



**LINEE GUIDA N. 5/2022**  
sull'uso della tecnologia di  
riconoscimento facciale

**Avv. Lorenzo Tamos**

lorenzo.tamos@avvocatinTEAM.com

Il 12 maggio 2022 l'EDPB ha licenziato le Linee Guida sul riconoscimento facciale quale trattamento di dati biometrici tra i più delicati, nonché sempre più diffuso e che, dall'angolo visuale della normativa c.d. "data protection", mette a dura prova i centrali elementi della **proporzionalità** e della **necessità** di (poter lecitamente) trattare i dati delle persone fisiche.



**Accertamento,  
prevenzione e  
SICUREZZA  
(COLLETTIVA)**

**LIBERTA' E  
DIRITTI  
FONDAMENTALI  
DELLA PERSONA**





**EDPB:** “L'uso dei dati biometrici e in particolare della FRT, può ledere il diritto alla dignità umana, quale diritto sancito dall'articolo 1 della Carta.

La **dignità umana** richiede che **gli individui non siano trattati come semplici oggetti**.

La FRT calcola le **caratteristiche esistenziali** e altamente personali, i tratti del viso, in una forma leggibile da una macchina **con lo scopo di usarli come targa umana o carta d'identità, oggettivando così il viso”**.

Dice Kant: «*L'imperativo pratico è formulabile nel modo seguente: Agisci in modo da trattare l'umanità, così nella tua persona come nella persona di ogni altro, sempre come un fine, e mai come un mezzo*»



Il riconoscimento facciale è usato per

(A) **autenticare** o

(B) **identificare** una persona

ed ha **due** principali **utilizzi**:

(1) **individuare** le persone già inserite in elenchi di polizia;

(2) **monitorare** i movimenti di una o più persone nello **spazio pubblico**



La **tecnologia FRT** si basa sul trattamento di **dati biometrici** e, pertanto, comprende il trattamento di categorie **particolari di dati personali** (art. 9 GDPR).

La FRT utilizza applicativi tecnologici **dell'intelligenza artificiale (AI)** o **dell'apprendimento automatico (ML)**.

## Cos'è la tecnologia FRT?



E' MOLTO  
PROBABILE...

Il riconoscimento facciale è una **tecnologia probabilistica** che **riconoscere automaticamente gli individui in base al loro viso** per autenticarli o identificarli. La FRT rientra nella **categoria della tecnologia biometrica**.

La **biometria** comprende in genere tutti i processi automatizzati utilizzati per **riconoscere un individuo in base alle caratteristiche fisiche, fisiologiche o comportamentali** (impronte digitali, struttura dell'iride, voce, andatura, schemi dei vasi sanguigni, ecc.). Tali caratteristiche sono definite "**dati biometrici**", perché **consentono o confermano l'identificazione univoca** di quella persona.

È il caso dei **volti delle persone** o, più precisamente, **della loro elaborazione tecnica** mediante dispositivi di riconoscimento facciale: infatti, riprendendo l'immagine di un volto (da una fotografia o da un video), chiamato "**campione**" biometrico è possibile estrarre una **rappresentazione digitale** di **caratteristiche distintive** di un **volto** (il "**modello**").

Un **modello biometrico** è una **rappresentazione digitale delle caratteristiche uniche** che sono state estratte da un campione biometrico e possono essere archiviate in un database biometrico. Il **modello dovrebbe essere unico e specifico per ogni persona** ed è, in linea di principio, **permanente nel tempo** (ciò potrebbe dipendere dal tipo di biometria e dall'età dell'interessato) In fase di riconoscimento, il dispositivo confronta questo modello con altri modelli precedentemente testati.



## Esempi di identificazione RTF

**ricerca, in un database di fotografie, dell'identità** di una persona non identificata;

**monitoraggio dei movimenti di una persona nello spazio pubblico.** Il suo volto viene confrontato con i modelli biometrici di persone che viaggiano o hanno viaggiato nell'area monitorata, ad es. quando viene lasciato un bagaglio o dopo che è stato commesso un reato;

**ricostruire il percorso di una persona e le sue successive interazioni con altre persone,** attraverso un confronto ritardato degli stessi elementi al fine di individuarne ad esempio i contatti. Tutti i volti catturati dal vivo dalle telecamere di video protezione vengono confrontati, in tempo reale, con un database tenuto dalle forze di sicurezza;

**riconoscimento automatico delle persone in un'immagine** per identificare, ad es., le loro relazioni su un social network che ne fa uso. L'immagine viene confrontata con i modelli di tutti coloro che in rete hanno acconsentito a questa funzionalità;

**accesso ai servizi, con alcuni sportelli automatici che riconoscono i propri clienti,** confrontando un volto catturato da una telecamera con il database delle immagini del viso in possesso della banca;

**tracciamento del viaggio di un passeggero.** Il template, calcolato in tempo reale, di qualsiasi persona che effettua il check-in ai varchi ubicati in determinate fasi del viaggio (punti di riconsegna bagagli, gate d'imbarco, ecc.), viene confrontato con i template delle persone precedentemente registrate nel sistema.





