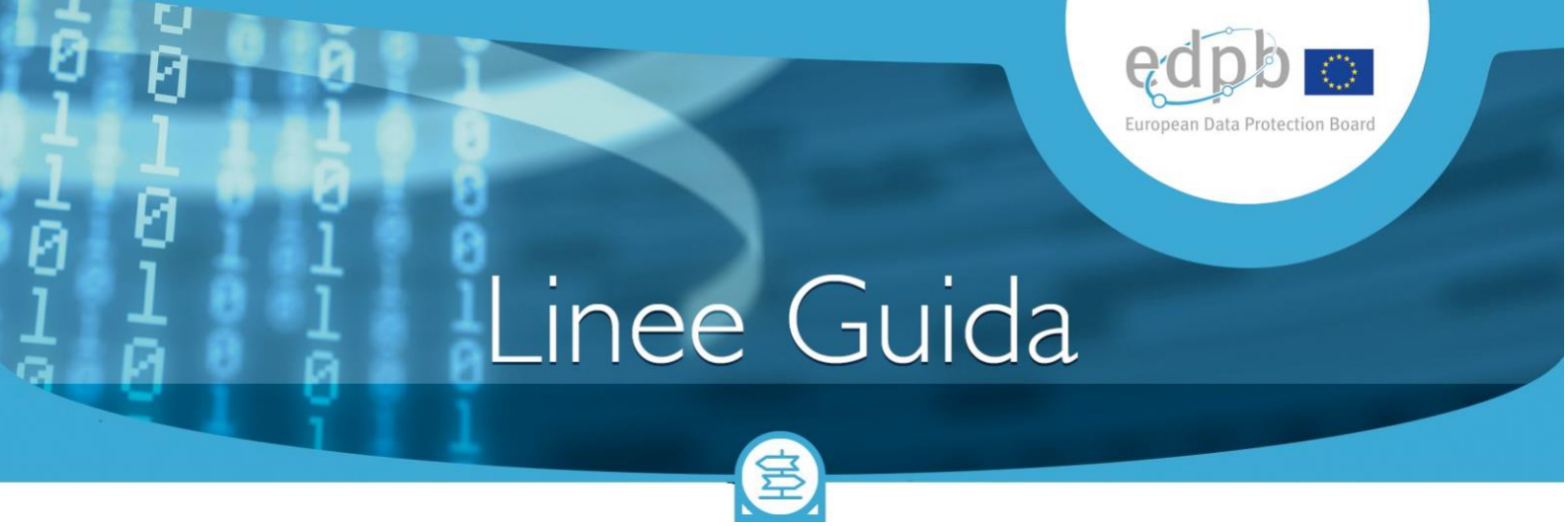

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto

Versione 2.0

Adottate il 26 aprile 2023

Cronologia delle versioni

Versione 1.0	12 maggio 2022	Adozione delle linee guida per consultazione pubblica
Versione 2.0	26 aprile 2023	Adozione delle linee guida dopo la consultazione pubblica

Indice

SINTESI

Un numero sempre maggiore di autorità di contrasto (LEA, *Law Enforcement Authorities*) applica o intende applicare la tecnologia di riconoscimento facciale (FRT, *Facial Recognition Technology*), che può essere utilizzata per **autenticare** o **identificare** una persona e può essere applicata nell'ambito dei video (ad esempio con le telecamere a circuito chiuso) o delle fotografie. Questa tecnologia può servire per varie finalità, tra cui la ricerca di persone nelle liste di controllo della polizia o il monitoraggio degli spostamenti di una persona nello spazio pubblico.

La FRT si basa sul trattamento dei **dati biometrici** e prevede dunque il trattamento di categorie particolari di dati personali. Spesso si avvale di componenti di **intelligenza artificiale** (IA) o di apprendimento automatico (ML). Se da un lato ciò consente di trattare dati su vasta scala, dall'altro comporta anche il rischio di discriminazione e di risultati falsi. La FRT può essere utilizzata in situazioni controllate di tipo 1:1, ma si applica anche a folle enormi e importanti nodi di trasporto.

La tecnologia di riconoscimento facciale è uno **strumento sensibile per le LEA,** che sono autorità esecutive e hanno poteri sovrani. La FRT tende a interferire con i diritti fondamentali (anche al di là del diritto alla protezione dei dati personali) e può incidere sulla nostra stabilità politica sociale e democratica.

Per quanto riguarda la protezione dei dati personali nel contesto delle attività di contrasto, devono essere soddisfatti **i requisiti della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva LED, *Law Enforcement Directive*)**. La direttiva LED prevede un determinato quadro per quanto riguarda l'uso della FRT, in particolare all'articolo 3, punto 13 (espressione «dati biometrici»), all'articolo 4 (principi applicabili al trattamento di dati personali), all'articolo 8 (liceità del trattamento), all'articolo 10 (trattamento di categorie particolari di dati personali) e all'articolo 11 (processo decisionale automatizzato relativo alle persone fisiche).

L'applicazione della FRT può incidere altresì su molti altri diritti fondamentali; pertanto la **Carta dei diritti fondamentali dell'Unione europea** («la Carta») è essenziale per l'interpretazione della direttiva LED, in particolare il diritto alla protezione dei dati di carattere personale di cui all'articolo 8 della Carta, ma anche il diritto al rispetto della vita privata di cui all'articolo 7 della Carta.

