove il diritto di critica – pilastro fondamentale di ogni sistema libero – viene di fatto messo al bando.

Il principio della "***casa di vetro***" è particolarmente rigoroso proprio laddove il potere è più invasivo. Un'amministrazione che ricorre a sistemi di riconoscimento biometrico altamente invasivi non può sostenere che il proprio operato sia opaco.

> "L'evoluzione verso la visibilità del potere [...] è la storia della lunga marcia verso la democrazia" (Adunanza Plenaria n. 10/2020).

SEZIONE 1

COME FUNZIONA UN SISTEMA DI RICONOSCIMENTO FACCIALE

- Come funziona (in teoria)
- Spazio
- Tempo
- Utilizzo in tempo reale
- Utilizzo ex-post
- I **rischi** del riconoscimento facciale

COME FUNZIONA UN SISTEMA DI RICONOSCIMENTO FACCIALE

Quando parliamo di sistemi di riconoscimento facciale, parliamo di sistemi complessi, il cui elemento centrale è un software in grado di riconoscere il volto di una persona all'interno di una foto (oppure il frame di un video) ed associarlo ad un'identità nota all'interno di un **database**.

Il **software** analizza l'immagine di un volto e lo riduce ad un identificativo processabile da un computer (es. calcolando la distanza tra alcuni punti fissi del volto).

Tuttavia, per avere un vero e proprio sistema di riconoscimento facciale non basta un software, serve un'infrastruttura che acquisisca immagini, si colleghi ad un database già esistente e confronti le immagini estratte dalle **telecamere** con quelle contenute nel database.

ELEMENTI MINIMI DI UN SISTEMA DI RICONOSCIMENTO FACCIALE

Un **DATABASE** che contenga le identità di alcune persone da riconoscere

Una (o più) **TELECAMERE**

Un **SOFTWARE** di riconoscimento facciale

Cosa influisce sulle prestazioni?

- qualità dell'immagine in input;
- limiti tecnici del software;
- qualità delle foto presenti nel database;
- modalità di utilizzo.

*Tutti questi **elementi** non vanno sottovalutati perché incidono profondamente sui risultati del sistema e dunque sulla sua **efficacia**. Ricordiamoci inoltre che tutto questo ha un costo, tanto in termini monetari quanto di tempo e risorse umane.*

COME FUNZIONA (in teoria)

Esistono diversi tipi di sistemi di riconoscimento facciale. La più importante distinzione può essere tracciata secondo due elementi: IL TEMPO e LO SPAZIO.

NEL TEMPO

I sistemi di riconoscimento facciale possono essere utilizzati:

↘ **Ex post** — un'immagine già ripresa da una telecamera viene estratta in un secondo momento e solamente il volto della persona o delle persone visibili nel video vengono analizzate e confrontate con il database di riferimento

↘ **In tempo reale** — le telecamere riprendono in tempo reale il flusso di tutte le persone che attraversano una certa zona. Le immagini acquisite vengono sottoposte ad analisi e confrontate con il database di riferimento.

NELLO SPAZIO

Opera attraverso telecamere:

↘ **In ambienti controllati** (es. la sala server di un'azienda)

↘ **In luoghi pubblici**

La combinazione che crea più problemi sia a livello tecnico che giuridico, è l'utilizzo in tempo reale in luoghi pubblici.

I RISCHI DEL RICONOSCIMENTO FACCIALE

Abbiamo detto più volte che le tecnologie di riconoscimento facciale presentano **rischi per i diritti e le libertà.**

Come impatta sulle nostre libertà?

UN ESEMPIO DALLA RUSSIA

Uno dei casi più emblematici di utilizzo del riconoscimento facciale per fini politici è il **caso Gluckhin**. Nel 2019 il signor Glukhin viaggia nella metropolitana di Mosca con una figura di cartone ritraente un dissidente, Konstanin Kotov, e uno striscione che ne lamentava l'incarcerazione. Il signor Glukhin mette in atto una protesta solitaria e pacifica, limitandosi ad esporre il proprio cartonato in pubblico. Tuttavia viene successivamente ***identificato attraverso il sistema di riconoscimento facciale ed arrestato con una scusa pretestuosa***. Il reato commesso avrebbe riguardato il divieto di manifestare con oggetti smontabili.

Casi simili si verificano nuovamente nel 2022 nei confronti di chi manifesta contro la guerra.*

* Nell'ambito della sorveglianza il livello di accettabilità cambia rapidamente. Fino a qualche anno fa, la Corte Europea dei diritti umani diceva chiaramente che "non ci sarà mai spazio per l'utilizzo di sistemi simili in Europa". Oggi, con l'entrata in vigore dell'IA ACT, l'utilizzo dell'identificazione biometrica, anche nella sua versione in tempo reale e in luoghi pubblici, è ammesso "in certi casi". Fra questi casi, le funzioni di sicurezza hanno un ruolo privilegiato .

1 UTILIZZO DI DATI BIOMETRICI

Trattare dati biometrici significa usare uno strumento molto più pervasivo rispetto a quelli comuni; il trattamento di questi dati è normalmente consentito in condizioni molto più stringenti e richiede misure di garanzia più forti per i cittadini. Ricordiamoci, inoltre, che costruire database di dati biometrici dei cittadini significa creare bersagli per possibili attacchi informatici.

2 RISCHI DI ERRORE

Anche ***gli algoritmi sbagliano,*** molto più di quanto vorremmo pensare.
Uno dei rischi riguarda proprio l'arresto della persona sbagliata, che dovrà comunque difendersi dalle accuse.
Un elemento da tenere particolarmente in considerazione è che gli algoritmi di riconoscimento facciale ***hanno un'efficacia diversa a seconda delle caratteristiche demografiche***. Se l'algoritmo funziona peggio a seconda dell'etnia, del genere o di altri elementi, c'è il rischio di introdurre forme di discriminazione automatizzata.

3 L'ANALISI È AFFIDATA AD UN SISTEMA AUTOMATIZZATO

Utilizzare sistemi automatizzati porta con sé dei rischi. È ormai noto che esiste un ***bias di conferma negli operatori*** che verificano i risultati, cioè una tendenza a prendere per buono il risultato e cercare elementi che lo giustifichino, piuttosto che metterlo in discussione. Questo ci riporta al punto 2.

C'è un ulteriore problema nell'utilizzo di un sistema automatizzato, spesso ***il vero e proprio funzionamento non è spiegabile***. Da un lato, perché molti algoritmi funzionano come black box, rendendo quindi opaca la logica che porta a un determinato risultato.
Dall'altro, perché le aziende che sviluppano questi software hanno interesse a mantenere segreti gli elementi che influenzano il risultato.
In queste condizioni *diventa molto più difficile*, per una persona identificata, difendersi e ***contestare la decisione.***

4 L'ANALISI AVVIENE ALL'INSAPUTA DEL SOGGETTO ANALIZZATO

Durante un normale controllo di polizia, ***la persona controllata sa ciò che sta succedendo***. Quando l'identificazione avviene da remoto, la persona controllata non sa cosa sta accadendo. Questo aggrava ulteriormente il problema della contestazione della decisione.

