

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, Bianca Stella Bruschi,
Maria Vittoria Capra, Angela Cianfagna Bracone, Federica Genovesi,
Alice Giannini, Lorenzo Sottile

Impaginato da: Serena Brighenti e Anna Florian

Aggiornato al: 17.09.2026

*Progetto “Building Accountability for Law Enforcement Facial
Recognition (SARI) in Italy”*

Funded by European
Artificial Intelligence
& Society Fund

INDICE

Introduzione		4
• Perché questa indagine? • Come abbiamo indagato		
Sezione 1	COME FUNZIONA UN SISTEMA DI RICONOSCIMENTO FACCIALE	8
• Come funziona (in teoria) • Tempo • Spazio • Utilizzo in tempo reale • Utilizzo ex-post • I rischi del riconoscimento facciale		
Sezione 2	IL RICONOSCIMENTO FACCIALE IN ITALIA: COME FUNZIONA SARI ENTERPRISE	14
LA BANCA DATI AFIS 17		
• Quali soggetti contiene AFIS • Il fotosegnalamento		
RISULTATI DELL'INDAGINE 19		
1. Scarsa collaborazione da parte delle autorità 2. Assenza di dati sull'efficacia e sui tassi d'errore 3. Uso crescente del riconoscimento facciale dalle forze dell'ordine 4. Evidenti criticità nel rispetto della normativa di riferimento		
DIRITTI FONDAMENTALI 24		
I tuoi diritti e come proteggerli		26
• La legge sul trattamento dei dati personali • Cosa fare in pratica		
Conclusioni		29
Le nostre richieste per il Ministero dell'interno		31
Approfondimento: RICHIESTA FOIA E RICORSO AL TAR 32		
• PT I: Le richieste di accesso FOIA 32 • PT II: I ricorsi al TAR 37 • L'Italia a confronto con l'Europa 43		

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

Il riconoscimento facciale è una tecnologia capace di identificare una persona a partire dal suo volto. È quindi uno strumento particolarmente invasivo, perché permette di trasformare una caratteristica fisica unica in un dato biometrico utilizzabile per riconoscerci, anche a distanza e senza che ce ne accorgiamo. Negli ultimi anni queste tecnologie si sono diffuse rapidamente, nel settore privato come in quello pubblico. Anche in Italia esiste un sistema di riconoscimento facciale utilizzato dalle forze dell'ordine, SARI Enterprise. Eppure, alla crescente capacità tecnologica delle autorità non ha corrisposto un analogo livello di trasparenza. Per anni il dibattito pubblico è stato quasi inesistente e le informazioni disponibili sono rimaste poche, frammentarie e spesso vaghe.

È da qui che nasce la nostra indagine.

Questo tipo di tecnologia ha un impatto sui diritti e sulle libertà fondamentali di ognuna di noi (uguaglianza, libertà di manifestazione del pensiero, libertà di riunione, ecc.), tale da ridisegnare il rapporto fra cittadini e autorità. Comprendere come viene utilizzata significa interrogarsi su chi può essere identificato, in quali circostanze, sulla base di quali regole, con quali margini di errore e con quali possibilità di controllo. Significa, soprattutto, evitare che strumenti di sorveglianza particolarmente invasivi come questi vengano progressivamente normalizzati.

I rischi non sono soltanto teorici. Sono numerosi gli esempi nel mondo di tecnologie di riconoscimento facciale utilizzate in maniera distorta, più come strumenti di sorveglianza e repressione politica che come mezzi per garantire la sicurezza dei cittadini.

Negli Stati Uniti, già nel 2016, circa metà della popolazione adulta risultava presente in reti di database accessibili alle forze dell'ordine per il riconoscimento facciale, comprese persone che non avevano mai commesso reati.¹

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

In Russia, il riconoscimento facciale è stato utilizzato anche per identificare partecipanti a proteste e forme di dissenso politico; proprio l'impiego della tecnologia per identificare, localizzare e arrestare un manifestante ha portato, nel caso Glukhin c. Russia, alla prima pronuncia della Corte europea dei diritti dell'uomo specificamente dedicata al suo utilizzo da parte delle autorità. Analoghi rischi sono emersi in Ungheria, Iran, Cina e in molti altri Paesi. Perché l'utilizzo del riconoscimento facciale non sfoci in abuso, **la trasparenza è una condizione essenziale**. Occorre sapere come questi sistemi vengono utilizzati, quali limiti incontrano e quali risultati producono. Solo sulla base di informazioni precise e verificabili cittadine e cittadini possono formarsi un'opinione consapevole, mentre giornalisti e società civile possono esercitare il proprio ruolo di controllo. All'interno di una società democratica, infatti, l'introduzione di strumenti capaci di incidere così profondamente sulla vita delle persone non può essere sottratta al vaglio pubblico.

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

I sistemi di riconoscimento facciale sono tecnologie complesse il cui elemento centrale è un software in grado di riconoscere il volto di una persona all'interno di una fotografia o di un frame video e associarlo a un'identità nota presente in 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



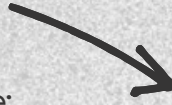
Una (o più) **TELECAMERE**



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. A ciò si aggiungono i **costi**, tanto in termini economici quanto di tempo e di 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 analizzati e confrontati 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

L'utilizzo delle tecnologie di riconoscimento facciale presenta rischi significativi per i diritti e le libertà fondamentali

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 Glukhin**. 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 giustificano, 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 ECONOMICI E ORGANIZZATIVI DEL SISTEMA

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 cittadine 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 che 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.

I 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 fotosegnalatici.**



C'è altro in Italia?

Un altro caso documentato riguarda lo Stadio Olimpico di Roma, dove è stato utilizzato un sistema di riconoscimento facciale collegato alla videosorveglianza degli accessi. Il sistema era stato oggetto già nel 2016 di una verifica preliminare del Garante per la protezione dei dati personali.

Una successiva [inchiesta di IrpiMedia](#) ha però ricostruito che, tra il 2021 e il 2025, le telecamere installate allo stadio fotografavano più volte gli spettatori in ingresso, associando le immagini ai dati del biglietto. Nel maggio 2025 il Garante ha chiesto al Ministero dell'Interno di sospendere l'utilizzo del riconoscimento facciale, ritenendo che il trattamento avvenisse in assenza di un'adeguata base giuridica.

Oltre a questo, [un'inchiesta di Fanpage.it](#) sembrerebbe indicare l'acquisto da parte dei carabinieri di un sistema di riconoscimento facciale noto come Corsight. Tuttavia non sono disponibili ulteriori informazioni pubbliche.

LA BANCA DATI AFIS

SARI Enterprise funziona, in sostanza, come un sistema automatizzato di ricerca all'interno della banca dati AFIS. Questo significa che può essere utilizzato per identificare chi è presente nel database e che, se i tuoi dati sono inseriti in AFIS, puoi esercitare i diritti previsti dalla normativa sulla protezione dei dati personali.

QUALI SOGGETTI CONTIENE AFIS?

Il vero problema, dal punto di vista della tenuta dello Stato di diritto, non riguarda soltanto il sistema di ricerca, ma anche la **banca dati su cui esso opera**. La concentrazione di grandi quantità di dati biometrici all'interno di un database di polizia pone infatti questioni rilevanti di **trasparenza, proporzionalità e rischio di discriminazione**, soprattutto quando vi confluiscono anche persone che non hanno commesso alcun reato.

AFIS contiene dati biometrici, tra cui fotografie del volto e impronte digitali, di **persone sottoposte a fotosegnalamento**, ma vi confluiscono anche i **dati di cittadine straniere raccolti per finalità amministrative**, ad esempio nell'ambito delle procedure di rilascio, rinnovo o conversione del permesso di soggiorno. Ciò significa che i **dati raccolti senza alcun collegamento con la commissione di un reato vengono inseriti nella stessa banca dati utilizzata dalle forze di polizia per finalità investigative**. È proprio questa differenza di trattamento, fondata sulla nazionalità, ad essere stata contestata da ASGI come discriminatoria.

Secondo le indagini svolte da ASGI e da Irpimedia, nel 2022 AFIS conteneva 13.516.259 cartellini riferiti a cittadine di Paesi extra-UE, 1.654.917 a cittadine di altri Stati membri dell'Unione europea e 3.289.196 a cittadine italiane. Nel 2023 sono stati inoltre registrati 992.093 ulteriori fotosegnalamenti.

Nell'ambito della nostra indagine **abbiamo chiesto al Ministero dell'Interno dati aggiornati** sulla consistenza e sulla composizione del database. In un primo momento l'Amministrazione ha negato l'accesso, sostenendo che l'estrazione e l'aggregazione dei dati avrebbero comportato la creazione di un nuovo documento. Abbiamo contestato tale impostazione davanti al TAR, che ha annullato il diniego su questo punto, chiarendo che l'estrazione di dati numerici già presenti nel database non costituisce di per sé la creazione di un nuovo documento.

In esecuzione della sentenza, il Ministero ha comunicato che nel 2024 risultavano 956.534 cartellini fotosegnalatici, di cui 76.443 riferiti a cittadine italiane, 14.938 a cittadine dell'Unione europea (non italiane), 764.787 a cittadine extra-UE e 100.366 privi dell'indicazione della nazionalità.

Alla luce dei dati precedentemente disponibili, questa cifra sembra riferirsi ai fotosegnalamenti effettuati nel corso del 2024 piuttosto che al numero complessivo dei cartellini presenti nel database. Il Ministero **non ha tuttavia fornito elementi sufficienti** per chiarire definitivamente questo aspetto.

Anche considerando il dato come riferito ai soli inserimenti del 2024, emerge una **forte sproporzione nella composizione del database**: circa l'80% dei cartellini complessivamente comunicati riguarda cittadine extra-UE, percentuale che supera l'89% se si considerano soltanto i record per i quali la nazionalità è indicata.

L'importanza del numero di soggetti presenti nel database e delle loro caratteristiche demografiche **non deve essere sottovalutata**.

Se alcuni gruppi risultano fortemente sovrarappresentati, aumenta anche la probabilità che compaiano tra i risultati prodotti dal sistema, con possibili conseguenze negative in caso di identificazioni errate. Per questo, oltre alla qualità dell'algoritmo, è essenziale interrogarsi anche sulla composizione, sulle finalità e sulle modalità di gestione della banca dati di riferimento.

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

IL FOTOSEGNALAMENTO

Poiché l'inserimento in AFIS avviene a seguito del **fotosegnalamento**, è importante comprendere con chiarezza **come questa operazione venga effettuata** e distinguerla da altre modalità di identificazione. Da alcuni anni riceviamo testimonianze di persone fotografate dalle forze dell'ordine, anche attraverso dispositivi personali degli agenti, nell'ambito di attività di identificazione. Non è però chiaro se e in quali casi l'acquisizione di una fotografia con queste modalità comporti anche il successivo inserimento dell'immagine nella banca dati AFIS.

*La prassi di mantenere all'interno dello stesso database persone con precedenti penali e cittadine straniere 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.*

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

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

RISULTATI DELL'INDAGINE

Alla luce delle informazioni raccolte attraverso le richieste di accesso, delle risposte ricevute dal Ministero dell'Interno e degli esiti dei due contenziosi promossi davanti al TAR Lazio, possiamo trarre alcune conclusioni.

1

SCARSA COLLABORAZIONE DA PARTE DELLE AUTORITÀ E TRASPARENZA ANCORA LIMITATA

L'indagine ha evidenziato persistenti **difficoltà nell'accesso a informazioni e documenti** relativi al funzionamento di SARI Enterprise. Una parte delle nostre richieste, soprattutto quelle riguardanti le garanzie per i diritti fondamentali, il funzionamento operativo del sistema e la composizione della banca dati AFIS, ha ricevuto **risposte generiche, parziali o veri e propri dinieghi**.

I due **ricorsi promossi davanti al TAR Lazio** hanno consentito di superare almeno in parte questa opacità, facendo emergere informazioni che non erano state fornite in seguito alle richieste FOIA. In particolare, nel corso del primo giudizio è stata confermata l'assenza di una specifica valutazione d'impatto sulla protezione dei dati relativa a SARI Enterprise; il secondo contenzioso ha, invece, consentito di ottenere dati ufficiali sulla composizione di AFIS e sui controlli di qualità delle immagini.