L'utilizzo della FRT non consenta solo l'elaborazione dei dati su **larga scala** ma crea anche il **rischio di discriminazione** personali e di **risultati falsi**. Del resto, la FRT, può essere utilizzata anche rispetto a grandi **folle di persone** ed importanti **snodi di trasporto**.

La tecnologia FRT è uno **strumento delicato messo a disposizione delle autorità competenti (LEA)**.

Le LEA sono **autorità esecutive** ed esercitano **poteri che dipendono dagli Stati sovrani**.

La FRT è incline ad **interferire con i diritti fondamentali** degli individui – anche al di là del diritto alla protezione dei dati personali – ed è peraltro **in grado di incidere sulla stabilità politica, sociale e democratica degli Stati**.



Per la protezione dei dati personali nel contesto delle FFOO, devono essere soddisfatti i **requisiti della** DPDPG che prevede un certo quadro normativo relativo all'uso della FRT: art. 3, par. 13, “dati biometrici”; art. 4, principi; art. 8, liceità; art. 10, categorie particolari di dati; art. 11: processo decisionale automatizzato.

**Molti diritti fondamentali possono essere pregiudicati dall'utilizzazione della FRT.**

Pertanto, la **CDFUE** è essenziale per l'interpretazione del diritto alla protezione dei dati personali di cui all'art. 8 della CDFUE, ma anche per il diritto alla “privacy” sancito dall'art. 7 della medesima Carta.

Le **misure legislative** che fungono da base giuridica per il trattamento dei dati **interferiscono direttamente** con i diritti garantiti dagli **artt. 7 e 8 della Carta**.

**Infatti, il trattamento dei dati biometrici costituisce in ogni circostanza, e di per sé, una grave interferenza.** E tale interferenza **non dipende solo dall'esito di un risultato costituito, ad esempio, da un abbinamento positivo che genera un dato biometrico.** Invero, **qualsiasi limitazione all'esercizio dei diritti e delle libertà fondamentali deve essere prevista dalla legge e rispettare l'essenza di tali diritti e libertà.**

La base giuridica deve essere **sufficientemente chiara** per fornire ai cittadini un'adeguata indicazione delle condizioni e delle circostanze in cui le autorità sono abilitate a ricorrere alla TFR. Un **mero recepimento nel diritto interno della clausola generale dell'art. 10 della DPDGP mancherebbe di precisione e prevedibilità.**

Prima che il **legislatore nazionale crei una nuova base giuridica** per qualsiasi forma di trattamento dei dati biometrici mediante il riconoscimento facciale, è **“opportuno” consultare l'autorità di controllo** della protezione dei dati competente.

Le misure legislative devono essere **idonee al raggiungimento** degli **obiettivi legittimi** perseguiti dalla normativa adottata. Un **obiettivo di interesse generale** – per quanto importante possa essere – **non giustifica, di per sé, una limitazione a un diritto fondamentale.**

Le misure legislative dovrebbero **differenziare** e prendere di mira le persone interessate alla luce di un obiettivo specifico, ad esempio contrastare specifici reati gravi. Se la misura **riguarda tutte le persone in modo generale** senza tale differenziazione, limitazione o eccezione, essa **intensifica la portata dell'interferenza, specie se il trattamento dei dati riguarda una parte significativa della popolazione.**



Se i dati sono trattati sistematicamente all'insaputa degli interessati, si può generare una **concezione generale di sorveglianza costante**.

Ciò può comportare **effetti devastanti per quanto riguarda alcuni o tutti i diritti fondamentali**: come la dignità umana ai sensi dell'art. 1, la libertà di pensiero, coscienza e religione (art. 10), la libertà di espressione (art. 11), la libertà di riunione e di associazione (art. 12) della Carta.

Il trattamento di **categorie particolari** di dati, come i dati biometrici, può essere considerato "**strettamente necessario**" (art. 10 DPDPG) solo se l'interferenza con la protezione dei dati personali e le sue limitazioni è **indispensabile**, escludendo qualsiasi trattamento di natura generale o sistematica.