5 COSTI PER IL PUBBLICO IN TERMINI DI TEMPO E SOLDI SPESI DALLA POLIZIA

Creare ***un sistema di riconoscimento facciale ha un costo***: bisogna approntare un'infrastruttura, prevedere costi di manutenzione e dedicare personale alla verifica dei risultati. Personale che dovrà essere formato. ***Si rischia di mettere in piedi un sistema molto più costoso di quanto sia necessario***.

6 L'UTILIZZO PUÒ TRASFORMARSI UN SISTEMA DI SORVEGLIANZA DI MASSA

È ormai ampiamente noto che la sorveglianza viene gradualmente normalizzata e tende ad espandersi e diventare sempre più invasiva. Introdurre sistemi che monitorano la popolazione costantemente e senza necessità di indagine fa sfumare il confine tra cittadini che hanno commesso reati e chi non li ha compiuti. Il risultato è l'idea della sorveglianza costante che finisce con il modificare il nostro comportamento e il nostro rapporto con lo spazio che viviamo.

Utilizzare il riconoscimento facciale non significa solamente automatizzare una funzione che già conosciamo, ma modificare lentamente il modo in cui si conducono indagini di polizia. A cambiare radicalmente è la quantità di persone analizzate a fronte dell'effettiva utilità.

Ad esempio, a Londra nel 2025, l'analisi tramite riconoscimento facciale ha interessato più di 3 milioni di persone, portando a meno di mille arresti
L'efficacia dello strumento è dello 0,03%.

SEZIONE 2

IL RICONOSCIMENTO FACCIALE IN ITALIA: COME FUNZIONA SARI ENTERPRISE

LA BANCA DATI AFIS

- Quali soggetti contiene AFIS
- Il fotosegnalamento

RISULTATI DELL'INDAGINE

- Scarsa collaborazione da parte delle autorità
- Assenza di dati sull'efficacia e sui tassi d'errore
- Dati sull'utilizzo in crescita
- Evidenti criticità nel rispetto della normativa di riferimento

DIRITTI FONDAMENTALI

COME FUNZIONA SARI ENTERPRISE

Ad oggi, l'unico sistema di riconoscimento facciale impiegato dalle forze dell'ordine su larga scala è SARI ENTERPRISE. Un sistema di identificazione biometrica "a posteriori" utilizzato dalla Polizia Scientifica per finalità investigative.

Il sistema è stato acquistato nel 2017 dal Ministero dell'Interno. La funzionalità SARI ENTERPRISE (in differita) **è attiva dal 2018** e ha ricevuto parere positivo del Garante per la protezione dei dati personali.

Il sistema **consente di analizzare e confrontare un'immagine del volto estratta da una telecamera con quelle contenute in una banca dati di riferimento**.

Nel caso di SARI Enterprise, il **database di riferimento è AFIS** (Automated Fingerprint Identification System), che include (anche) le immagini dei volti delle persone sottoposte a fotosegnalamento.

Se si ha a disposizione un frame video in cui si vede il volto di una persona che sta commettendo un reato, si può estrarre il template biometrico del volto dell'autore del reato e confrontarlo con i volti presenti nella banca dati AFIS. Il sistema restituisce un elenco di potenziali candidati con relativi punteggi (in percentuale di somiglianza).

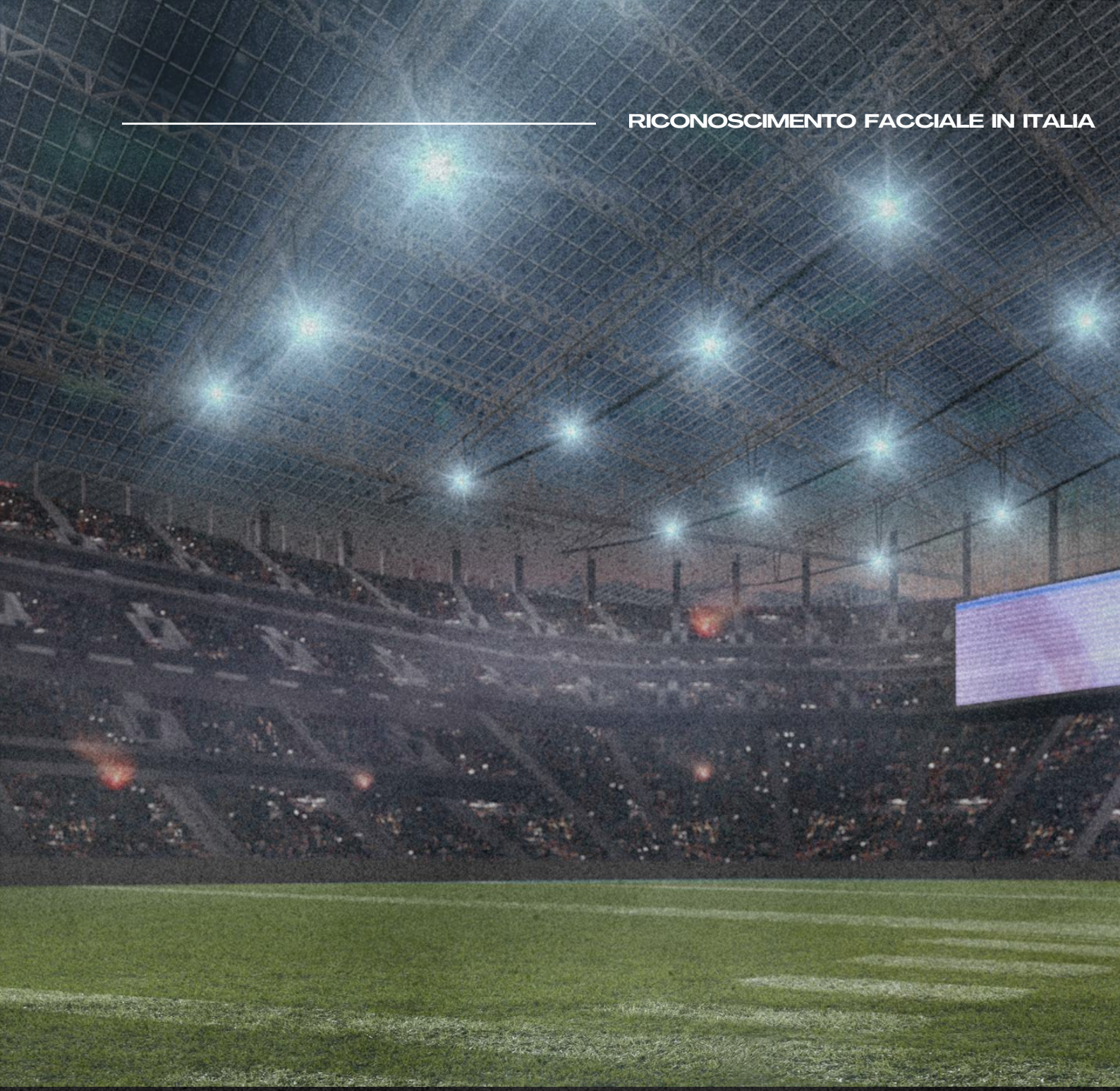
Sistemi come questi possono essere utilizzati in modalità diverse:

- **Rank based:** mostrano solo un certo numero di candidati;
- **Threshold base:** mostrano solamente i candidati con una percentuale di somiglianza supera una soglia prestabilita;
- **Modalità mista:** combinando i due parametri.