Altri aspetti, soprattutto quelli relativi al funzionamento tecnico del sistema, alla formazione degli operatori e alle modalità del coinvolgimento umano nell'utilizzo di SARI Enterprise, **sono rimasti sottratti all'accesso**. Il quadro che emerge resta quindi caratterizzato da una **trasparenza solo parziale**.

Questa esperienza evidenzia anche come l'efficacia della strategia FOIA dipenda dalla reale collaborazione delle istituzioni. L'accesso civico generalizzato è uno strumento gratuito, pensato per favorire la trasparenza e il controllo diffuso sull'operato delle amministrazioni. Quando, però, informazioni rilevanti vengono negate o rese accessibili solo a seguito di un ricorso al TAR, che richiede tempo e risorse economiche, il rischio è che la funzione stessa del FOIA venga fortemente depotenziata. Nel nostro caso, senza il contenzioso non avremmo ottenuto alcune delle informazioni più importanti emerse dall'indagine.

2

ASSENZA DI DATI SULL'EFFICACIA e SUI TASSI DI ERRORE

Utilizzare un algoritmo di intelligenza artificiale non significa, di per sé, ottenere risultati affidabili. **La capacità del sistema di individuare con chiarezza una persona dipende da diversi fattori**. Le caratteristiche demografiche (etnia, età, sesso) possono incidere sulle prestazioni dell'algoritmo.

Anche la qualità delle immagini è determinante. Le immagini disponibili nel corso di un'indagine 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**. Su questo punto, a seguito del secondo contenzioso, il Ministero ha confermato che SARI Enterprise effettua una valutazione automatizzata della qualità delle immagini prima dell'estrazione del dato biometrico e che quelle che non raggiungono i requisiti minimi di idoneità vengono scartate.

Controllare la qualità delle immagini, tuttavia, non equivale a misurare l'efficacia del sistema. Per capire se SARI Enterprise sia effettivamente utile come strumento investigativo servono dati precisi sui tassi di efficacia registrati in concreto, non soltanto sulle prestazioni dell'algoritmo in condizioni sperimentali.

SARI Enterprise restituisce infatti una lista di possibili corrispondenze, successivamente sottoposte alla valutazione degli operatori. Abbiamo quindi chiesto quanti risultati prodotti dal sistema abbiano consentito concretamente di proseguire un'indagine e con quale frequenza le corrispondenze suggerite si siano rivelate errate. In altre parole: **quante volte SARI Enterprise permette davvero di individuare la persona ricercata?**

Nonostante il sistema sia utilizzato dalle forze dell'ordine da circa 8 anni, il Ministero dell'Interno ha dichiarato di non disporre di dati sulla sua effettiva efficacia. Non risultano raccolti neppure dati sistematici sui falsi positivi, cioè sui casi in cui il sistema restituisce tra i propri risultati una persona che non corrisponde a quella ricercata.

Si tratta di una **lacuna particolarmente significativa**, anche perché le linee guida prese come riferimento per l'utilizzo di sistemi di riconoscimento facciale dedicano specifica attenzione alla valutazione delle prestazioni e alla configurazione del sistema in relazione alle diverse esigenze investigative. Secondo le informazioni raccolte da IrpiMedia, inoltre, l'algoritmo utilizzato da SARI avrebbe mostrato **prestazioni differenti a seconda delle caratteristiche demografiche** dei soggetti analizzati. Per le persone non bianche, la probabilità di individuare la persona ricercata tra i primi dieci risultati era pari a circa il 77%.

Ad oggi non disponiamo di dati aggiornati.

L'assenza di dati sull'efficacia ci sembra uno degli elementi più sorprendenti emersi dall'indagine. Si tratta infatti dell'informazione essenziale per comprendere se SARI Enterprise sia realmente utile alle forze dell'ordine. Al di là delle esigenze di trasparenza verso l'esterno, raccogliere questi dati dovrebbe servire alla stessa Amministrazione per verificare, sulla base di elementi oggettivi, se una tecnologia così sofisticata produca effettivamente risultati proporzionati alle risorse impiegate e ai rischi che comporta.

Sino ad ora, abbiamo individuato soltanto due casi giudiziari di pubblico dominio nei quali SARI Enterprise è stato utilizzato per l'identificazione dell'imputato. Nel primo, la percentuale di somiglianza restituita dal sistema era pari al 52%. Nel secondo, il risultato prodotto da SARI Enterprise si è rivelato sostanzialmente inutilizzabile. In entrambi i casi, l'accertamento giudiziario ha richiesto l'esame di ulteriori elementi probatori.

Il problema, quindi, non riguarda soltanto la trasparenza. Quando un'amministrazione investe in uno strumento tecnologico destinato all'attività investigativa, dovrebbe essere in grado di verificarne nel tempo l'effettiva utilità. In assenza di un monitoraggio dei risultati, **diventa difficile stabilire se le risorse pubbliche impiegate producano un beneficio concreto** o se si stia continuando a utilizzare una tecnologia senza disporre degli elementi necessari per valutarla.

In altri Paesi, come il Regno Unito, i risultati dell'utilizzo dei sistemi di riconoscimento facciale sono oggetto di pubblicazione periodica e il funzionamento degli algoritmi impiegati dalle forze di polizia è stato sottoposto anche a valutazioni indipendenti accessibili al pubblico.

3

DATI SULL'UTILIZZO IN CRESCITA

Pur continuando a mancare dati che consentano di valutarne l'efficacia concreta, l'utilizzo di SARI Enterprise è **creciuto sensibilmente negli ultimi anni**, anche se la ricerca senza impiego di algoritmi rimane largamente più utilizzata.

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

- nel 2019 è stato utilizzato 41.888 volte;
- nel 2020 è stato utilizzato 38.315 volte;
- nel 2021 è stato utilizzato 52.539 volte;
- 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;

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

MODALITÀ 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

Uno dei profili più problematici emersi dalla nostra indagine riguarda il **rispetto della normativa applicabile**, sia con riferimento alla disciplina sul trattamento dei dati personali per finalità di polizia, contenuta principalmente nel d.lgs. n. 51/2018, sia rispetto alle garanzie previste a tutela dei diritti fondamentali.

Il quadro normativo italiano è stato finora frammentario e privo di una disciplina organica specificamente dedicata all'utilizzo del riconoscimento facciale da parte delle forze dell'ordine. Al momento della nostra indagine, il principale riferimento era rappresentato dalla normativa sul trattamento dei dati personali per finalità di polizia. Il quadro è tuttavia in *fase di evoluzione* perché nell'estate del 2026 il Governo ha iniziato a lavorare su uno schema di decreto legislativo di adeguamento all'AI Act che introduce una disciplina specifica per l'utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia, compreso il riconoscimento facciale in tempo reale e a posteriori.

SARI Enterprise è stato sottoposto nel 2018 all'esame del Garante per la protezione dei dati personali, il quale ne ha autorizzato l'impiego fornendo un parere positivo. Bisogna però 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 la conformità di SARI Enterprise alla normativa applicabile, la nostra ricerca si è incentrata in particolare su due aspetti: **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, **il trattamento deve essere preceduto da una valutazione d'impatto sulla protezione dei dati personali** (DPIA), prevista dall'art. 23 del d.lgs. n. 51/2018.

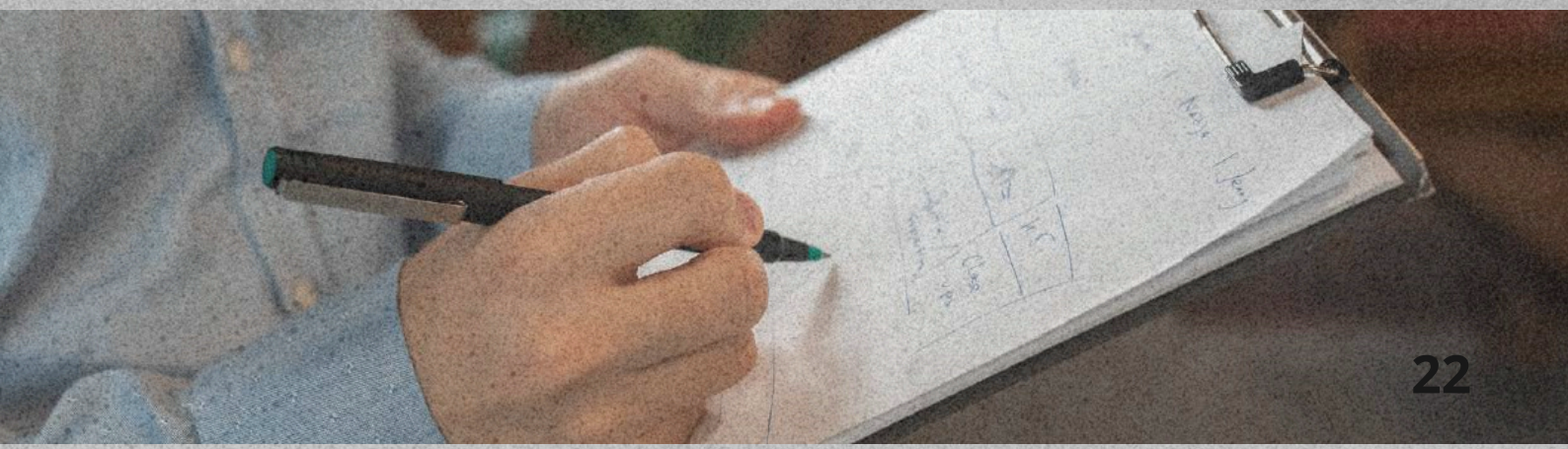
La valutazione serve a individuare preventivamente i rischi connessi al trattamento e le misure necessarie per mitigarli. Nel caso del riconoscimento facciale, queste garanzie assumono particolare importanza perché il sistema tratta dati biometrici, sottoposti a una tutela particolarmente rigorosa. Questi passaggi sono espressamente previsti per legge e sono **fondamentali per garantire un utilizzo corretto del sistema e assicurare il rispetto dei diritti** delle cittadine. Alle nostre richieste di accesso il Ministero aveva risposto rinviando genericamente al parere del Garante per la protezione dei dati personali del 2018, senza chiarire se fosse stata predisposta una specifica valutazione d'impatto. La questione è stata chiarita soltanto grazie al primo ricorso davanti al TAR Lazio. Nel corso del giudizio, il Ministero ha dichiarato che **la DPIA relativa a SARI Enterprise non è mai stata predisposta**.

L'assenza di una specifica valutazione d'impatto rappresenta una delle criticità più rilevanti emerse dall'indagine. A nostro avviso, tale omissione pone seri interrogativi sulla conformità del trattamento agli obblighi previsti dall'art. 23 del d.lgs. n. 51/2018.

LA PROCEDURA DI GARANZIA DEI DIRITTI E DELLE LIBERTÀ DEI CITTADINI

Più **incerto** è invece il quadro relativo alle condizioni di utilizzo di SARI Enterprise e alle procedure previste a tutela dei diritti e delle libertà degli interessati, anch'esse richieste dalla normativa applicabile. Anche su questo punto, la prima risposta del Ministero si è limitata a un generico rinvio al parere del Garante del 2018, che non contiene però una disciplina dettagliata delle procedure né la documentazione richiesta. A una successiva istanza, l'Amministrazione ha dichiarato di non disporre di ulteriore documentazione.

Questa risposta ha fatto sorgere il dubbio che tali procedure non esistano, non siano mai state formalizzate in documenti specifici o, quantomeno, non siano rese conoscibili all'esterno. Si tratta di una carenza particolarmente rilevante anche sul piano della trasparenza, considerando che in altri Paesi documenti analoghi sono pubblicati online e liberamente consultabili.



ALTRE CRITICITÀ SOTTO IL PROFILO DELLA LEGALITÀ

PER QUALI REATI VIENE UTILIZZATO SARI

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 importanti sia per valutarne l'efficacia sia per verificare la necessità e la proporzionalità dell'interferenza con i diritti fondamentali. Al momento l'ipotesi più probabile è che SARI Enterprise venga utilizzato per qualunque reato, senza distinzioni.