## Alcuni principi

Il fatto che **una fotografia** sia stata **manifestamente resa pubblica** dall'interessato **non comporta che i relativi dati biometrici, desumibili dalla fotografia con mezzi tecnici, siano considerati resi pubblici**. Le impostazioni predefinite di un servizio, ad es. caratterizzati dall'assenza di scelta, quali i modelli resi pubblici senza che l'utente possa modificare l'impostazione, **non devono mai essere interpretate come dati resi pubblici**.

L'art. 11 LED riguarda il **processo decisionale automatizzato**. La FRT usa dati particolari e può comportare profilazione, a seconda delle modalità e finalità per le quali è stata adottata. Ai sensi del diritto UE e dell'art. 11, par. 3, LED, è **vietata la profilazione che comporti una discriminazione nei confronti di persone fisiche sulla base di categorie particolari di dati**.

L'art. 6 LED impone di **distinguere tra diverse categorie di interessati**. Per gli interessati per i quali **non esistono elementi idonei a far pensare che la loro condotta possa avere un nesso**, anche indiretto o remoto, con la finalità legittima perseguita, è probabile che **non vi è giustificazione di un'ingerenza**.

Il **principio di minimizzazione dei dati** (art. 4, par. 1, lett. e, LED) richiede che qualsiasi **materiale video non pertinente allo scopo del trattamento sia sempre rimosso o reso anonimo** (ad es. sfocando senza possibilità di recuperare i dati) prima della diffusione.

Il titolare del trattamento deve considerare bene **come e se può** soddisfare i **diritti dell'interessato prima che venga avviato qualsiasi trattamento FRT** poiché spesso esso comporta il trattamento di categorie particolari di dati senza alcuna interazione apparente con l'interessato.

L'effettivo **esercizio dei diritti è subordinato all'adempimento** da parte del titolare dei propri **obblighi di informazione** (art. 13 LED). Nel valutare un "caso specifico" è necessario considerare diversi fattori, compreso se i dati personali sono raccolti all'insaputa dell'interessato.

Se il processo decisionale si basa solo su tecnologia FRT, **gli interessati devono essere informati sulle caratteristiche del processo decisionale automatizzato**.

Per le **richieste di accesso**, quando i dati biometrici sono archiviati e collegati a un'identità anche mediante dati **alfanumerici**, ciò dovrebbe consentire all'autorità di dare riscontro ad una richiesta di accesso basata su una ricerca mediante tali dati alfanumerici, senza ulteriori elaborazioni di dati biometrici altrui.

I **rischi** per gli interessati sono **gravi** se **dati inesatti sono archiviati in un database di polizia** e/o condivisi con altri soggetti. Il titolare deve **correggere** i dati memorizzati e i sistemi di FRT (C. 47 LED).

Il diritto alla **restrizione** diventa molto importante quando si tratta di tecnologia di FRT basata su **algoritmi** e quindi **non porti mai un risultato definitivo** in situazioni in cui vengono raccolte grandi quantità di dati e l'accuratezza e la qualità dell'identificazione possono variare.



**Una DPIA prima dell'uso di FRT è un requisito obbligatorio**, cfr. art. 27 LED.

L'EDPB **raccomanda di rendere pubblici i risultati di tali valutazioni**, o **almeno i principali risultati e conclusioni della DPIA**, come misura di rafforzamento della fiducia e della trasparenza.

La maggior parte dei casi di diffusione e utilizzo di FRT **comporta un rischio intrinseco elevato** per i diritti e le libertà degli interessati. Pertanto, l'autorità che utilizza l'FRT dovrebbe **consultare l'autorità di vigilanza competente prima dell'installazione del sistema**.

Posta la natura unica dei dati biometrici, l'autorità che usa tecnologia FRT dovrebbe prestare particolare attenzione alla **sicurezza del trattamento**, in linea con l'art. 29 LED. Le autorità dovrebbero garantire che il sistema sia conforme alle norme e attuare misure di protezione dei modelli biometrici.

**I principi e le garanzie di protezione dei dati devono essere incorporati nella tecnologia prima dell'inizio del trattamento**. Pertanto, anche quando una LEA intende applicare e utilizzare FRT da **fornitori esterni**, **deve garantire**, ad esempio **attraverso la procedura di appalto**, che siano implementate solo le FRT basate sui principi della **protezione dei dati fin dalla progettazione e per impostazione predefinita**.

La **registrazione** (cfr. art. 25 LED) costituisce un importante presidio per la verifica della liceità del trattamento, sia internamente (es. autocontrollo da parte del titolare/responsabile del trattamento) sia da parte delle autorità di controllo esterne. Nell'ambito dei sistemi di riconoscimento facciale, la registrazione è consigliata anche per le modifiche al database di riferimento e per tentativi di identificazione o verifica inclusi utente, esito e punteggio di affidabilità.