La scelta di questa impostazione ha un impatto diretto sulle indagini: includere molti risultati nella lista potrebbe rallentare le indagini perché ci sono troppi indagati, viceversa restringere troppo la lista rischia di escludere soggetti rilevanti.
Per quanto riguarda SARI ENTERPRISE, vengono mostrati i primi 50 risultati, senza soglie minime di somiglianza.

l risultato viene quindi verificato manualmente da un operatore e diventa un risultato operativo. Quindi utilizzabile nel prosieguo delle indagini, ma non una vera e propria prova utilizzabile in tribunale.

Ciò che fa SARI ENTERPRISE, in sostanza, è **automatizzare, attraverso l'uso di un algoritmo di intelligenza artificiale, l'attività di ricerca all'interno dei cartellini fotosegnaletici.**



C'è altro in Italia?

Abbiamo soltanto un altro esempio certo di utilizzo di sistemi di riconoscimento facciale per fini di polizia: il sistema di sicurezza dello Stadio **Olimpico di Roma**.

Oltre a questo, un'inchiesta di Fanpage.it sembrerebbe indicare l'acquisto da parte dell'Arma dei Carabinieri di un sistema di riconoscimento facciale noto come **Corsight**. Tuttavia, non sono disponibili ulteriori informazioni pubbliche.

LA BANCA DATI AFIS

Il sistema SARI ENTERPRISE è sostanzialmente un'automazione della ricerca all'interno della banca dati AFIS. Questo significa che può essere utilizzato per identificare chi è inserito all'interno di questa banca dati e che i tuoi diritti possono essere esercitati in relazione a questa banca dati.

QUALI SOGGETTI CONTIENE AFIS?

Il vero problema a livello di tenuta dello Stato di diritto non è tanto il sistema di ricerca, quanto la banca dati in sé. Catalogare sempre più cittadini, magari sulla base delle opinioni politiche o sulla base dell'etnia, senza che questi abbiano commesso un reato, è una prassi tipica di uno stato autoritario. In casi come questi, lo strumento non serve ad indagare sui reati proteggendo i cittadini, ma a sorvegliare le persone sgradite per proteggere il gruppo al potere.

La banca dati AFIS è costituita da persone italiane e straniere sottoposte a procedimenti penali. Inoltre, vi rientrano tutti coloro che fanno domanda di permesso di soggiorno o richiesta di asilo, anche in assenza di collegamento con reati.

Purtroppo non siamo riusciti a scoprire quanti soggetti sono contenuti nel database AFIS.
Il dipartimento di pubblica sicurezza ci ha fatto sapere di non conoscere il numero di record contenuti nel database e di non essere in grado di eseguire la relativa estrazione di dati.
Secondo le indagini svolte da ASGI e da Irpimedia, i soggetti compresi nella banca dati AFIS nel 2022 erano 13.516.259 cittadini da Paesi extra-europei, 1.654.917 cittadini europei e 3.289.196 cittadini italiani, a cui si sono aggiunti ulteriori 992.093 fotosegnalamenti nel 2023.

L'importanza del numero di soggetti compresi nel database e le loro caratteristiche demografiche non devono essere sottovalutate.
Se le persone con alcune caratteristiche sono sovrarappresentate, sarà più probabile che vengano individuate all'interno dei risultati anche in casi errati, influenzando in maniera negativa il proseguimento delle indagini. Una delle pratiche per evitare questo problema è compartimentare i database.

L'importanza dei test

Nel 2020, la Polizia del Galles del Sud è stata sanzionata dall'autorità inglese per la protezione dei dati personali, per non aver svolto test adeguati sulle performance dell'algoritmo di riconoscimento facciale sulle diverse etnie. [2]

[2] www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

IL FOTOSEGNALAMENTO

Dato che la registrazione all'interno di AFIS avviene a seguito di un fotosegnalamento sarebbe utile avere maggiore chiarezza su come avvenga questa operazione. Da alcuni anni riceviamo testimonianze di persone fotografate dalla polizia attraverso il dispositivo personale dell'agente. Ad oggi non è chiaro se questa modalità di acquisizione dell'immagine significhi che la persona fotografata sarà registrata in AFIS.

La prassi di mantenere all'interno dello stesso database persone con precedenti penali e cittadini stranieri che non hanno precedenti penali è stata ritenuta discriminatoria ed è oggetto di una causa promossa da ASGI. [3]
In assenza di un'adeguata compartimentazione del database il rischio è anche quello di rendere meno efficiente la ricerca in caso di indagine.

3 www.asgi.it/antidiscriminazione/casellario-afis-una-banca-dati-discriminatoria-forze-di-polizia

RISULTATI DELL'INDAGINE

Da questa prima fase di indagine possiamo trarre le seguenti conclusioni.

1 SCARSA COLLABORAZIONE DA PARTE DELLE AUTORITÀ

Seppure con un certo miglioramento rispetto al passato, ***le autorità si dimostrano ancora molto evasive nel condividere informazioni e documenti che il cittadino ha diritto ad ottenere*** per espressa previsione di legge. Una parte considerevole delle nostre richieste, specialmente quelle relative alle procedure di garanzia dei diritti fondamentali, ha ricevuto risposte estremamente vaghe e in alcuni casi l'autorità ha semplicemente dichiarato di non avere a disposizione i relativi documenti. *Documenti che, vale la pena ricordare, sono obbligatoriamente previsti per legge.*

2 ASSENZA DI DATI SULL'EFFICACIA e SUI TASSI DI ERRORE

Utilizzare un algoritmo di intelligenza artificiale non significa di per sé che verranno ottenuti buoni risultati. ***La capacità dell'algoritmo di individuare con chiarezza un individuo dipende da diversi fattori:*** anzitutto le **caratteristiche demografiche** (etnia, età, genere), che influiscono in maniera considerevole sulle prestazioni.

Bisogna altresì ricordare che le immagini a disposizione non sono necessariamente di alta qualità. Le ***condizioni di visibilità, di illuminazione, l'angolazione, la risoluzione della telecamera*** sono fattori che influenzano fortemente la performance dell'algoritmo. Per ovviare a questi problemi, le immagini possono essere pulite; tuttavia, anche questa operazione può influire negativamente sul funzionamento del sistema.

Per questo motivo è fondamentale avere dati precisi sui tassi di efficacia registrati nel concreto e non solamente quelli derivanti dalla sperimentazione in laboratorio.
Dato che SARI ENTERPRISE fornisce elenchi di possibili sospettati, abbiamo chiesto quanti risultati operativi idonei al proseguimento delle indagini sono stati generati.
Ad esempio, se il sistema riesce ad identificare un sospettato con una probabilità del 10%, il risultato verrà comunque utilizzato o verrà semplicemente scartato?