INFORMATIVA AGLI INTERESSATI

Un'ulteriore criticità riguarda le informazioni rese alle persone i cui dati sono contenuti nella banca dati AFIS, in particolare rispetto alle modalità con cui possono esercitare i propri diritti. A differenza di quanto avviene per altre banche dati utilizzate dalle forze di polizia, non risulta disponibile una pagina pubblica dedicata ad AFIS che illustri in maniera organica le finalità del trattamento, i tempi di conservazione e le modalità di esercizio dei diritti.

QUANTO A LUNGO SI RESTA NEI DATABASE DELLA POLIZIA

I tempi di conservazione dei dati personali in AFIS sono estremamente lunghi. I dati relativi ai "controlli di polizia" vengono anonimizzati dopo 20 anni dal fotosegnalamento, mentre quelli riferiti ad "attività di polizia giudiziaria" dopo 40 anni.

Questo significa che, una volta fotosegnalata, una persona può rimanere all'interno della banca dati per decenni. Tempi così estesi rendono molto difficile uscire effettivamente dal sistema, anche perché la conservazione può essere ulteriormente prolungata nei casi previsti dalla normativa.

FORMAZIONE PER LA POLIZIA

Un'ulteriore criticità riguarda la formazione del personale abilitato all'utilizzo di SARI Enterprise e le modalità con cui viene esercitato il controllo umano sui risultati prodotti dal sistema.

Abbiamo chiesto informazioni sui percorsi formativi previsti per gli operatori, anche rispetto ai limiti della tecnologia e al suo impatto sui diritti fondamentali. Il Ministero ha negato l'accesso a queste informazioni richiamando esigenze di tutela dell'ordine e della sicurezza pubblica, e il TAR ha ritenuto legittimo il diniego. Di conseguenza, non è ancora possibile conoscere in modo completo come viene formato il personale né valutare quali strumenti siano previsti per garantire un uso consapevole e un adeguato controllo umano del sistema.

DIRITTI FONDAMENTALI

Oltre alla normativa in tema di protezione dei dati personali, vanno rispettate anche le norme poste a tutela dei diritti fondamentali.

L'utilizzo di un sistema come SARI ENTERPRISE costituisce una limitazione di diritti fondamentali. Per valutare se una limitazione di questi diritti sia legittima è necessario fare riferimento, tra l'altro, all'**art. 52 della Carta dei diritti fondamentali dell'Unione europea**.

La norma richiede che ogni limitazione sia prevista dalla legge, rispetti il contenuto essenziale dei diritti coinvolti e, nel rispetto dei principi di necessità e proporzionalità, risponda effettivamente a finalità di interesse generale.

Il contesto normativo: Le limitazioni di diritti fondamentali sono consentite all'interno di un quadro giuridico chiaro e definito, che permetta alle cittadine 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 delle cittadine.

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. Si segnala, ad ogni modo, che il Governo sta lavorando ad uno schema di decreto legislativo di adeguamento all'AI Act che introduce una disciplina specifica per l'utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia, compreso il riconoscimento facciale in tempo reale e a posteriori.

Principio di necessità: Una limitazione dei diritti fondamentali deve essere necessaria. Questo significa che il ricorso a uno strumento invasivo come il riconoscimento facciale dovrebbe essere giustificato da un'esigenza concreta e accompagnato dalla valutazione dell'esistenza di alternative meno invasive capaci di raggiungere lo stesso risultato.

L'introduzione di una nuova tecnologia investigativa, quindi, non dovrebbe dipendere soltanto dalla sua disponibilità sul mercato o dalle sue potenzialità tecniche, ma dalla dimostrazione della sua effettiva necessità in assenza di alternative meno impattanti. Tale valutazione dovrebbe essere documentata attraverso elementi oggettivi e verificabili.

Bisogna anche ricordare che il trattamento di dati biometrici dovrebbe avvenire solo in casi di *stretta necessità*, quindi la valutazione dovrebbe essere ancora più stringente.

Nel corso della nostra indagine non ci è stata fornita documentazione che dimostri l'esistenza di una specifica valutazione sulla necessità dell'utilizzo di SARI Enterprise. L'assenza di dati sulla sua effettiva efficacia e la mancata predisposizione della valutazione d'impatto indicano una probabile violazione del principio di necessità.

Principio di proporzionalità: Anche quando una misura è ritenuta necessaria, occorre verificare che sia proporzionata. In altre parole, i benefici attesi devono superare gli svantaggi.

Questa valutazione deve tenere conto, tra gli altri elementi, della natura dei dati trattati, del numero di persone coinvolte, del rischio che persone estranee alle indagini siano interessate dal trattamento, delle modalità di raccolta e utilizzo dei dati, del numero di soggetti che possono accedervi e della durata della loro conservazione. Anche un'interferenza apparentemente limitata per il singolo può assumere una rilevanza molto maggiore quando la tecnologia viene utilizzata su larga scala o quando i dati vengono conservati per periodi molto lunghi. Una corretta valutazione di proporzionalità dovrebbe inoltre consentire di individuare specifiche misure di salvaguardia per ridurre i rischi emersi.

Nel caso di SARI Enterprise, la forte crescita nell'utilizzo del sistema, la dimensione e la composizione della banca dati AFIS, i lunghi tempi di conservazione dei dati e, soprattutto, l'assenza di informazioni sull'efficacia concreta rendono **difficile verificare se sia stato effettuato un adeguato bilanciamento tra benefici investigativi e impatto sui diritti fondamentali.**



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:

- **TITOLARE DEL TRATTAMENTO** (chi tratta i dati. Nel nostro caso Ministero dell'interno – Dipartimento della Pubblica Sicurezza)
- **SOGGETTO 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 la cittadina 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 qualcuna di esperti)

→ Se pensi di essere stato soggetto 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 (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 le cittadine 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 a 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 le cittadine.

LE NOSTRE RICHIESTE AL MINISTERO DELL'INTERNO

La nostra posizione è favorevole alla sospensione dell'utilizzo dei sistemi di riconoscimento biometrico da parte delle forze dell'ordine, sia in tempo reale sia a posteriori. Se queste tecnologie continueranno comunque a essere utilizzate, il loro impiego dovrà almeno essere accompagnato da regole chiare, garanzie effettive, controlli indipendenti e maggiore trasparenza.

Chiediamo pertanto alle autorità competenti di:

1. **Istituire un registro pubblico dei sistemi di identificazione biometrica utilizzati dalle forze dell'ordine;**
2. **Raccogliere e pubblicare dati sull'efficacia dei sistemi, compresi i risultati utili alle indagini, i falsi positivi, i falsi negativi e le differenze di performance tra gruppi demografici;**
3. **Pubblicare dati aggiornati sulla composizione delle banche dati biometriche, compreso il numero di soggetti presenti, le categorie interessate e i tempi di conservazione;**
4. **Predisporre una specifica valutazione d'impatto sulla protezione dei dati relativa a SARI Enterprise e una valutazione dell'impatto sui diritti fondamentali;**
5. **Rivalutare la conformità di SARI Enterprise alla luce delle informazioni emerse dopo il parere del Garante del 2018, compresa l'assenza di una specifica DPIA;**
6. **Adottare misure specifiche di salvaguardia dei diritti e delle libertà fondamentali, con particolare attenzione ai principi di necessità, proporzionalità, non discriminazione e supervisione umana;**
7. **Pubblicare linee guida sull'utilizzo del riconoscimento facciale per finalità di polizia, indicando condizioni di utilizzo, procedure operative, criteri di verifica e responsabilità degli operatori;**
8. **Garantire una formazione specifica e verificabile del personale sui limiti della tecnologia, sui rischi di errore e discriminazione e sull'impatto sui diritti fondamentali;**
9. **Creare una pagina pubblica dedicata ad AFIS e ai sistemi biometrici utilizzati dalla polizia, con informazioni chiare su finalità, tempi di conservazione e modalità di esercizio dei diritti;**
10. **Prevedere una relazione pubblica annuale sull'utilizzo dei sistemi di riconoscimento biometrico, con dati sul numero di utilizzi, sui reati interessati, sui risultati, sugli errori e sull'impatto sui diritti fondamentali;**
11. **Rafforzare il controllo delle autorità indipendenti competenti, garantendo loro accesso alla documentazione necessaria e un ruolo effettivo nelle procedure di controllo, reclamo e tutela dei diritti;**
12. **Completare e aggiornare il quadro normativo sui trattamenti di dati per finalità di polizia, eliminando le lacune ancora esistenti e definendo regole chiare su utilizzo, accesso, conservazione e cancellazione dei dati.**

APPROFONDIMENTO:

Richieste FOIA e ricorso al TAR

Parte 1 → LE RICHIESTE DI ACCESSO FOIA

Per ricostruire il funzionamento concreto di SARI Enterprise abbiamo utilizzato lo strumento dell'accesso civico generalizzato (FOIA), articolando l'indagine in due fasi successive di richieste

- **La prima fase**, avviata nel settembre 2025, aveva un carattere ampio ed esplorativo: volevamo comprendere quali regole disciplinassero il sistema, quali garanzie fossero previste per gli interessati e quali dati esistessero sul suo utilizzo e sulla sua efficacia.
- **La seconda fase**, avviata nel gennaio 2026, ha approfondito le questioni rimaste aperte dopo le prime risposte. Le nuove richieste erano più specifiche e sono state formulate anche sulla base delle linee guida ENFSI, indicate dallo stesso Ministero come riferimento per l'utilizzo di SARI Enterprise.

PRIMA FASE DI RICHIESTE (Settembre 2025)

Nel settembre 2025 abbiamo presentato tre richieste di accesso civico generalizzato, dedicate rispettivamente alla protezione dei dati personali, alle modalità concrete di utilizzo di SARI Enterprise e alle statistiche di utilizzo e di efficacia del sistema.

RICHIESTA 1 - PROTEZIONE DEI DATI E GARANZIE PER GLI INTERESSATI

La prima richiesta era diretta a comprendere quali misure fossero state adottate per proteggere i dati personali trattati attraverso SARI Enterprise e quali garanzie fossero previste per gli interessati.

ABBIAMO CHIESTO

1. Quali fossero le specifiche finalità del trattamento;
2. Quali condizioni di liceità fossero state individuate per ciascuna finalità;
3. Se gli interessati potessero essere sottoposti a decisioni automatizzate;
4. Se SARI Enterprise utilizzasse tecnologie di intelligenza artificiale, comprese tecniche di deep learning e machine learning;
5. Se fosse prevista una valutazione periodica dell'efficacia delle misure adottate a tutela degli interessati;
6. Copia di eventuali valutazioni d'impatto sulla protezione dei dati (DPIA) e di altre valutazioni interne del rischio;
7. Quali fossero le regole relative alla conservazione e alla cancellazione dei dati biometrici;
8. Quali misure di sicurezza tecniche e organizzative fossero state adottate;
9. Se fossero previsti audit o verifiche indipendenti sul rispetto delle garanzie in materia di protezione dei dati.

COSA ABBIAMO OTTENUTO

Il Ministero ha rinviato al parere del Garante del 2018 per le finalità del trattamento, le condizioni di liceità e il tema delle decisioni automatizzate. Ha però confermato che SARI Enterprise utilizza un sistema di intelligenza artificiale basato su reti neurali profonde e che i risultati vengono sempre sottoposti alla verifica manuale di un operatore.

RICHIESTA 2 - MODALITÀ CONCRETE DI UTILIZZO

La seconda richiesta riguardava il funzionamento concreto di SARI Enterprise: le regole di utilizzo, l'algoritmo impiegato, le banche dati interrogate, la formazione degli operatori e gli eventuali sistemi di monitoraggio.