L'EDPB ricorda la sua richiesta congiunta con quella del GEPD di **vietare** determinati tipi di **trattamento** in relazione a:

- (1) **identificazione biometrica a distanza di individui in spazi accessibili al pubblico;**
- (2) sistemi di **riconoscimento facciale supportati dall'IA che categorizzano gli individui** in base ai loro dati biometrici in raggruppamenti in base **all'etnia, al genere, nonché all'orientamento politico o sessuale** o ad altri motivi di discriminazione;
- (3) uso del **riconoscimento facciale** o tecnologie simili, per **dedurre le emozioni** di una persona fisica;
- (4) trattamento di dati personali in un contesto di applicazione della legge che farebbe affidamento su una **banca dati popolata** da una raccolta di dati **personali su larga scala** e in modo **indiscriminato**, ad esempio mediante il "**raschiamento**" di fotografie e immagini di volti **accessibili online**.

**Le Linee guida si rivolgono** ai legislatori a livello nazionale e dell'UE, nonché alle LEA e ai loro funzionari nell'attuazione e nell'utilizzo dei sistemi FRT.

**Le persone fisiche** sono considerate dalle linee guida in commento nella misura in cui sono interessate in generale o in quanto interessati in particolare per quanto riguarda i diritti delle stesse.





## PRECISAZIONI E DISTINZIONI

Il semplice rilevamento di volti da parte di telecamere cosiddette "intelligenti" **non costituisce necessariamente un sistema di riconoscimento facciale**. Pur sollevando importanti questioni etiche e di efficacia, tecniche digitali per rilevare comportamenti anormali o eventi violenti, o per riconoscere emozioni facciali o addirittura sagome, essi **non possono essere considerati sistemi biometrici che trattano categorie speciali di dati personali, a condizione che non mirano ad identificare in modo univoco una persona** e che il trattamento dei dati personali coinvolto non include altre categorie particolari di dati personali.

Esempi che non sono, tuttavia, completamente estranei al RTF e sono soggetti alle norme sulla protezione dei dati. Inoltre, tali **sistemi di rilevamento potrebbero essere utilizzati in combinazione con altri sistemi** volti all'identificazione di una persona e quindi essere considerati una tecnologia RTF.

Diversamente dai sistemi di acquisizione ed elaborazione video che, ad es., richiedono l'installazione di dispositivi fisici, **il riconoscimento facciale è una funzionalità software che può essere installata all'interno di sistemi esistenti** (telecamere, database di immagini, ecc.). Tali funzionalità possono quindi essere collegate o interfacciate con una moltitudine di sistemi, e combinate con altre funzionalità. Tale **integrazione in un'infrastruttura già esistente richiede un'attenzione specifica perché comporta rischi intrinseci** dovuti al fatto che la tecnologia RTF potrebbe essere **priva di barriere e facilmente nascosta**.

EDPB: è inoltre importante evidenziare che **l'intervento umano, nella valutazione dei risultati della tecnologia di riconoscimento facciale, potrebbe non fornire necessariamente una garanzia sufficiente** nel rispetto dei diritti delle persone e in particolare del diritto alla protezione dei dati personali, tenuto conto dei possibili pregiudizi e errori che potrebbero derivare dall'elaborazione stessa.

Inoltre, è importante valutare in modo critico i risultati della FRT durante l'intervento umano.



Le LED possano beneficiare dei migliori strumenti per identificare rapidamente gli autori di reati gravi. Tuttavia, **tali strumenti dovrebbero essere utilizzati nel rigoroso rispetto del quadro giuridico applicabile e solo nei casi in cui soddisfino i requisiti di necessità e proporzionalità.**

Le **moderne tecnologie** possano essere parte della soluzione, **non sono affatto un "proiettile d'argento"**.

Vi sono casi d'uso delle tecnologie di RTF che pongono **rischi inaccettabilmente elevati** per gli individui e la società ("**linee rosse**"). Per questi motivi l'EDPB e l'EDPS hanno chiesto il loro divieto generale.

**NB: L'identificazione biometrica remota di individui in spazi accessibili al pubblico pone un alto livello di rischio di intrusione nella vita privata e non trova posto in una società democratica poiché, per sua natura, esso comporta una sorveglianza di massa.**

l'EDPB considera anche **i sistemi di riconoscimento facciale supportati dall'IA** che **categorizzano** gli individui in base alla loro biometria in gruppi in base all'**etnia**, al **genere**, all'**orientamento politico o sessuale**, **non compatibili con la Carta**.

*Studio Legale*

**Tamos & Partners**

avvocatinteam.com

# Approfondimenti

**Avv. Lorenzo Tamos**

Lorenzo.tamos@avvocatinteam.com