Nonostante il sistema sia *in uso* alle forze dell'ordine *da circa 8 anni*, il Ministero dell'Interno *non ha a disposizione dati sull'efficacia* del sistema. Per stessa ammissione del dipartimento di pubblica sicurezza, questi dati non sono mai stati raccolti.

La percentuale di falsi positivi (i casi in cui una persona viene identificata in maniera errata) **non viene calcolata**, nonostante le linee guida in uso alla polizia dedichino diverse sezioni alle modalità di valutazione delle prestazioni di un algoritmo come SARI ENTERPRISE e di configurazione differente a seconda delle esigenze di indagine.

Secondo le informazioni raccolte da IRPI MEDIA l'algoritmo performava in maniera differente su soggetti bianchi e non. Per le persone non bianche, la possibilità di individuare il ricercato tra i primi dieci risultati era di circa il 77%. Ad oggi non disponiamo di dati aggiornati.

L'assenza di dati effettivi sull'efficacia ci ha lasciati particolarmente stupiti, dato che questo sarebbe il dato più utile a valutare l'effettiva utilità del sistema come strumento di indagine. Troviamo piuttosto assurdo che il dipartimento di pubblica sicurezza non si sia mai preoccupato di raccogliere dati sull'utilizzo di una tecnologia simile, non solo per ragioni di trasparenza ma più semplicemente per valutare sulla base di dati oggettivi se il sistema è effettivamente di aiuto alla polizia.

Ad oggi, abbiamo identificato pochissimi provvedimenti in cui si fa riferimento all'utilizzo di SARI ENTEPRISE. Tra questi, nel 2023 la Corte di Cassazione ha ammesso l'utilizzabilità degli esiti dell'utilizzo di SARI ENTERPRISE qualora gli stessi si inseriscano in un più strutturato complesso di indizi (Cass. Pen. sez. IV, n. 39551/2023). Nella stessa ottica, in una decisione del 2025 (Cass. Pen. sez. II, n. 18099/2025) si afferma che il sistema aveva fornito una compatibilità solo del 55,2% (definita una "***non rassicurante percentuale"***) e che perciò tale risultato dovesse avere una ***valenza indiziaria limitata.*** In ogni caso, i risultati forniti da SARI ENTERPRISE ***non possono, da soli, costituire il fondamento di una responsabilità penale.***

In generale, il rapporto delle pubbliche amministrazioni italiane con la tecnologia è ancora piuttosto ingenuo. Quando si acquista un sistema sofisticato di indagine, non si verifica che abbia effettivamente un impatto positivo sull'operato delle forze dell'ordine. Il rischio è quello di investire in sistemi poco utili facendo l'interesse solamente delle aziende che si aggiudicano gli appalti di fornitura.

In altri paesi, come ad esempio il Regno Unito, i risultati sono oggetto di una pubblicazione annuale. Il funzionamento dell'algoritmo utilizzato dalla polizia è inoltre oggetto di revisione indipendente, anche questa analisi è liberamente accessibile online.

3 DATI SULL'UTILIZZO IN CRESCITA

Pur non essendo in grado di sapere con esattezza se il sistema funziona bene o no, l'utilizzo appare in crescita. Anche se la ricerca senza impiego di algoritmi rimane largamente più utilizzata.

Le ricerche svolte tramite SARI ENTERPRISE sono molto aumentate negli anni:

- nel 2022 è stato utilizzato 79.362 volte;
- nel 2023 è stato utilizzato 131.023 volte;
- nel 2024 è stato utilizzato 181.705 volte, a fronte di 515.447 ricerche testuali senza algoritmi.;
- nel 2019 è stato utilizzato 41.888 volte;
- nel 2020 è stato utilizzato 38.315 volte;
- nel 2021 è stato utilizzato 52.539 volte;

Il sistema prevede 3 tipi di ricerca:

- ricerca sulla base di una sola foto;
- ricerca sulla base di più foto;
- ricerca combinata, sulla base di foto ed elementi testuali.

Le ultime due modalità dovrebbero essere più efficaci rispetto alla prima, che però rimane quella più utilizzata.

MODALITA' RICERCA IN AFIS	
Totale ricerche tramite riconoscimento facciale	26.06%
Ricerche testuali	73.94%

TOTALE RICERCHE	% SU TOTALE RICERCHE IN AFIS	% SU TOTALE RICERCHE SARI
Ricerche per immagini	23.25%	89.19%
Ricerche multi-foto	1.67%	6.40%
Ricerche combinate	1.15%	4.41%

4 EVIDENTI CRITICITÀ NEL RISPETTO DELLA NORMATIVA DI RIFERIMENTO

Il profilo più critico emerso dalla nostra ricerca riguarda il rispetto della normativa vigente, sia sotto il profilo del trattamento dei dati per finalità di polizia, disciplinato dal d.lgs. 51/2018, sia con riferimento alle garanzie poste a tutela dei diritti fondamentali.

Va anzitutto rilevato che la legislazione italiana in materia presenta gravi lacune. Non esiste, infatti, una disciplina specifica sull'utilizzo del riconoscimento facciale da parte delle forze dell'ordine. Il principale riferimento normativo resta quello relativo al trattamento dei dati per fini di polizia, che tuttavia appare in più punti inadeguato rispetto alle caratteristiche e ai rischi propri di queste tecnologie e, a nostro avviso, richiederebbe una revisione.

L'utilizzo di SARI ENTERPRISE è stato autorizzato con parere positivo del Garante per la protezione dei dati personali. Occorre tuttavia evidenziare che ***il parere è molto sintetico, le motivazioni sulle valutazioni sono praticamente assenti e la documentazione visionata dal Garante non è disponibile al pubblico***.

Per valutare il rispetto della normativa applicabile, la nostra ricerca si è incentrata su due aspetti fondamentali: **la valutazione di impatto sulla protezione dei dati personali e le misure di garanzia per i diritti fondamentali.**

LA VALUTAZIONE DI IMPATTO

Dato che l'utilizzo di un sistema di riconoscimento facciale da parte della polizia presenta un rischio elevato per i diritti e le libertà delle persone, dovrebbe essere preceduto da una valutazione d'impatto sulla protezione dei dati personali *(questo passaggio è obbligatorio per legge)*.
Una volta effettuata la valutazione, dovrebbero poi essere previste garanzie, misure di sicurezza e meccanismi per garantire la protezione dei dati personali (misure ancor più stringenti considerando che il sistema tratta dati biometrici).

Questi passaggi sono fondamentali per garantire un utilizzo corretto, assicurando il rispetto dei diritti dei cittadini e fornendo una chiara protezione dai possibili abusi. Sotto questo profilo, le risposte sono state molto vaghe ed elusive. Il dipartimento di pubblica sicurezza ci ha rimandati genericamente al parere di autorizzazione del Garante, che tuttavia non contiene i documenti richiesti.