ABBIAMO CHIESTO

1. Se esistesse un documento che disciplinasse le condizioni di utilizzo;
2. Quale algoritmo fosse stato scelto;
3. Quale punteggio di accuratezza avesse ottenuto nell'ambito della procedura di acquisto;
4. Quali procedure fossero previste a garanzia dei diritti e delle libertà degli interessati;
5. Se esistesse un documento che individuasse i reati per i quali SARI può essere utilizzato;
6. Su quali banche dati fosse possibile effettuare la ricerca;
7. Se fosse prevista una procedura specifica di valutazione delle modalità di utilizzo e funzionamento;
8. Se esistesse una valutazione periodica dei risultati;
9. Se fossero disponibili manuali interni, linee guida operative o programmi di formazione;
10. Se fossero previste procedure di aggiornamento periodico dell'algoritmo.

COSA ABBIAMO OTTENUTO

Il Ministero ha comunicato che l'algoritmo utilizzato è sviluppato da Neurotechnology e che SARI Enterprise opera esclusivamente sulla banca dati AFIS dei soggetti fotosegnalati.

Ha inoltre chiarito che il sistema dispone di strumenti amministrativi per monitorare le diverse tipologie di ricerca, ma che i risultati operativi delle indagini non vengono gestiti informaticamente dal sistema. Gli operatori vengono formati internamente e dispongono di manuali funzionali e operativi, che tuttavia non sono stati resi accessibili. Il Ministero ha infine dichiarato che gli algoritmi vengono aggiornati sulla base delle nuove versioni rilasciate dal produttore.

RICHIESTA 3 - UTILIZZO, EFFICACIA E TASSI DI ERRORE

La terza richiesta mirava a ottenere dati quantitativi sull'utilizzo di SARI Enterprise nel 2024 e, soprattutto, a comprendere se il Ministero ne monitorasse l'efficacia concreta.

ABBIAMO CHIESTO

1. Il numero di ricerche effettuate con SARI Enterprise;
2. Il numero complessivo di volti analizzati;
3. Il numero o la percentuale di risultati effettivamente utili al proseguimento delle indagini;
4. Il tasso di errore del sistema prima dell'intervento degli operatori;
5. Il tasso di errore con riferimento a caratteristiche demografiche quali etnia, sesso e genere;
6. Il numero e la qualifica degli operatori autorizzati e le informazioni relative alla loro formazione.

COSA ABBIAMO OTTENUTO

Il Ministero ha comunicato che nel 2024 sono state effettuate 181.705 ricerche tramite immagini facciali, di cui 162.064 ricerche per immagine singola, 11.621 multi-foto e 8.020 combinate. A queste si aggiungono 515.447 ricerche testuali effettuate senza utilizzare algoritmi di riconoscimento facciale. Non sono stati invece forniti dati sul numero di corrispondenze effettivamente utili alle indagini, perché tali informazioni non vengono gestite informaticamente dal sistema. Per i tassi di errore, anche con riferimento alle caratteristiche demografiche, il Ministero ha rinviato ai test effettuati dal NIST sull'algoritmo, senza fornire dati relativi all'utilizzo operativo di SARI Enterprise in Italia.

SECONDA FASE DI RICHIESTE (Gennaio 2026)

Le risposte al primo giro hanno permesso di ottenere alcune informazioni, ma hanno anche fatto emergere nuove domande. Nel gennaio 2026 abbiamo quindi presentato quattro ulteriori richieste, questa volta costruite in maniera più mirata anche sulla base delle linee guida ENFSI, indicate dallo stesso Ministero tra i riferimenti utilizzati per SARI Enterprise.

RICHIESTA 1 - CONTROLLO UMANO E FORMAZIONE DEGLI OPERATORI

La prima richiesta era diretta a comprendere come avvenga concretamente il controllo umano sui risultati prodotti da SARI Enterprise e quali competenze siano richieste agli operatori.

ABBIAMO CHIESTO

1. Se sia previsto un numero minimo di operatori incaricati della verifica manuale;
2. Se venga redatto un verbale dell'operazione effettuata con SARI e quale ne sia il contenuto minimo;
3. Una descrizione delle principali fasi di utilizzo del sistema;
4. Come vengano formati gli operatori autorizzati;
5. Se le loro competenze siano sottoposte a verifiche periodiche;
6. Se siano previste le qualifiche di face reviewer e face examiner e quanti operatori appartengano alle due categorie;
7. Se venga effettuato un test attitudinale prima della formazione.

COSA ABBIAMO OTTENUTO

Il Ministero **ha negato integralmente l'accesso alle informazioni richieste**, sostenendo che la loro divulgazione potrebbe arrecare un pregiudizio concreto all'ordine e alla sicurezza pubblica e rivelare informazioni relative alle tecniche investigative.

RICHIESTA 2 - CONFIGURAZIONE E FUNZIONAMENTO DEL SISTEMA

La seconda richiesta riguardava la configurazione tecnica di SARI Enterprise e il modo in cui vengono presentati e valutati i risultati.

ABBIAMO CHIESTO

1. Se il sistema venga utilizzato in modalità rank based e, in caso affermativo, se siano stati svolti test sulla Cumulative Match Curve e quanti risultati vengano restituiti;
2. Se venga utilizzato in modalità threshold based, quale sia l'eventuale soglia minima di similarità e come venga mostrato lo score all'operatore;
3. Se esista una policy formalizzata per l'analisi dei risultati;
4. Se il sistema venga utilizzato anche su minori e se esista una disciplina specifica;
5. Se sia stato effettuato un quality assessment nella fase di inserimento delle immagini nel database.

COSA ABBIAMO OTTENUTO

Su questo punto abbiamo ottenuto una delle **informazioni più rilevanti** dell'intera indagine: SARI Enterprise restituisce una lista di 50 candidati, ordinati sulla base di un indice di similarità espresso in percentuale. Non esiste però una soglia di similarità oltre la quale si determini automaticamente un match. La lista deve sempre essere verificata manualmente da un operatore qualificato e le eventuali corrispondenze possono essere utilizzate soltanto per il proseguimento dell'attività investigativa. Il Ministero ha inoltre precisato che SARI lavora esclusivamente sui soggetti fotosegnalati. Per le ulteriori specificazioni e per gli altri quesiti ha invece negato l'accesso, richiamando nuovamente la tutela dell'ordine e della sicurezza pubblica.

RICHIESTA 3 - PERFORMANCE ED ERRORI DELL'ALGORITMO

La terza richiesta mirava ad approfondire uno dei principali problemi emersi nel primo giro: l'assenza di dati sull'efficacia e sugli errori registrati nell'utilizzo concreto del sistema.

ABBIAMO CHIESTO

1. Il False Positive Identification Rate (FPIR) e l'esistenza di documentazione del fornitore o di test indipendenti;
2. Il False Negative Identification Rate (FNIR) e l'esistenza di analoghi test;
3. Il punteggio di equitability, cioè la capacità del sistema di mantenere prestazioni comparabili tra diversi gruppi;
4. Il tasso di errore effettivamente registrato nell'utilizzo di SARI Enterprise da parte delle forze dell'ordine italiane nel 2023 e nel 2024;
5. Se esistessero procedure specifiche per monitorare gli errori in relazione a caratteristiche quali etnia, sesso, genere o altri elementi demografici.

COSA ABBIAMO OTTENUTO

Per FPIR, FNIR ed equitability, il Ministero **ha nuovamente rinviato alla documentazione pubblicata dal NIST relativa all'algoritmo**.

Alla richiesta di conoscere invece i tassi di errore registrati nell'utilizzo operativo del sistema in Italia, ha risposto che **tali dati non sono disponibili** perché SARI non restituisce un vero e proprio "match": la corrispondenza viene individuata manualmente dall'operatore e i relativi risultati non vengono gestiti informaticamente, ma rimangono collegati alle singole indagini di polizia giudiziaria. La stessa risposta è stata fornita rispetto all'eventuale misurazione degli errori su base demografica.

RICHIESTA 4 - DATABASE AFIS E QUALITÀ DELLE IMMAGINI

La quarta richiesta riguardava la banca dati AFIS, che costituisce il database di riferimento utilizzato da SARI Enterprise, e la qualità delle immagini che vi sono contenute.

ABBIAMO CHIESTO

1. Il numero di cartellini fotosegnalatici presenti in AFIS nel 2024, suddivisi per nazionalità;
2. Se fosse stato effettuato un test sulla qualità delle immagini presenti nel database;
3. Se la qualità delle immagini e la correttezza dei metadati venissero verificate periodicamente;
4. Se il database contenesse immagini con diversi livelli di qualità e fosse eventualmente compartimentato sulla base di tali livelli;
5. Se venissero effettuati controlli per eliminare record duplicati;
6. Se fosse prevista una soglia minima di qualità per le immagini sottoposte all'algoritmo;
7. Se fosse possibile elaborare o modificare le immagini prima della ricerca;
8. Se esistesse una procedura formalizzata per il caricamento delle immagini.

COSA ABBIAMO OTTENUTO

Il Ministero ha **negato inizialmente anche queste informazioni**. Per il numero di cartellini fotosegnalatici presenti in AFIS ha sostenuto che fornire il dato avrebbe richiesto un'attività di estrazione e aggregazione e quindi la creazione di un nuovo documento, attività che l'Amministrazione non sarebbe tenuta a svolgere nell'ambito dell'accesso civico.

Per tutti gli altri quesiti ha opposto un **diniego fondato sulle esigenze di tutela dell'ordine e della sicurezza pubblica**. Proprio questi dinieghi sono poi diventati uno degli oggetti principali del secondo ricorso davanti al TAR Lazio. Il contenzioso ha consentito di ottenere successivamente sia i dati sulla composizione di AFIS sia nuove informazioni sui controlli di qualità delle immagini.

DALLE RICHIESTE FOIA AL CONTENZIOSO

I due giri di accesso mostrano una progressiva evoluzione della nostra indagine. Le prime richieste avevano l'obiettivo di ricostruire il funzionamento generale di SARI Enterprise; le seconde sono state formulate sulla base delle lacune emerse e delle stesse fonti tecniche indicate dal Ministero.

Alcune informazioni importanti sono state ottenute attraverso il semplice accesso civico. Altre, invece, sono rimaste inaccessibili oppure hanno ricevuto risposte che abbiamo ritenuto insufficienti. In particolare, i dubbi sull'esistenza della DPIA, le informazioni sul controllo umano e sulla formazione degli operatori, la composizione di AFIS e i controlli sulla qualità delle immagini hanno portato alla successiva fase di contenzioso davanti al TAR Lazio.

La ricostruzione completa dei due ricorsi e delle relative decisioni è contenuta nella sezione successiva.

Parte 2 → I RICORSI AL TAR

I due giudizi promossi ex art. 116 c.p.a. dinanzi al TAR Lazio hanno consentito di far luce su alcuni profili del SARI Enterprise, ottenendo un'**esplicita conferma dell'inesistenza della DPIA** e l'**ostensione dei dati ufficiali sulla composizione quali-quantitativa del database biometrico AFIS**.

FOIA 1

RICORSO: R.G. n. 626/2026 del 17.01.2026 - TAR LAZIO, Sez. I ter

Sentenza n. 7413/2026 del 23.04.2026 | [link pdf](#)

Ricorrenti: StraLi ETS Odv, Privacy Network APS, Hermes Center

Resistente: Ministero dell'Interno - Dipartimento per l'amministrazione generale, per le Politiche del personale dell'amministrazione civile e per le Risorse strumentali e finanziarie - Ufficio per le attività del Responsabile della prevenzione della corruzione e della trasparenza

Il primo ricorso è stato promosso a seguito del procedimento di riesame ex art. 5, co. 7, d.lgs. n. 33/2013 per contestare il sostanziale diniego opposto alle istanze dirette ad ottenere:

- la Valutazione di Impatto sulla Protezione dei Dati;
- il documento di regolamentazione delle condizioni d'uso e delle procedure di garanzia dei diritti degli interessati.

Cosa abbiamo impugnato:

- il **provvedimento di riesame ex art. 5, co. 7 del d.lgs. n. 33/2013 emesso dal Responsabile della Prevenzione della Corruzione e della Trasparenza del Ministero dell'Interno**, limitatamente alle parti in cui recava un sostanziale diniego di accesso ai documenti e alle informazioni richiesti con i quesiti: n. 6 della "Richiesta 1" e nn. 1 e 4 della "Richiesta 2".
- la **nota della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica** allegata alla decisione del Responsabile della Prevenzione della Corruzione e della Trasparenza del Ministero dell'Interno.