Nel corso del contenzioso, riguardo al nostro quesito relativo alla DPIA, l'avvocatura dello stato ha dichiarato che questo documento **non è mai stato predisposto da parte del ministero dell'interno.**
Resta da capire, per quale motivo, il Garante per la protezione dei dati personali abbia considerato lecito l'impiego di un sistema di riconoscimento facciale in assenza di una valutazione di impatto dedicata, posto che questo sembrerebbe rappresentare un'aperta violazione dell'art. 23 del D.lgs 51/2018.

LA PROCEDURA DI GARANZIA DEI DIRITTI E DELLE LIBERTÀ DEI CITTADINI
In maniera molto simile sono state trattate le nostre richieste relative alle procedure pensate per garantire i ***diritti e le libertà dei cittadini***, anch'esse esplicitamente richieste per legge.
Anche in questo caso, la prima risposta ricevuta dalle autorità è stata un rimando generico al parere di autorizzazione del Garante, che non contiene spiegazioni e documenti.
Ad una seconda richiesta, il dipartimento di pubblica sicurezza ha candidamente ammesso di non avere documentazione disponibile. ***Abbiamo quindi fondato motivo di ritenere che le procedure semplicemente non esistano o almeno non siano mai state formalizzate***.

Merita infine segnalare che in altri Paesi questo tipo di documenti è disponibile online e liberamente consultabile.

ALTRE CRITICITÀ SOTTO IL PROFILO DELLA LEGALITÀ

PER QUALI REATI VIENE UTILIZZATO SARI
Ad aggravare ulteriormente la situazione, non sono state fornite informazioni rispetto all'elenco di reati per i quali viene utilizzata la ricerca tramite riconoscimento facciale o indicazioni chiare sull'effettiva modalità di utilizzo del sistema. Informazioni di questo tipo sono fondamentali per valutare l'efficacia del sistema, nonché il livello di interferenza con i diritti fondamentali. Al momento l'ipotesi più probabile è che SARI ENTERPRISE venga utilizzato arbitrariamente per qualunque reato.

INFORMATIVA AGLI INTERESSATI
Un problema ulteriore riguarda le informazioni rese agli interessati, in particolare le modalità di esercizio dei propri diritti. Tali informazioni dovrebbero essere disponibili online, quasi tutte le banche dati della polizia hanno una pagina web dedicata. Tuttavia, per la banca dati AFIS non esiste nessuna pagina.

QUANTO A LUNGO SI RESTA NEI DATABASE DELLA POLIZIA
Infine, il tempo di ritenzione dei dati personali è estremamente lungo. Quando una persona entra nella banca dati AFIS, i suoi dati vengono anonimizzati dopo 20 anni dal fotosegnalamento. Mentre quelli riferiti ad "attività di polizia giudiziaria" dopo 40 anni. Dati i tempi di ritenzione, *una volta fotosegnalati, è praticamente impossibile uscire dalle banche dati*, anche perché il tempo può essere ulteriormente esteso in caso di necessità.

FORMAZIONE PER LA POLIZIA
Un'ulteriore criticità riguarda la formazione del personale di polizia sull'utilizzo del sistema. Sul tema, non risultano disponibili dati o informazioni accessibili al pubblico relative ai percorsi formativi eventualmente adottati. Questa mancanza di trasparenza rende difficile valutare se l'utilizzo del sistema da parte degli operatori avvenga a seguito di adeguati approfondimenti, in particolare in merito all'impatto della tecnologia sui diritti fondamentali dei soggetti.

DIRITTI FONDAMENTALI

Oltre alla normativa in tema di protezione dei dati personali, va rispettata anche la normativa sulla protezione dei diritti fondamentali.

L'utilizzo di un sistema come SARI ENTERPRISE costituisce una *limitazione di diritti fondamentali.* Per valutare se questa operazione è lecita bisogna guardare all'art. 52 della Carta dei Diritti Fondamentali dell'Unione Europea.

Per valutare eventuali violazioni della disciplina sui diritti fondamentali, si devono analizzare alcuni parametri:

Il contesto normativo: Le limitazioni di diritti fondamentali sono consentite all'interno di un quadro giuridico chiaro e definito, che permetta ai cittadini di comprendere come verrà utilizzato lo strumento e come fare valere i propri diritti. L'obiettivo è quello di evitare applicazioni differenti, utilizzi arbitrari, abusi e diminuire la capacità di ricorso dei cittadini.

Sotto questo profilo, la normativa italiana è piuttosto carente. Non esiste una normativa dedicata all'impiego per fini di polizia del riconoscimento facciale, mentre la disciplina relativa al trattamento di dati per fini di polizia prevede l'emanazione di alcuni decreti attuativi, che, ad oggi, non sono stati emanati.

Principio di necessità: La limitazione deve rispondere al principio di necessità. Questo significa che, prima di introdurre una limitazione di questo tipo, occorrerebbe valutare altre alternative meno invasive e rischiose.

L'introduzione di misure fortemente impattanti sui diritti e sulle libertà non deve dipendere solamente dall'arrivo sul mercato di un nuovo e più potente mezzo d'indagine, ma dall'effettiva assenza di alternative.
La buona prassi dovrebbe essere che la valutazione svolta dall'autorità sia documentata attraverso analisi oggettive e verificabili.
Bisogna anche ricordare che il trattamento di dati biometrici dovrebbe avvenire solo in casi di ***stretta necessità***, la valutazione quindi dovrebbe essere ancora più stringente.

Anche sotto questo aspetto non ci è stata fornita alcuna documentazione a sostegno del fatto che sia stata svolta una valutazione di necessità. Anzi, l'assenza di dati sull'efficacia e della DPIA, indica una probabile violazione del principio di necessità.

Principio di proporzionalità: Introdurre nuove limitazioni o utilizzare nuovi sistemi di indagine ha dei vantaggi e degli svantaggi. Una limitazione rispetta il principio di proporzionalità quando i vantaggi superano gli svantaggi.
Nell'ambito della protezione dei dati, la gravità della limitazione è misurata dalla profondità delle analisi che si possono trarre.
A questo fine dovrà essere valutata la natura dei dati trattati, il numero di soggetti coinvolti (ponendo particolare attenzione al rischio che altri siano accidentalmente investiti dall'analisi), il contesto in cui i dati sono raccolti, il numero di soggetti che possono avervi accesso ecc., senza dimenticare il tempo per cui i dati sono conservati e la revisione periodica.

È importante ricordare che nei casi in cui l'interferenza sia poco rilevante per il singolo, l'applicazione su vasta scala può porre un grave rischio per la collettività.

Una volta valutati gli svantaggi, si potranno adottare specifiche misure di salvaguardia per mitigare rischi. ***Anche in questo caso il principio di proporzionalità non sembra essere stato rispettato.***

I TUOI DIRITTI E COME PROTEGGERLI

Nonostante durante la nostra ricerca abbiamo riscontrato una scarsa applicazione delle leggi in vigore, il trattamento di dati personali da parte delle forze dell'ordine deve avvenire nel rispetto della normativa di riferimento.