Le nostre argomentazioni

Nel ricorso abbiamo sostenuto, in primo luogo, che il rinvio generico al parere del Garante Privacy del 2018 non fosse idoneo a soddisfare le nostre istanze conoscitive. Quel parere valutava il sistema in una fase ancora progettuale, mentre le nostre richieste riguardavano l'operatività concreta del sistema in uso: un disallineamento temporale, ancor prima che di contenuto.

In secondo luogo, abbiamo evidenziato che la redazione della DPIA non è facoltativa, bensì obbligatoria per trattamenti ad alto rischio (art. 35 GDPR e art. 23 d.lgs. n. 51/2018), come confermano, in riferimento al riconoscimento facciale, anche l'elenco dei trattamenti soggetti a DPIA, adottato dal Garante Privacy l'11 ottobre 2018, le Linee guida del Gruppo di Lavoro art. 29 (WP 248, rev. 01), e le Linee Guida sull'utilizzo del riconoscimento facciale per fini di Polizia dell'EDPB (Guidelines 05/2022).

Abbiamo inoltre segnalato che, poiché nel parere del Garante non c'era alcuna menzione puntuale dei documenti o delle informazioni trasmesse dal Dicastero, la risposta del Ministero - "*questo servizio non dispone di altra documentazione*" - fosse oscura, non consentendo di comprendere in che termini fosse "altra", ossia rispetto a quali documenti.

La mancanza di indicazioni chiare da parte del Ministero sull'esistenza di tale documento era apparsa sintomatica di una carenza nell'adempimento degli obblighi di accountability.

La decisione del TAR

- **Cessazione della materia del contendere sulla DPIA:** nel corso del giudizio, dalle difese del Ministero, è emerso che la DPIA non è mai stata predisposta dal Ministero dell'Interno. Tale dichiarazione ha soddisfatto - seppur in negativo - il nostro interesse conoscitivo, portando il TAR a dichiarare **la cessazione della materia del contendere** su questo punto.
- **Inammissibilità per le restanti richieste:** con riguardo agli eventuali documenti recanti le condizioni d'uso del sistema e le procedure di garanzie dei diritti degli interessati, il TAR ha dichiarato il ricorso **inammissibile per difetto di interesse**, ritenendo che le informazioni richieste fossero già desumibili sia dal provvedimento del Garante della Privacy sia dalla nota emessa in sede di riesame dalla Direzione Centrale per la Polizia Scientifica.

“- in relazione alle richieste n. 1 e n. 4 della richiesta n. 2, attinenti al documento che regola l'utilizzo del sistema SARI Enterprise e alle procedure di garanzia dei diritti e delle libertà degli interessati, quanto richiesto è desumibile dal provvedimento del Garante protezione dati personali, anch'esso in atti;

- è in atti altresì la nota allegata all'atto di riesame predisposta da Ministero Interno - Direzione centrale per la Polizia scientifica, che fornisce risposta alle restanti richieste di chiarimenti n.1 e n. 2.;
- l'Amministrazione ha già fornito risposte complete e motivate”.

La strategicità del risultato conseguito

Come già evidenziato, la conferma giudiziale della omessa redazione della DPIA rappresenta, a nostro avviso, un'ammissione rilevante sotto il profilo della mancata compliance al GDPR e al d.lgs. n. 51/2018. In quest'ottica e in quella propria della strategic litigation, il giudizio ha rappresentato **l'occasione per sottrarre ad una zona d'ombra e di ambiguità un'informazione decisiva** (l'esistenza o meno della DPIA), mai dichiarata espressamente in sede procedimentale.

Al di là dell'esito processuale, l'azione promossa ha consentito di raggiungere un **risultato non scontato, né pienamente preventivabile**.

Da un lato, la notifica del ricorso ha indotto l'Amministrazione ad articolare le proprie difese, argomentando e giustificando formalmente il proprio operato nell'implementazione e nella gestione del sistema SARI Enterprise. Per altro profilo, l'aver promosso sia il riesame sia il giudizio innanzi al Giudice Amministrativo ci ha permesso di acquisire una visione d'insieme, procedimentale e processuale, sull'effettivo grado di trasparenza e sulle linee difensive delle Amministrazioni dinanzi a richieste di accesso che intersechino ambiti ad elevata sensibilità, quale l'uso di sistemi algoritmici nell'esercizio delle funzioni di polizia.

FOIA 2

RICORSO: R.G. n. 4289/2026 del 28.03.2026 - TAR LAZIO, Sez. I ter

Sentenza n. 11961/2026 del 01.07.2026 | [link pdf](#)

Ricorrenti: StraLi ETS Odv, Privacy Network APS, Hermes Center

Resistente: Ministero dell'Interno - Dipartimento della Pubblica Sicurezza, Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

In assenza di un previo riesame al RPCT, il secondo ricorso ha impugnato direttamente il diniego di accesso ad elementi chiave del sistema SARI Enterprise: le modalità di coinvolgimento umano nell'uso del sistema (human-in-the-loop), i parametri di configurazione dell'algoritmo, i controlli di qualità delle immagini e la consistenza quantitativa e qualitativa del database AFIS (Automated Fingerprint Identification System).

I dinieghi

Il Ministero aveva opposto:

- Un diniego pressoché totale di accesso ai profili tecnici e di coinvolgimento umano (adesione agli standard internazionali pubblici, aspetti organizzativi, formazione erogata al personale abilitato all'uso del SARI), motivato con il ricorso alla formula, tendenzialmente standard, del potenziale pregiudizio all'ordine e alla sicurezza pubblica (art. 5-bis, co.1, d.lgs. n. 33/2013).

“Non è possibile divulgare le informazioni richieste, al fine di evitare un pregiudizio concreto alla tutela dell'interesse pubblico inerente all'ordine ed alla sicurezza pubblica, ai sensi dell'art. 5 bis comma1, D. Lgs. 14 marzo 2013, n. 33.

Tale pregiudizio può derivare, infatti, anche dalla conoscibilità di documenti, dati o informazioni attinenti alle strutture, ai mezzi, alle dotazioni, al personale ed alle azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riguardo alle tecniche investigative”.

- Un diniego motivato dall'assenza di un documento preesistente per la richiesta del numero di cartellini fotosegnalatici presenti in AFIS, sostenendo che fornirli avrebbe imposto una non dovuta attività di elaborazione di nuovi documenti.

“L'eventuale risposta comporterebbe, infatti, un'attività di estrazione e aggregazione dei dati presenti nei sistemi informativi, con conseguente formazione di un nuovo documento.

Pertanto, non essendo l'Amministrazione tenuta, nell'ambito dell'accesso civico, alla creazione di nuova documentazione o alla rielaborazione di dati non già disponibili nella forma richiesta, non è possibile dare seguito all'istanza nei termini prospettati”.

Le nostre argomentazioni:

Sul piano generale, abbiamo evidenziato che una formula identica e stereotipata, priva di un accertamento specifico del pregiudizio per ciascuna delle informazioni richieste, non soddisfa lo standard richiesto dalla Circolare del Ministro per la Semplificazione e la Pubblica Amministrazione n. 2/2017 e dalle Linee Guida ANAC adottate con deliberazione n. 1309/2016 Par. 5.2: il pregiudizio per l'interesse-limite contrapposto all'istanza conoscitiva deve essere concreto, non meramente ipotetico, né evocato in via del tutto generica e astratta.

Abbiamo inoltre rilevato che il diniego era stato formulato “in blocco”, senza alcun vaglio specifico delle singole informazioni richieste e senza valutare la possibilità di un accesso parziale, in contrasto con il cd. harm test richiamato dalla giurisprudenza (T.A.R. Lazio Roma, Sez. I bis, 01 febbraio 2023, n. 1779) e con il bilanciamento richiesto dalle Linee Guida in materia FOIA.

A sostegno di tali censure, nel ricorso abbiamo distinto tra i diversi quesiti oggetto della Richiesta 1, evidenziando che la stessa modalità stereotipata di diniego fosse stata applicata a informazioni di natura diversa tra loro. Nel merito:

- **Standard tecnici pubblici** (verbalizzazione delle operazioni, flowchart delle fasi d'uso, modalità di formazione degli operatori - quesiti 2,3,4): si tratta di parametri indicati dalle stesse Linee Guida ENFSI che il Ministero aveva individuato come riferimento in una precedente risposta all'accesso. Chiedere se l'uso del sistema SARI Enterprise fosse conforme alle buone pratiche non avrebbe potuto arrecare un pregiudizio concreto all'interesse pubblico “inerente all'ordine ed alla sicurezza pubblica” né rivelare “tecniche investigative” riservate.

- **Aspetti di natura organizzativa** (numero minimo di operatori, frequenza delle verifiche periodiche - quesiti 1 e 5): trattandosi di macro-dati, la loro conoscibilità non avrebbe compromesso alcuna operazione investigativa né rivelato dotazioni operative specifiche e sensibili.
- **Formazione del personale** abilitato all'uso del S.A.R.I. Enterprise (test attitudinale, qualifiche di face reviewer/face examiner - quesiti 6 e 7): abbiamo rimarcato che la disclosure di tali informazioni fosse insuscettibile di arrecare un pregiudizio concreto agli interessi pubblici richiamati;
- **il provvedimento, oltre a non essere adeguatamente motivato, appariva illogico nella misura in cui negava la conoscibilità di dati inerenti l'implementazione di standard a cui la stessa Amministrazione aveva fatto riferimento.**
- Sul punto abbiamo:
 - richiamato la giurisprudenza amministrativa sulla c.d. riserva di umanità (human oversight);
 - sostenuto che il controllo sull'output di un sistema come SARI non sia un dettaglio tecnico-operativo, ma una condizione di legittimità del suo impiego;
 - argomentato che le informazioni su come questo controllo avvenga (oggetto della Richiesta 1) meritassero una ponderazione particolarmente accurata, non una formula standard di rigetto.

Avverso il diniego sui dati AFIS, è stato evidenziato che l'estrazione di un'informazione già presente in un database ed ottenibile mediante una semplice interrogazione non equivale alla creazione di un nuovo documento, e non può quindi essere negata invocando l'assenza di un atto preesistente (TAR Veneto, sez. III, 29 ottobre 2024, n. 2548). Peraltro, un dato analogo era già stato fornito dal Ministero in risposta ad un accesso civico promosso da ASGI, pertanto la loro non ostensione appariva palesemente contraddittoria rispetto al precedente.

La decisione del TAR: la ponderazione e il bilanciamento degli interessi

Conferma del diniego su configurazione e coinvolgimento umano

Il Tribunale ha ritenuto legittimo il diniego per le informazioni concernenti il funzionamento tecnico e le modalità del coinvolgimento umano, giudicando congrua la motivazione ministeriale fondata su dedotte esigenze di tutela della sicurezza e dell'ordine pubblico ed evidenziando che l'Amministrazione avesse già provveduto agli obblighi informativi ritenuti compatibili con la tutela degli interessi pubblici coinvolti.

Su questo punto, il TAR ha richiamato un principio consolidato: il bilanciamento tra interesse conoscitivo e interessi-limite resta riservato all'Amministrazione e spetta ad essa *“la valutazione degli interessi pubblici nel caso ritenuti prevalenti rispetto all'interesse alla conoscenza vantato dalle associazioni ricorrenti”*.

L'applicazione di tale principio, in questo caso, ha condotto ad un controllo giurisdizionale che si è fermato alla congruità formale della motivazione, senza il vaglio puntuale del nesso di causalità concreto tra l'accesso e il pregiudizio allegato.

Accoglimento sulle caratteristiche del database AFIS e sulla qualità delle immagini

Di contro, il TAR ha annullato il diniego di ostensione relativo:

- al numero di cartellini fotosegnalatici in AFIS suddivisi per nazionalità, con riferimento al 2024;
- alla qualità delle immagini in AFIS e alla correttezza dei metadati associati;

ordinando all'Amministrazione di fornire il dato entro 30 giorni.

Il Giudice Amministrativo ha ribadito importanti principi in materia di trasparenza e accessibilità ai dati contenuti nel database anagrafico-biometrico.

Inconsistenza del pregiudizio astratto:

“Ritiene inoltre il Collegio che in effetti non risulta logico negare l'accesso sul rilievo che le informazioni richieste rivelerebbero, in modo pregiudizievole per la sicurezza, il livello di affidabilità del patrimonio informativo anagrafico-biometrico. Peraltro il pregiudizio agli interessi considerati dall'art. 5 bis, commi 1 e 2, deve essere concreto nel senso che deve sussistere un preciso nesso di causalità tra l'accesso e il pregiudizio.”

Insussistenza dell'onere rielaborativo:

Il Giudice ha ritenuto che l'estrazione di dati numerici dal database AFIS non costituisca creazione di un nuovo documento.

“Il dato richiesto, suddiviso per macro-categorie, non richiederebbe un'elaborazione complessa o eccessivamente onerosa e non si pone in contrasto con la tutela degli interessi pubblici primari che, ex art. 5 bis c.1 citato, sono affidati dal legislatore all'Amministrazione”.

I DATI OTTENUTI A SEGUITO DELL'OTTEMPERANZA

In esecuzione della sentenza n. 11961/2026, in data 10.08.2026, il Ministero dell'Interno ha inoltrato i dati richiesti, fornendo informazioni utili per l'analisi della composizione di AFIS e per la conoscenza delle modalità di controllo della qualità delle immagini biometriche inserite.

Consistenza del database AFIS (anno 2024)

I dati trasmessi rivelano che il database di riferimento su cui opera SARI Enterprise contava, nell'anno 2024, 956.534 cartellini fotosegnalatici, di cui:

- Nazionalità Italiana → 76.443
- Nazionalità UE (esclusa l'Italia) → 14.938
- Nazionalità Extra UE → 764.787
- Fotosegnalamenti privi di nazionalità → 100.366

Note di analisi:

- Il dato di **956.534 cartellini fotosegnalatici riferito al 2024** appare difficilmente compatibile con i dati precedentemente disponibili sulla consistenza complessiva di AFIS. Alla luce dei numeri emersi per il 2022 e dei 992.093 ulteriori fotosegnalamenti registrati nel 2023, riteniamo più plausibile che il dato comunicato dal Ministero si riferisca ai **nuovi inserimenti effettuati nel corso del 2024**, e non allo stock complessivo dei cartellini presenti nel database. Il Ministero non ha tuttavia fornito elementi sufficienti per chiarire definitivamente questo aspetto;
- Anche considerando il dato come riferito ai soli inserimenti del 2024, emerge una **forte sproporzione nella composizione**: circa l'80% dei cartellini complessivamente comunicati riguarda cittadine extra-UE, percentuale che supera l'89% se si considerano soltanto i record per i quali la nazionalità è indicata. Il dato conferma quindi il **rischio di una significativa sovrarappresentazione di cittadine extra-UE all'interno della banca dati**.

Controllo di qualità delle immagini e gestione dei metadati

In merito all'aderenza alle raccomandazioni internazionali (p. 5.4 delle linee guida ENFSI), il Ministero ha chiarito la natura e la modalità dei controlli sulla qualità delle immagini processate dal SARI Enterprise:

- **Valutazione preliminare automatizzata**

Se è stato svolto un test per verificare la qualità delle immagini presenti nel database di riferimento, come suggerito al p. 5.4 delle linee guida ENFSI:

Gli algoritmi di riconoscimento facciale del sistema SARI effettuano una valutazione preliminare della qualità delle immagini prima di procedere all'estrazione dei dati biometrici, sia per le immagini utilizzate per la ricerca, sia per le immagini presenti nel database di riferimento. Le immagini che non raggiungono i requisiti minimi di idoneità vengono scartate. Questo controllo preliminare garantisce che solo le immagini di qualità adeguata siano utilizzate per l'estrazione del template biometrico.

- **Il controllo continuo e la gestione dei metadati**

Se avviene una verifica periodica della qualità delle immagini e della correttezza dei metadati associati come suggerito al p. 5.4 delle linee guida ENFSI:

Come descritto al punto 2), la valutazione della qualità viene effettuata sistematicamente all'atto dell'estrazione del dato biometrico e ogni immagine effettivamente elaborata da SARI possiede quindi una qualità adeguata. Il controllo della qualità non è quindi periodico, ma continuo.

In relazione ai metadati, SARI opera direttamente sulla banca dati AFIS e non genera né gestisce metadati aggiuntivi associati alle immagini: la correttezza dei dati associati è, pertanto, demandata al sistema AFIS di riferimento.

La strategicità del risultato conseguito

Il giudizio ha permesso di raggiungere **due risultati di rilievo**, sia sul piano della prassi amministrativa in ambito FOIA sia su quello della trasparenza della banca dati AFIS.

1. **Un principio valido oltre il caso SARI:** per le future istanze FOIA afferenti a dati già indicizzati in un database a gestione pubblica (strutturato in modo simile ad AFIS), l'Amministrazione non potrà negare l'accesso opponendo un presunto onere rielaborativo o l'assenza di documenti già formati. È stato, così, infranto un alibi procedimentale che potrebbe potenzialmente ostacolare la trasparenza di questa tipologia di dati. In tal senso, la sentenza, consolidando uno standard di trasparenza vincolante, reca preziose indicazioni operative per le Pubbliche Amministrazioni che si trovino dinanzi ad istanze di accesso a database pubblici
2. **Una disclosure ufficiale:** per la prima volta vengono acquisite informazioni sulla gestione delle immagini immesse in AFIS e dati ufficiali relativamente all'anno 2024.



UN CONFRONTO CON L'EUROPA

La ricerca comparata condotta nell'ambito del progetto **ha esaminato l'uso e la regolamentazione** delle tecnologie di riconoscimento facciale in dieci giurisdizioni europee: Regno Unito, Francia, Germania, Spagna, Paesi Bassi, Grecia, Svezia, Polonia, Ungheria e Repubblica Ceca. Pur con significative differenze nelle tecnologie impiegate e nei loro scopi operativi, questi paesi condividono un quadro giuridico europeo comune: GDPR, Direttiva Polizia (LED), Convenzione Europea dei Diritti dell'Uomo (CEDU) e, in misura crescente, l'AI Act dell'Unione europea (UE). Ciononostante, dietro questa cornice comune si nascondono pratiche profondamente diverse: il livello di trasparenza, di supervisione e di responsabilità nell'uso del riconoscimento facciale da parte delle forze dell'ordine varia sensibilmente da un paese all'altro.

Uno dei risultati principali della ricerca,

è tanto semplice quanto scomodo: **le norme regolamentari, da sole, non bastano a determinare gli esiti in termini di responsabilità.** La governance pratica del riconoscimento facciale dipende piuttosto da un ecosistema istituzionale più ampio: la capacità e l'indipendenza delle autorità di protezione dei dati, l'accesso ai tribunali e al contenzioso strategico, il controllo parlamentare, il giornalismo investigativo e la capacità della società civile di indagare e contestare le pratiche di sorveglianza.

Il confronto colloca così l'esperienza italiana del sistema SARI all'interno di una tendenza europea più ampia, mettendo notevolmente in luce lacune particolarmente significative nel quadro giuridico italiano.

1. DIVERSI MODELLI DI RESPONSABILITÀ

REGNO UNITO

Il Regno Unito fornisce forse l'esempio più chiaro di **responsabilità costruita attraverso il contenzioso**. La polizia del Galles del Sud iniziò a implementare il sistema di Live Facial Recognition (LFR) nel 2017, senza un quadro sufficientemente chiaro per regolare le implementazioni e le liste di controllo, e con una valutazione inadeguata dei rischi relativi alla protezione dei dati e all'uguaglianza. Nella causa *R (Bridges) v Chief Constable of South Wales Police*,⁴ la Corte stabilì che il quadro normativo lasciava un'eccessiva discrezionalità alle agenti, che la valutazione d'impatto sulla protezione dei dati (DPIA) era inadeguata e che la polizia non aveva adottato misure ragionevoli per valutare i possibili pregiudizi razziali o di genere, quindi in violazione dell'obbligo di uguaglianza nel settore pubblico.

⁴ *R. (on the application of Edward Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 (Court of Appeal, 11 August 2020).

È importante sottolineare che la sentenza non dichiarò discriminatoria la tecnologia in sé, ma stabilì l'obbligo di valutare questo rischio.

È da sottolineare che il riconoscimento facciale non è scomparso dopo *Bridges*. Al contrario, il suo utilizzo si è anzi ampliato notevolmente. Tuttavia, questa espansione è avvenuta all'interno di un quadro di responsabilità molto più sviluppato. La polizia del Galles del Sud pubblica oggi DPIA, valutazioni d'impatto sull'uguaglianza e registri di impiego,⁵ mentre i suoi algoritmi sono stati testati in modo indipendente dal *National Physical Laboratory*.⁶ Nell'agosto 2025 l'Ufficio del Garante per la protezione dei dati ha verificato le operazioni di riconoscimento facciale della polizia del Galles del Sud e della polizia di Gwent, confermando la presenza di “valutazioni d'impatto sulla protezione dei dati appropriate” e attestando un “alto livello di garanzia che i processi e le procedure siano in atto”. Rispetto all'esperienza italiana, caratterizzata dalla mancata divulgazione delle DPIA e dei tassi di errore sulla base dell'invocata “sicurezza”, colpisce che le forze di polizia britanniche pubblichino regolarmente queste informazioni senza compromettere la sicurezza operativa. Va comunque notato che, nonostante i diritti procedurali garantiti da *Bridges*, le forze soggette a tali requisiti hanno da allora ampliato l'utilizzo del LFR a un ritmo senza precedenti, imponendo alle oppositrici oneri di risorse ingenti sostenibili solo da una società civile ben organizzata.



FRANCIA

La Francia, invece, illustra un problema diverso: **solide garanzie legali e costituzionali formali non impediscono necessariamente l'impiego occulto di queste tecnologie.** Un'indagine di Disclose ha rivelato nel 2023 che le forze dell'ordine francesi utilizzavano dal 2015 il software di videosorveglianza BriefCam senza aver svolto la necessaria valutazione d'impatto sulla protezione dei dati né averne notificato l'impiego all'autorità francese competente (CNIL). Il software includeva funzionalità di riconoscimento facciale che, secondo una fonte di polizia citata da Disclose, venivano attivamente utilizzate al di fuori del quadro giuridico applicabile; e, notevolmente, BriefCam sarebbe stato impiegato dalle polizie municipali di oltre 100 comuni francesi.⁸ Le conclusioni del CNIL di dicembre 2024 hanno confermato che, pur non essendo stato utilizzato operativamente il riconoscimento facciale in tempo reale negli spazi pubblici, la funzione era disponibile nei software installati, ed è stato documentato *almeno un caso* del suo utilizzo in un'indagine giudiziaria.⁹

Il caso francese mostra il ruolo cruciale del giornalismo investigativo e della società civile nell'individuare, denunciare e contrastare l'impiego illecito o opaco delle tecnologie biometriche. Il lavoro delle ONG come La Quadrature du Net o Ligue des droits de l'Homme (LDH) dimostra come il contenzioso strategico possa tradursi in una reale responsabilizzazione istituzionale di fronte a violazioni sistemiche dei diritti umani.¹⁰

⁵ Polizia del Galles del Sud. Documentazione sulla tecnologia di riconoscimento facciale, 2017-2025

⁶ Polizia del Galles del Sud. Documentazione sulla tecnologia di riconoscimento facciale, 2017-2025, reperito tramite: [link](#), ultimo accesso il 13/09/2026.

⁷ Information Commissioner's Office: audit of the use of Facial Recognition Technology | South Wales Police

⁸ Disclose.ngo – La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale

⁹ Utilizzo di BriefCam e di altri software di analisi video da parte dello Stato e dei comuni: la CNIL emette diverse comunicazioni formali.

¹⁰ Ligue des droits de l'Homme, “BriefCam: souriez, vous êtes filmés!” (2023), recuperato tramite: <https://www.ldh-france.org/briefcam-souriez-vous-etesfilmés/>, ultimo accesso il 12/09/2026.