Tale normativa prevede alcuni obblighi per chi tratta i dati, una serie di diritti per il cittadino e le modalità per esercitarli. Il cittadino che venga inserito nella banca dati AFIS e che quindi può essere identificato tramite SARI ENTERPRISE, può esercitare questi diritti.

A parte la normativa sul trattamento dei dati personali, rimangono sempre validi i diritti previsti dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione Europea e la Convenzione Europea dei Diritti dell'Uomo.

LA LEGGE SUL TRATTAMENTO DEI DATI PERSONALI

La disciplina di riferimento è il Dlgs 51/2018. Prima di entrare nei dettagli è necessario chiarire alcuni termini:

- T**ITOLARE DEL TRATTAMENTO** (chi tratta i dati. Nel nostro caso Ministero dell'interno – Dipartimento della Pubblica Sicurezza)
- S**OGGETTO INTERESSATO** (La persona i cui dati sono trattati)

La disciplina è fondata su alcuni **obblighi per il TITOLARE** e alcuni **diritti per l'INTERESSATO,** in primis il diritto di accesso, per verificare la propria presenza all'interno del database. Sono previste una serie di limitazioni ai diritti e, in caso di rifiuto , si può proporre reclamo al garante o tentare di esercitare gli stessi diritti ai sensi del codice penale (se attinente).

OBBLIGHI DEL TITOLARE (ART 9 - 10)

Il primo obbligo per il TITOLARE DEL TRATTAMENTO è quello di **mettere a disposizione dell'interessato una serie di informazioni.** Questo passaggio è importante affinché il cittadino sia in condizione di sapere cosa sta accadendo e come esercitare i propri diritti.

Informazioni da fornire

Le informazioni che devono essere fornite sono le seguenti
a) l'identità e i dati di contatto del titolare del trattamento;
b) i dati di contatto del responsabile della protezione dei dati, se previsto;
c) le finalità del trattamento cui sono destinati i dati personali;

d) la sussistenza del diritto di proporre reclamo al Garante e i relativi dati di contatto;
e) la sussistenza del diritto di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano.

Se previsto da legge o regolamento
a) il titolo giuridico del trattamento;
b) il periodo di conservazione dei dati personali o, se non è possibile, i criteri per determinare tale periodo;
c) le categorie di destinatari dei dati personali, anche in Paesi terzi o in seno a organizzazioni internazionali;
d) le ulteriori informazioni ritenute utili all'esercizio dei diritti, in particolare nel caso in cui i dati personali siano stati raccolti all'insaputa dell'interessato.

Come devono essere fornite le informazioni
Queste informazioni devono essere messe a disposizione, anche attraverso il proprio sito internet.
È espressamente previsto che le informazioni siano trasmesse "con qualsiasi mezzo adeguato, anche per via elettronica, se possibile con le stesse modalità della richiesta."
Inoltre, è previsto che "Il titolare del trattamento facilita l'esercizio dei diritti." Infine che, in caso di richiesta, Il titolare del trattamento informi "l'interessato senza ingiustificato ritardo e per iscritto dell'esito della sua richiesta."

DIRITTI ESERCITABILI (ART. 11-12)

Chi fa richiesta ha diritto di ottenere:

1. Conferma dell'esistenza di un trattamento in corso di dati personali che lo riguardano
2. Le finalità e il titolo giuridico del trattamento;
3. Le categorie di dati personali trattati;
4. I destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati;
5. Il periodo di conservazione dei dati personali o, se non è possibile, i criteri per determinare tale periodo

Altri diritti
1. Rettifica
2. Cancellazione (se in contrasto con l'art. 3)
3. Limitazione del trattamento
4. Proporre reclamo al Garante
5. Comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.
6. Integrazione

ECCEZIONI (ART. 14)

In alcuni casi la richiesta da parte dell'INTERESSATO può essere rifiutata se i dati sono contenuti in
- una decisione giudiziaria,
- in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini,
- nel casellario giudiziale
- in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale,

Inoltre, l'esercizio dei diritti può essere ritardato, limitato o escluso, con nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata.

La limitazione può avvenire per le seguenti finalità:
a) non compromettere il buon esito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza;
b) tutelare la sicurezza pubblica;
c) tutelare la sicurezza nazionale;
d) tutelare i diritti e le libertà altrui.

IN CASO DI RIFIUTO (ART 12C5)

L'interessato ha diritto di essere **informato per iscritto dal titolare del trattamento del rifiuto** di rettifica, di cancellazione o di limitazione del trattamento e dei **relativi motivi.**
Di fronte al rifiuto si può proporre reclamo dinanzi al Garante o di proporre ricorso giurisdizionale davanti al Tribunale.

Questo significa che, se hai fatto una richiesta di accesso, il titolare non può limitarsi a non rispondere oppure rispondere negativamente, ma deve spiegarti il motivo

COSA FARE IN PRATICA

→ Le banche dati della polizia sono disponibili a questo link
→ La banca dati AFIS, dovrebbe essere contenuta all'interno della Banca dati del DNA
→ Per scoprire se il tuo volto è all'interno di una delle banche dati puoi usare questo modulo.

ATTENZIONE. Da quando invii il modulo scattano i 30 giorni per ottenere una risposta! Imposta un timer, una sveglia, segnalo nell'agenda o nel calendario.

Dopo i 30 giorni dovresti ricevere una risposta da parte dell'autorità competente.
Hai avuto la risposta che cercavi?

✅ Sì, molto bene! Speriamo non ti serva altro.

❌ **No. Allora la faccenda si complica.** → *Puoi proporre un reclamo al Garante o ricorre al Tribunale*

- Per il reclamo al Garante, usa questo modulo
- Per ricorrere ad un tribunale dovrai rivolgerti ad un avvocato (in generale, è sempre
- consigliabile farsi seguire da qualcuno di esperto)

→ Se pensi di essere stata soggetta ad identificazione biometrica e che i tuoi diritti siano stati violati, contattaci tramite i nostri canali social oppure alla nostra email:
info@strali.org - contatti@privacy-network.it.

CONCLUSIONI

La nostra posizione.

Dopo avere analizzato i dati che siamo riusciti a ricostruire e averne fatto un'analisi giuridica, riteniamo che l'impiego del riconoscimento facciale, come qualunque altra forma di **identificazione biometrica, non rappresenti uno strumento di indagine realmente utile e che i rischi derivanti dall'utilizzo superino di gran lunga i benefici.**

Privacy Network e STRALI sono parte della RETE DIRITTI UMANI DIGITALI.
Pertanto richiediamo il divieto assoluto di questo tipo di tecnologia, tanto nelle sue versioni in tempo reale quanto ex post.

Il motivo per cui riteniamo che le tecnologie di sorveglianza biometrica debbano essere sottoposte ad un veto non deve essere frainteso. **Il progresso tecnologico non va rifiutato ma governato con metodo scientifico.**

Il problema che ci troviamo ad affrontare non riguarda solamente l'introduzione di uno strumento tecnologico, quanto l'approccio alla sicurezza in sé.