Questo successo nello smascherare l'uso illegale delle tecnologie convive però con una **tendenza parallela alla normalizzazione**: nel settembre 2025 il Ministro della Giustizia Gérald Darmanin ha istituito un gruppo di lavoro per legalizzare il riconoscimento facciale in tempo reale, ribaltando la posizione assunta nel 2022 - un cambiamento che segna una più ampia ricalibrazione dell'approccio francese alla sorveglianza biometrica, in cui le esigenze di sicurezza vengono sempre più spesso invocate per giustificare l'espansione.¹¹

GERMANIA

La Germania offre un quadro più articolato: **la sua struttura federale crea al tempo stesso vulnerabilità e meccanismi di responsabilità che mancano ai sistemi più centralizzati**. Il sistema di riconoscimento facciale dell'Ufficio federale di polizia criminale (BKA), noto come GES, confronta fotografie riprese da telecamere di sorveglianza o reperite online con i database della polizia per identificare persone sconosciute; sistemi analoghi sono stati adottati dall'Ufficio di polizia criminale bavarese e da altre autorità di polizia statali.¹² Solo nel 2023 il sistema del BKA ha elaborato 117.894 ricerche, mentre il database INPOL conteneva circa 7,3 milioni di fotografie relative a oltre 5 milioni di persone.¹³ Un dato particolarmente rilevante per il confronto con l'Italia è che oltre 3 milioni di queste immagini provengono da “fonti non di polizia”, per lo più richieste di asilo:¹⁴ un parallelismo significativo con la composizione del database SARI, anch'esso *in larga parte alimentato da dati biometrici legati all'immigrazione*. A differenza dell'Italia, però, **i meccanismi di controllo parlamentare tedeschi rendono pubbliche le informazioni sulla portata e sulla composizione di questi database**.¹⁵

La Germania offre altri due esempi rilevanti.

Durante il progetto pilota **Berlin Südkreuz** del 2017-2018, la Polizia Federale testò tre sistemi di riconoscimento facciale presso un'importante stazione ferroviaria, utilizzando un database di riferimento composto da immagini di partecipanti volontari; la valutazione finale fu positiva, e concluse che la tecnologia avrebbe potuto rappresentare uno strumento utile per le perquisizioni di polizia in ambito ferroviario.¹⁶

Invece, in seguito all'utilizzo del sistema **Video 360** per analizzare l'ampio materiale audiovisivo delle proteste del G20 di Amburgo nel 2017,¹⁷ l'Autorità per la protezione dei dati di Amburgo concluse che il trattamento mancava di un'adeguata base giuridica e ordinò la cancellazione del database biometrico creato dalla polizia.

¹¹ Bastien Loeuillot, “Caméra «Opposé» à la reconnaissance faciale en 2022, Gérald Darmanin souhaite désormais la création d'un groupe de travail sur le sujet”, *Liberation* (2025), recuperato tramite: [link](#), ultimo accesso il 12/09/2026; Félix Tréguer, “Le serpent de mer de la reconnaissance faciale”, *Analyse Opinion Critique* (2025), recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

¹² [Deutsch institut für menschenrechte, Polizeiliche Gesichtserkennung Menschenrechtliche Herausforderungen einer Risikotechnologie, p.11.](#)

¹³ Matthias Monroy. New police technology in Germany: Unleashed facial recognition takes off. *digit.site36.net*, 16 December 2024, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

¹⁴ Ibidem.

¹⁵ <https://netzpolitik.org/2024/neues-bka-system-polizeiliche-gesichtserkennung-geht-steil/>

¹⁶ Bundespolizeipräsidium, Abschlussbericht des Bundespolizeipräsidiums zum Teilprojekt 1 „Biometrische Gesichtserkennung“ am Bahnhof Berlin Südkreuz, 18 September 2018.

¹⁷ Videmo 360 è un software di riconoscimento facciale che rileva i volti in immagini e video, estrae i tratti somatici caratteristici e li converte in modelli matematici memorizzati in un database di riferimento. Questi modelli possono quindi essere confrontati con grandi quantità di filmati per identificare la stessa persona e ricostruirne i movimenti, il comportamento e i contatti sociali in luoghi e momenti diversi.

L'ordine fu impugnato dalle autorità di Amburgo e inizialmente annullato dal Tribunale amministrativo locale, ma la polizia cancellò comunque il database nel 2020; il successivo procedimento d'appello fu archiviato nel 2023 senza una sentenza definitiva sulla legalità del sistema. Nonostante ciò, gli sviluppi successivi al 2024 mostrano una continua espansione delle capacità di sorveglianza biometrica: nella primavera del 2024 indagini parlamentari e giornalistiche hanno rivelato l'uso occulto del sistema PerIS, sviluppato dalla polizia della Sassonia e impiegato anche in indagini condotte con altri Länder,¹⁸ mentre nel dicembre 2025 il Parlamento di Berlino ha adottato una riforma di ampia portata della legge di polizia cittadina (ASOG), ampliando i poteri di sorveglianza e autorizzando espressamente, previa approvazione giudiziaria, l'uso di dati biometrici per identificare o localizzare individui attraverso il confronto con immagini e altri dati pubblicamente accessibili online.¹⁹



GRECIA

La Grecia offre un esempio particolarmente istruttivo dei rischi legati all'acquisizione e implementazione di tecnologie di sorveglianza biometrica prima che siano predisposte adeguate garanzie legali e istituzionali.²⁰

Il programma **Smart Policing** ha dotato la polizia ellenica di dispositivi portatili in grado di riconoscimento facciale e identificazione delle impronte digitali,²¹ mentre l'infrastruttura di sorveglianza più ampia, che comprende i sistemi Centaur e Hyperion, si estende ai sistemi biometrici dispiegati nei campi profughi e ai confini del paese.²² Il programma Smart Policing è particolarmente significativo perché i suoi obiettivi dichiarati includevano esplicitamente l'identificazione delle cittadine di paesi terzi che avevano superato il periodo di residenza autorizzato, a dimostrazione di come il riconoscimento facciale possa essere strettamente integrato con le attività di contrasto all'immigrazione.²³ A seguito di una denuncia presentata da Homo Digitalis e di oltre cinque anni di indagini, l'Autorità ellenica per la protezione dei dati ha concluso nel 2025 che il quadro giuridico esistente **non forniva una base legale sufficiente** per l'attivazione del programma Smart Policing e che la Polizia ellenica **non aveva condotto una DPIA tempestiva e adeguata**.²⁴

¹⁸ Sächsische Datenschutz- und Transparenzbeauftragte, Tätigkeitsbericht Datenschutz 2024, pp. 26 ff. (section 1.1, Polizeilicher Einsatz automatisierter Gesichtserkennung in Strafverfahren); see also Lower Saxony Data Protection Authority investigation into the use of PerIS, Giugno 2024.

¹⁹ Abgeordnetenhaus Berlin, Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts, adopted 4 December 2025; see in particular § 28a ASOG, Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet.

²⁰ Computer Weekly, "Greek government fined over AI surveillance in refugee camps," April 2024, recuperato tramite: [Greek government fined over AI surveillance in refugee camps | Computer Weekly](#), ultimo accesso il 12/09/2026.

²¹ Homo Digitalis and AlgorithmWatch, joint investigative publication, dicembre 2019; AlgorithmWatch, "Flush with EU funds, Greek police to introduce live face recognition before the summer," gennaio 2021, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

²² Homo Digitalis, "Drones & Artificial Intelligence at Greece's high-tech borders," recuperato tramite: [homodigitalis.gr/en/posts/131019](#), ultimo accesso il 12/09/2026.

²³ Eleftherios Chelioudakis, "Greece: Technology-led policing awakens," about:intel, 29 June 2020, Available at [aboutintel.eu](#). See also Homo Digitalis, "Hellenic Police plans to introduce face recognition technology," 16 December 2019, recuperato tramite: [homodigitalis.gr/en/posts/4965](#), ultimo accesso il 12/09/2026.

²⁴ HDPA, Decisione 45/2025, 31 dicembre 2025, disponibile (in greco) all'indirizzo [dpa.gr](#). Riassunto in inglese in [Posttoo.de](#), "Greece: Planned 'smart policing' system is unlawful," 20 gennaio 2026.

L'Autorità ha quindi vietato l'attivazione del sistema nell'ambito del quadro giuridico vigente, rendendo necessaria una nuova legislazione per il suo utilizzo lecito. Il caso evidenzia i rischi dell'acquisizione di tecnologie biometriche ad alto rischio senza adeguate garanzie legali e i limiti strutturali di una supervisione istituzionale efficace. Al contempo, grazie all'impegno costante di Homo Digitalis, questa circostanza dimostra, ancora una volta, il **ruolo cruciale che la società civile** può svolgere nel contrastare la sorveglianza illegale e nell'assicurare una reale responsabilizzazione.²⁵ L'esperienza greca offre quindi un esempio particolarmente prezioso per le ONG, dimostrando come strategie legali e di sensibilizzazione mirate possano tradurre le preoccupazioni relative alle tecnologie emergenti in vincoli istituzionali concreti per la loro diffusione.

**ALTRE GIURISDIZIONI RIVELANO INVECE FORME DI
RESPONSABILITÀ
SOSTANZIALMENTE PIÙ DEBOLI.**

 SPAGNA

In Spagna, il Sistema automatizzato di identificazione biometrica (ABIS), implementato dalla Polizia nazionale e dalla Guardia civile, operativo dal 2023 e contenente circa 4,4-5 milioni di immagini facciali, fu testato senza consultare l'Autorità spagnola per la protezione dei dati (AEPD), e la supervisione indipendente resta oggi limitata.²⁶

Le esperte hanno espresso preoccupazione per un quadro normativo giudicato troppo generico per garantire tutele sostanziali, con lacune significative relative alle garanzie rispetto all'acquisizione delle immagini, alla gestione del database e alle condizioni d'uso:²⁷ sebbene l'utilizzo di ABIS richieda un'autorizzazione giudiziaria, la normativa non prevede audit algoritmici indipendenti.²⁸

Si tratta di una mancanza particolarmente preoccupante, dato il rischio che i sistemi algoritmici operino in modo opaco e discriminatorio, ragione per cui le studiose sottolineano la **necessità di maggiori garanzie costituzionali nell'utilizzo del riconoscimento facciale** in Spagna.²⁹ Il paese assomiglia così all'Italia nel combinare un sistema di identificazione biometrica ex post su larga scala con una verifica indipendente limitata delle sue effettive prestazioni. Inoltre, il caso spagnolo mostra perché la valutazione del riconoscimento facciale non possa prescindere dall'analisi di com'è costruito il database sottostante, da dove provengono i dati biometrici e per quali scopi furono originariamente raccolti.

²⁵ Homo Digitalis e AlgorithmWatch, pubblicazione investigativa congiunta, dicembre 2019. Vedi anche AlgorithmWatch, "Ricca di fondi UE, la polizia greca introdurrà il riconoscimento facciale in tempo reale prima dell'estate", gennaio 2021, consultato tramite: [Grazie ai finanziamenti europei, la polizia greca introdurrà il riconoscimento facciale in tempo reale prima dell'estate - AlgorithmWatch](#), ultimo accesso il 12/09/2026.

²⁶ Business Insider, "Il Ministero dell'Interno ammette di non aver consultato l'Agenzia spagnola per la protezione dei dati (AEPD) in merito all'algoritmo di riconoscimento facciale che sta addestrando per la polizia" 26 dicembre 2022, recuperato tramite: [link](#), ltimo accesso il 12/09/2026.