Negli ultimi decenni il tema della sicurezza ha smesso di essere oggetto di dibattito critico. L'argomento viene affrontato, a livello politico e mediatico, attraverso una sequenza di luoghi comuni. **Ad essere completamente assente è un'analisi della realtà fondata sui dati, tanto delle esigenze del territorio, quanto dell'efficacia delle misure.**

L'intero discorso sulla sicurezza spesso sconta una serie di errori di partenza che rendono pressoché impossibile proporre alternative alla mera risposta repressiva.

In primo luogo, l'unica metrica utilizzata per misurare la sicurezza delle nostre città è il numero di reati commessi. Non ci poniamo alcune domande altrettanto importanti (Ad es.: È sicura una città in cui la qualità dell'aria è tanto scarsa da farci ammalare?).

Inoltre, il numero di arresti viene presentato come una misura di prevenzione, quando in realtà vuol dire proprio il contrario. Se c'è un arresto, un reato è già stato presumibilmente commesso, e quindi **la prevenzione ha fallito**. Tappezzare la città di sensori non serve senza tribunali efficienti e strutture carcerarie adeguate alla riabilitazione di chi viene condannato.

In secondo luogo, **ci si rifiuta di vedere le cause profonde della microcriminalità, in primis l'esclusione sociale**.

Come si può pensare di costruire comunità sicure se non esistono mezzi per far fronte all'ingiustizia sociale e chi nasce in un certo contesto è (quasi) sempre automaticamente condannato ad una vita fuori dalla legalità?

Infine vi è il rifiuto sistematico di riconoscere che **le tecnologie di sorveglianza possono creare rischi per la democrazia**. Perché ciò significherebbe ammettere che l'abuso di una posizione di autorità è qualcosa di reale.

Questo approccio semplicistico **nasce dal rifiuto della politica di applicare il metodo scientifico tanto nella fase dell'analisi dei bisogni della società, quanto nella revisione periodica delle politiche di contrasto alla criminalità.**

Non è difficile immaginare il motivo per cui tale atteggiamento trova sempre più fortuna: per i rappresentanti politici è molto più semplice vendere soluzioni apparentemente perfette, piuttosto che attuare strategie di lungo periodo.

Per chi sviluppa sistemi tecnologici, vuol dire incassare grossi profitti dalla vendita di sistemi di sorveglianza; mentre per i media è molto più semplice generare attenzione attraverso una rappresentazione della realtà esagerata, piuttosto che dare al pubblico analisi complesse.

Fintanto che l* cittadin* non riescono a mettere in discussione questa prospettiva, non possiamo aspettarci risposte serie e concrete dalle forze politiche.

L'incapacità di leggere le cause della criminalità ed elaborare soluzioni efficaci, si traduce nella rincorsa continua di soluzioni di facciata, come l'acquisto di nuove telecamere che non portano alcuna utilità se non il profitto delle aziende.

Tappezzare la città di sensori, creare enormi banche dati ed espandere sempre di più i poteri della polizia è inutile in assenza di politiche di lungo termine che sappiano dare risposte ai reali bisogni della cittadinanza, ripartendo dagli investimenti in ambito sociale e garanzie reali per l* cittadin*

LE NOSTRE RICHIESTE AL MINISTERO DELL'INTERNO

I sistemi di riconoscimento facciale sono già ampiamente in uso. Se non si volesse procedere con la sospensione totale di queste tecnologie, allora il loro utilizzo dovrebbe quantomeno essere adeguato ai dettami legislativi ed alle buone prassi elaborate nel corso degli anni.

Chiediamo pertanto, alle autorità competenti di mettere in atto le seguenti azioni:

1. **Adozione di un registro pubblico dei sistemi di identificazione biometrica in uso alla polizia;**
2. **Implementazione di un sistema di verifica dei risultati;**
3. **Implementazione di un sistema di conteggio del numero di persone all'interno dei database;**
4. **Revisione del parere emesso dal Garante;**
5. **Redazione della DPIA in relazione al sistema SARI;**
6. **Implementazione di misure dedicate di salvaguardia per i diritti e le libertà fondamentali;**
7. **Implementazione di una pagina dedicata nella sezione privacy del sito della Polizia di Stato e delle altre forze dell'ordine;**
8. **Emanazione del decreto di cui all'art. 49 del D.Lgs. 51/2018, nella versione precedente alla modifica di cui al milleproroghe;**
9. **Adozione formale e pubblicazione di linee guida sull'utilizzo del riconoscimento facciale per fini di polizia;**
10. **Creazione di un organismo di vigilanza sull'utilizzo.**

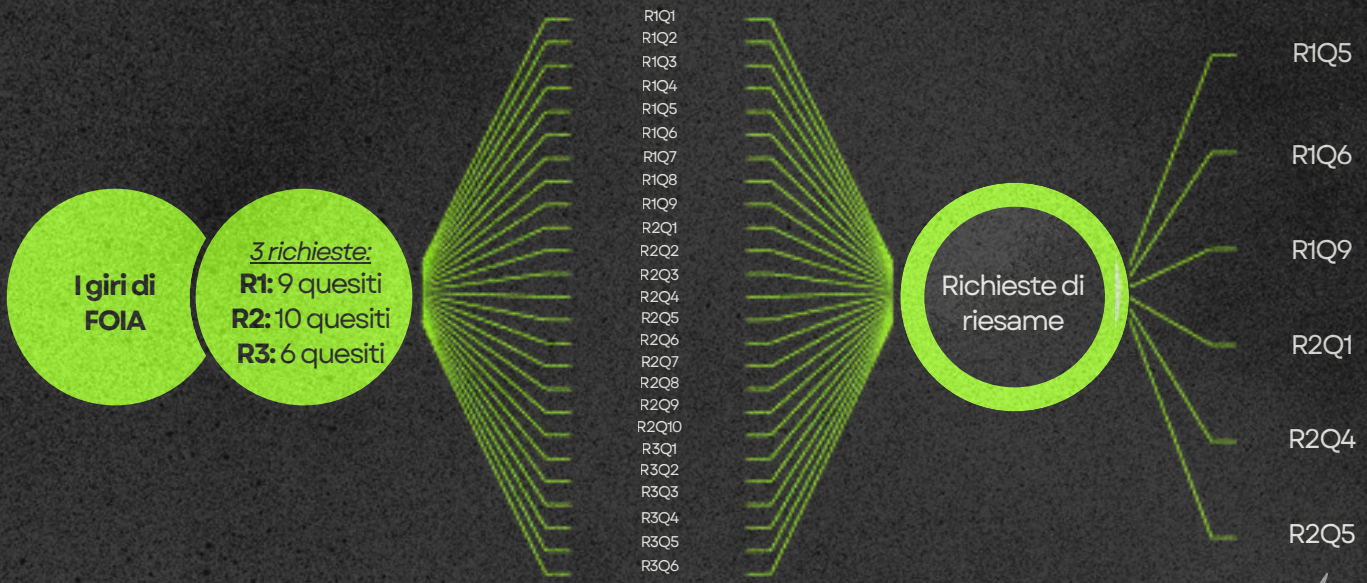
APPROFONDIMENTO

A.1 → Ricorso al TAR

Non sempre le pubbliche amministrazioni rispondono come ci aspetteremmo alle richieste, in questo caso non tutte le nostre domande erano state soddisfatte. Questo però non vuol dire autonomamente che il rifiuto sia legittimo. DI fronte al silenzio o a risposte insoddisfacenti, si possono usare diversi metodi di ricorso.