²⁷ Lorena Pérez Campillo, "the Use of Artificial Intelligence and the Processing of Biometric Data by Law Enforcement Authoritties" (Forthcoming), [link](#); M^a Josefa Ridaura Martínez, " El reconocimiento facial como herramienta securitaria" (2025), recuperato tramite: [link](#), ultimo accesso 12/09/2026

²⁸ COPolicial, "El uso del sistema automático de reconocimiento facial en las investigaciones policiales" (2024), recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

²⁹ Lorena Pérez Campillo, "the Use of Artificial Intelligence and the Processing of Biometric Data by Law Enforcement Authoritties" (Forthcoming), [link](#); M^a Josefa Ridaura Martínez, " El reconocimiento facial como herramienta securitaria" (2025), recuperato tramite: [link](#), ultimo accesso 12/09/2026



PAESI BASSI

I Paesi Bassi presentano un confronto particolarmente rilevante con l'Italia, soprattutto per l'architettura a doppio database del sistema CATCH (Centrale Automatische TeChnologie voor Herkenning van personen).³⁰ Secondo fonti di polizia, CATCH si basa su due categorie principali di immagini di riferimento: i) immagini raccolte in contesti di giustizia penale (persone arrestate, sospettate e condannate - CATCH Strafrecht/diritto penale); ii) un database separato di immagini relative alle "straniere".³¹ Commenti accademici e inchieste giornalistiche hanno sollevato dubbi sul fatto che quest'ultimo possa includere foto di permessi di soggiorno di richiedente asilo, studente straniero ed espatriate - individui spesso non sospettati di alcun reato - rendendo così disponibile al confronto facciale della polizia un'ampia popolazione estranea a qualsiasi indagine.³² L'esistenza e il funzionamento di CATCH-Vreemdelingen hanno attirato notevole attenzione pubblica nel 2023, a seguito di un'inchiesta giornalistica che ha rivelato la presenza di milioni di fotografie di cittadine straniere in un database utilizzabile dalla polizia per il confronto facciale, sollevando interrogativi parlamentari sulla base giuridica del sistema, sull'accesso della polizia al database e sulla sua compatibilità con i requisiti di protezione dei dati dell'UE.³³

Allo stesso tempo, le comunicazioni pubbliche della polizia offrono informazioni solo limitate sulla base giuridica e sul funzionamento di CATCH: mancano infatti dati sistematici su politiche di conservazione delle informazioni, meccanismi di verifica, tassi di errore e altre misure di sicurezza tecniche. Questa **mancaanza di trasparenza** è particolarmente problematica data l'elevata rischiosità del riconoscimento facciale e **limita la possibilità di un controllo pubblico efficace** sull'utilizzo del sistema e sui dati biometrici delle persone coinvolte.

30 Politie.nl, Veel herkenning bij gezichtsvergelijkingen voor opsporing in 2024 (21 Jul 2025), recuperato tramite: [linkpolitie.nl](#), ultimo accesso il 12/09/2026.

31 Politie.nl, Veel herkenning bij gezichtsvergelijkingen voor opsporing in 2024 (21 Jul 2025), recuperato tramite: [link1|politie.nl](#), ultimo accesso il 12/09/2026.

32 Expats, asylum seekers and foreign students in biometric police database, Utrecht University 16 February, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

33 Autoriteit Persoonsgegevens, Juridisch kader gezichtsherkenning; [link1](#); [link2](#)

IL CONFRONTO IDENTIFICA ANCHE TRAJETTORIE PIÙ RECENTI E DIVERGENTI.



SVEZIA, POLONIA, UNGHERIA, REPUBBLICA CECA

La **Svezia** si è orientata verso una regolamentazione esplicita del riconoscimento facciale, che prevede, tra l'altro, meccanismi di autorizzazione per ogni singola implementazione (salvo un'esenzione di emergenza di 24 ore), collegando al contempo esplicitamente l'espansione della tecnologia di riconoscimento facciale (FRT) all'applicazione delle norme in materia di immigrazione.³⁴ Anche la **Polonia** ha ampliato il quadro normativo sull'uso dei dati biometrici, incluse le immagini facciali, da parte delle forze dell'ordine a fini di identificazione, indagine e prova. Questi poteri, tuttavia, devono ora essere interpretati alla luce dei requisiti più stringenti dell'AI Act dell'UE, che disciplina l'identificazione biometrica remota in tempo reale negli spazi pubblicamente accessibili, imponendo in linea di principio l'autorizzazione preventiva di un'autorità giudiziaria o amministrativa indipendente.³⁵ L'**Ungheria** solleva preoccupazioni ancora più acute sul piano dei diritti umani, con una legislazione che consente l'uso del riconoscimento facciale per identificare i partecipanti a eventi Pride vietati.³⁶

La **Repubblica Ceca** offre, invece, un esempio di come un'applicazione rigorosa delle norme possa costruire un efficace strumento di controllo: nell'agosto 2025 il riconoscimento facciale presso l'aeroporto Václav Havel di Praga è stato interrotto a seguito di un'attenta analisi regolatoria, con il nuovo quadro normativo sull'intelligenza artificiale che ha contribuito a stabilirne l'illegittimità.³⁷

34 Biometric Update, Sweden authorizes police use of live facial recognition, 29 Maggio 2026 recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

35 Poland, Act on the Police of 6 April 1990, consolidated tda ext Dz.U. 2025 poz. 636, Art. 20(1aa); Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(h), (2)–(5). Poland, Act on the Police of 6 April 1990, consolidated text Dz.U. 2025 poz. 636, Art. 20(1aa); Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(h), (2)–(5).

36 Civil Liberties Union for Europe. Facial Recognition to Target Pride in Hungary: Civil Society Orgs Call On The EU to Commit to Rights and Rule of Law. Liberties.eu, 24 June 2025, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

37 Iuridicum Remedium (IuRe). Czech police forced to turn off facial recognition at the airport. European Digital Rights (EDRI), 29 ottobre 2025, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

2. IL PROBLEMA STRUTTURALE: CHI FIGURA NEL DATABASE?

Uno dei risultati più importanti della ricerca non riguarda l'algoritmo di riconoscimento facciale in sé, ma la **composizione dei database** su cui vengono effettuate le ricerche. In Italia, Germania, Paesi Bassi e Grecia, informazioni biometriche originariamente raccolte nell'ambito di procedure di immigrazione o asilo sono state collegate alle infrastrutture di identificazione delle forze dell'ordine.

In Germania, circa 3,06 milioni delle 7,29 milioni di fotografie del database INPOL provengono da fonti non di polizia, prevalentemente da richieste di asilo.³⁸ Nei Paesi Bassi, il database CATCH Aliens contiene circa otto milioni di fotografie di cittadini non appartenenti all'UE.³⁹ In Grecia, il programma Smart Policing, finanziato dall'UE, includeva esplicitamente tra i propri obiettivi l'identificazione dei cittadini di paesi terzi in soggiorno irregolare.⁴⁰

Questo schema è particolarmente rilevante per l'Italia, dove circa l'80% delle immagini facciali presenti nel database in questione riguarda cittadini stranieri, pur rappresentando quest'ultime solo circa il 9% della popolazione. Il problema, dunque, non si limita a stabilire se un algoritmo si comporti diversamente in base all'etnia, al sesso o all'età: **il pregiudizio può generarsi anche a livello strutturale, attraverso la composizione stessa della popolazione di riferimento.** I gruppi sovrarappresentati in un database sono di conseguenza più esposti alle ricerche biometriche e al rischio di errata identificazione, mentre il riutilizzo a fini di un'indagine penale di dati biometrici raccolti originariamente in contesto migratorio o amministrativo solleva questioni specifiche in materia di limitazione delle finalità, base giuridica e conservazione dei dati.

La Spagna illustra un meccanismo correlato: laddove le comunità razzializzate sono esposte in modo sproporzionato a fermi di polizia e pratiche di identificazione,⁴¹ le **disuguaglianze preesistenti rischiano di riprodursi nei database successivamente utilizzati per il riconoscimento facciale.** La governance di queste tecnologie non può quindi essere valutata solo sulla base dell'accuratezza algoritmica: richiede un'attenta analisi di come vengono costruiti i database di riferimento, di chi vi figura, del motivo per cui i dati sono originariamente raccolti e per quanto tempo vengono conservati.

LE DISUGUAGLIANZE PREESISTENTI RISCHIANO DI RIPRODURSI NEI DATABASE SUCCESSIVAMENTE UTILIZZATI PER IL RICONOSCIMENTO FACCIALE.

³⁸ Biometric Update, Sweden authorizes police use of live facial recognition, 29 Maggio 2026 recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

³⁹ Poland, Act on the Police of 6 April 1990, consolidated text Dz.U. 2025 poz. 636, Art. 20(1aa); Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(h), (2)–(5). Poland, Act on the Police of 6 April 1990, consolidated text Dz.U. 2025 poz. 636, Art. 20(1aa); Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(h), (2)–(5).

⁴⁰ Civil Liberties Union for Europe. Facial Recognition to Target Pride in Hungary: Civil Society Orgs Call On The EU to Commit to Rights and Rule of Law. Liberties.eu, 24 June 2025, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

⁴¹ Iuridicum Remedium (IuRe). Czech police forced to turn off facial recognition at the airport. European Digital Rights (EDRI), 29 ottobre 2025, recuperato tramite: [link](#), ultimo accesso il 12/09/2026.

3. CONCLUSIONI: COSA CI DICE QUESTO CONFRONTO SU SARI

In questo contesto europeo, le lacune di responsabilità relative a SARI Enterprise emergono con particolare evidenza. Nel 2024 il sistema è stato utilizzato per 181.705 ricerche di riconoscimento facciale, contro le 79.362 del 2022, un aumento di circa il 130% in due anni. Il Ministero dell'Interno, tuttavia, non ha fornito dati che consentano di valutarne l'efficacia, i tassi di falsi positivi o le prestazioni demografiche; la ricerca ha inoltre riscontrato l'assenza di una DPIA specifica per SARI, di un quadro di valutazione indipendente pubblicato e di una documentazione chiara sulla necessità e proporzionalità del suo utilizzo.

Il confronto europeo dimostra che **questo livello di opacità non è tecnicamente inevitabile**. Le forze di polizia del Regno Unito pubblicano valutazioni d'impatto, statistiche d'impiego e informazioni sui test degli algoritmi. I meccanismi parlamentari tedeschi rendono pubbliche la portata del riconoscimento facciale e la composizione dei database di polizia. Le autorità olandesi pubblicano informazioni sui risultati del progetto CATCH, e l'autorità nazionale per la protezione dei dati ha sollevato pubblicamente dubbi su alcuni suoi aspetti. Tribunali e autorità di protezione dei dati, nel Regno Unito come in Francia, Germania e in altre giurisdizioni, sono intervenuti per esaminare o limitare impieghi specifici della tecnologia.

Il confronto suggerisce quindi che una **reale responsabilizzazione richieda più della semplice conformità formale** a un quadro normativo europeo comune. Sono necessari, come minimo: una base giuridica chiara e specifica; valutazioni d'impatto dedicate; la raccolta e pubblicazione sistematica di dati su implementazione, risultati ed errori; test tecnici indipendenti, incluse le prestazioni demografiche; una supervisione efficace da parte delle autorità di protezione dei dati e dei tribunali; e un esame approfondito di composizione, scopo e periodi di conservazione dei database biometrici. In questo senso, l'AI Act aggiunge un ulteriore livello di responsabilità, comprese le restrizioni sull'identificazione biometrica remota in tempo reale e gli obblighi per i sistemi ad alto rischio; tuttavia, la sua efficacia dipenderà, in ultima analisi, dalla sua concreta applicazione.

La lezione fondamentale derivante da questa ricerca comparativa è che **il vero nodo della responsabilità non sta nella tecnologia di riconoscimento facciale in sé, ma nella possibilità di renderne visibile, misurabile e contestabile il funzionamento**. La prassi europea dimostra che misure di salvaguardia più efficaci sono possibili.

QUINDI, LA TRASPARENZA INSOLITAMENTE LIMITATA CHE CIRCONDA SARI NON VA LETTA COME CONSEGUENZA INEVITABILE DELLA SEGRETEZZA DELLE FORZE DELL'ORDINE, MA COME IL RISULTATO, ALMENO IN PARTE, DI PRECISE SCELTE ISTITUZIONALI E NORMATIVE.

**Questo report è stato
realizzato da:**

STRALI
strategic litigation



**PRIVACY
NETWORK**



**Seguici sui social di Privacy
Network e Strali**

PER MAGGIORI INFORMAZIONI:

privacy-network.it
www.strali.org

Funded by European
Artificial Intelligence
& Society Fund