Le prime richieste di accesso FOIA:

Le richieste di riesame: (perché abbiamo selezionato solo determinati casi di diniego)



Vedi nella pagina successiva le domande e le risposte che abbiamo ricevuto dopo le nostre richieste di riesame

R1Q5

QUESITO:

Se viene effettuata una periodica valutazione dell'efficacia delle misure adottate per tutelare i diritti degli interessati

RISPOSTA:

Non sono previste valutazioni periodiche dell'efficacia delle misure adottate; l'Ufficio adotta tutte le precauzioni necessarie per impedire l'accesso non autorizzato o l'uso improprio dei dati; sono inoltre in vigore procedure di verifica interne volte a garantire la costante tutela dei diritti degli interessati

R1Q6

QUESITO:

Copia di eventuali Valutazioni d'Impatto sulla Protezione dei Dati (DPIA) redatte ai sensi dell'art. 35 GDPR, nonché di altre valutazioni di rischio interne

RISPOSTA:

Si rimanda alle motivazioni espresse nel parere del Garante per la protezione dei dati del 26 luglio 2018, in merito al SARI Enterprise.

R1Q9

QUESITO:

La frequenza e risultati di eventuali audit o verifiche sul indipendenti rispetto delle misure di protezione dei dati

RISPOSTA:

L'ufficio opera nel rispetto della normativa vigente, adottando le misure necessarie a garantire la protezione dei dati personali e i diritti degli interessati, in conformità con le linee guida e le direttive emanate dalle autorità competenti, definiscono le che modalità operative e le procedure. Viene prestata costante attenzione all'efficacia e all'adeguatezza delle misure adottate.

R2Q1

QUESITO:

Se esiste un documento che descrive e disciplina le condizioni d'uso

RISPOSTA:

Si rimanda alle motivazioni espresse nel parere del Garante per la protezione dei dati del 26 luglio 2018, in merito al SARI Enterprise.

R2Q4

QUESITO:

Se sono state stabilite procedure volte a garantire i diritti e le libertà delle persone interessate e, in caso affermativo, quali siano

RISPOSTA:

Si rimanda alle motivazioni espresse nel parere del Garante per la protezione dei dati del 26 luglio 2018, in merito al SARI Enterprise.

R2Q5

QUESITO:

Se esiste un documento che elenca i tipi di reati per i quali è possibile utilizzare il sistema SARI

RISPOSTA:

Si rimanda alle motivazioni espresse nel parere del Garante per la protezione dei dati del 26 luglio 2018, in merito al SARI Enterprise.

LE NOSTRE ARGOMENTAZIONI PER IL RIESAME:

Abbiamo basato le nostre richieste di riesame su due argomentazioni principali:

- Risposte prive di informazioni concrete. Inoltre, non vi sono prove che tali dati relativi a SARI Enterprise siano stati pubblicati altrove.
- La documentazione richiesta non è inclusa nel parere dell'Autorità Garante per la Protezione dei Dati.

LA RISPOSTA DEL MINISTERO

Il RPCT del Ministero, in risposta alla nostra richiesta di riesame, ha affermato che:

- Non sono previsti piani per la valutazione periodica dell'efficacia delle misure adottate a tutela dei diritti degli interessati;
- Non sono previsti audit o controlli indipendenti per verificare il rispetto delle garanzie in materia di protezione dei dati.
- In merito alla DPIA: «L'Autorità per la protezione dei dati ha ampiamente illustrato i motivi per cui il trattamento dei dati personali che sarà effettuato tramite il sistema SARI Enterprise non presenta criticità in termini di protezione dei dati. Si precisa che questo Servizio non dispone di altra documentazione».
- Il sistema SARI Enterprise non effettua alcun trattamento aggiuntivo rispetto all'AFIS-SSA, ma si limiterà ad automatizzare alcune operazioni che in precedenza richiedevano l'inserimento manuale delle caratteristiche identificative. Pertanto, tutta la normativa applicabile all'AFIS-SSA si applica anche a SARI.

QUALIFICARE LA (NON) RISPOSTA DEL MINISTERO COME RIFIUTO ILLEGITTIMO

Il quadro normativo del FOIA è concepito per i rifiuti espliciti. L'amministrazione fa solitamente riferimento all'art. 5-bis del D.Lgs. 33/2013 (ad es. sicurezza nazionale, ordine pubblico).

La procedura può essere riassunta come segue:

> Il richiedente contesta l'eccezione → **il tribunale valuta la necessità e la proporzionalità** → il tribunale dichiara il rifiuto illegittimo o lo conferma.

Risultato: un terreno ben delineato con una giurisprudenza consolidata.

Quello che si è presentato davanti a noi è invece un caso insolito: una risposta evasiva senza un rifiuto esplicito. Il Ministero dell'Interno non ha mai invocato le eccezioni previste dalla legge.

Il problema diventa perciò strutturale: come contestare una risposta formalmente conforme ma sostanzialmente nulla? Il quadro normativo del FOIA, infatti, presuppone un rifiuto da contestare. Non esiste una disposizione chiara che disciplini un rinvio sistematico che funga da rifiuto velato. Per questo, il nostro contenzioso ha dovuto basarsi su motivi non convenzionali.

L'ARCHITETTURA DELLE NOSTRE ARGOMENTAZIONI GIURIDICHE ALLA BASE DEI RICORSI (T.A.R.) IN CORSO

- **«Risposta apparente»:** ai sensi della Circolare n. 2/2017 sulla FOIA, par. 7, una risposta parziale priva di spiegazioni in merito alle omissioni equivale a un rifiuto parzialmente illegittimo.
- **Incoerenza sostanziale:** il Ministero ha sistematicamente fatto riferimento a un parere del Garante del 2018 che non contiene i documenti richiesti. Il rinvio a un documento che non risponde alla domanda non costituisce una risposta.
- **Disallineamento temporale:** il parere del 2018 valutava il progetto SARI nella sua fase di progettazione. Le nostre richieste riguardavano il sistema operativo. Il rinvio è sia insufficiente che categoricamente inappropriato.

LETTURE PER APPROFONDIRE

L'importanza della trasparenza della pubblica amministrazione

- *Corte europea dei diritti dell'uomo caso Magyar c. Ungheria, 8 novembre 2016, § 165).*

Discriminazione tramite algoritmi

- *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia. Cathy O'Neil. Bompiani, 2017*

Sentenze sul riconoscimento facciale

- *Corte e.d.u., 4 luglio 2023, Glukhin c. Russia*

Seguici sui social di Privacy Network e Strali

Questo report è stato realizzato da:

STRALI
strategic litigation

PRIVACY NETWORK

PER MAGGIORI INFORMAZIONI:

privacy-network.it
www.strali.org

Funded by European Artificial Intelligence & Society Fund