Le misure legislative che fungono da base giuridica per il trattamento dei dati personali interferiscono direttamente con i diritti garantiti dagli articoli 7 e 8 della Carta, e in tutte le circostanze il trattamento dei dati biometrici costituisce di per sé una grave ingerenza, indipendentemente dal risultato (per esempio un confronto con esito positivo). Eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà.

Nella sua formulazione, la base giuridica deve essere **sufficientemente chiara** da fornire ai cittadini un'indicazione adeguata in merito alle condizioni e alle circostanze in cui le autorità possono ricorrere a qualsiasi misura di raccolta di dati e di sorveglianza segreta; un mero recepimento nel diritto nazionale della clausola generale di cui all'articolo 10 della direttiva LED difetterebbe di precisione e prevedibilità.

Prima che il legislatore nazionale crei una nuova base giuridica per qualsiasi forma di trattamento dei dati biometrici che si avvalga del riconoscimento facciale, si dovrebbe **consultare** l'autorità di controllo competente per la protezione dei dati.

Le misure legislative devono essere **appropriate** per raggiungere gli obiettivi legittimi perseguiti dalla normativa in questione. Per quanto importante possa essere, un **obiettivo di interesse generale** non giustifica di per sé la limitazione di un diritto fondamentale. Le misure legislative dovrebbero **distinguere** le persone interessate e rivolgersi a loro in funzione dell'obiettivo, per esempio la lotta contro specifiche forme gravi di criminalità. Se la misura interessa in generale tutti, senza alcuna distinzione, limitazione o eccezione di questo tipo, essa intensifica l'ingerenza, anche nel caso in cui il trattamento dei dati riguardi una parte considerevole della popolazione.

I dati devono essere trattati in modo da garantire l'applicabilità e l'efficacia delle norme e dei principi di protezione dei dati dell'UE. In base a ogni situazione, la **valutazione della necessità e della proporzionalità** deve inoltre individuare e considerare tutte le possibili implicazioni per altri diritti fondamentali. Se i dati vengono trattati sistematicamente all'insaputa degli interessati, è probabile che si generi un **senso generale di sorveglianza costante**, che può comportare effetti inibitori per quanto concerne alcuni o tutti i diritti fondamentali interessati, come la dignità umana ai sensi dell'articolo 1 della Carta, la libertà di pensiero, di coscienza e di religione ai sensi dell'articolo 10 della Carta, la libertà di espressione ai sensi dell'articolo 11 della Carta e la libertà di riunione e di associazione ai sensi dell'articolo 12 della Carta.

Il trattamento di categorie particolari di dati, quali ad esempio i dati biometrici, si può considerare «**strettamente necessario**» (articolo 10 della direttiva LED) solo se l'ingerenza nella protezione dei dati personali e le sue limitazioni non eccedono la misura assolutamente necessaria, ossia indispensabile, escludendo qualsiasi trattamento di carattere generale o sistematico.

Il fatto che una fotografia sia stata **resa manifestamente pubblica** dall'interessato (articolo 10 della direttiva LED) non implica che i relativi dati biometrici, ricavabili dalla fotografia con mezzi tecnici specifici, si considerino resi manifestamente pubblici. Le impostazioni predefinite di un servizio (per esempio la messa a disposizione del pubblico di modelli o l'assenza di scelta, come quando i modelli vengono resi pubblici senza che l'utente possa modificare tale impostazione) non dovrebbero in alcun modo essere interpretate come dati resi manifestamente pubblici.

L'articolo 11 della direttiva LED istituisce un quadro per **il processo decisionale automatizzato relativo alle persone fisiche**. Il ricorso alla FRT comporta l'utilizzo di categorie particolari di dati e può comportare la profilazione, a seconda del modo e della finalità per cui la FRT viene applicata. In ogni caso, ai sensi del diritto dell'Unione e dell'articolo 11, paragrafo 3, della direttiva LED, la profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali è vietata.

L'articolo 6 della direttiva LED riguarda la necessità di **distinguere tra diverse categorie di interessati**. Riguardo alle persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o remoto, con l'obiettivo legittimo ai sensi della direttiva LED, è assai probabile che non si possa giustificare un'ingerenza.

Inoltre, in base al **principio di minimizzazione dei dati** [articolo 4, paragrafo 1, lettera e), della direttiva LED], qualsiasi materiale video non pertinente per la finalità del trattamento dovrebbe essere sempre cancellato o anonimizzato (per esempio offuscando l'immagine senza alcuna possibilità retroattiva di recuperare i dati) prima dell'utilizzo.

Il titolare del trattamento deve valutare attentamente come (o se possa) rispettare i requisiti relativi ai **diritti dell'interessato** prima di avviare un trattamento basato sulla FRT, dal momento che spesso quest'ultima comporta il trattamento di categorie particolari di dati personali senza alcuna interazione apparente con l'interessato.

L'effettivo esercizio dei diritti dell'interessato dipende dall'adempimento, da parte del titolare del trattamento, dei propri **obblighi di informazione** (articolo 13 della direttiva LED). Nel valutare l'esistenza di un «caso specifico» ai sensi dell'articolo 13, paragrafo 2, della direttiva LED, occorre prendere in considerazione diversi fattori, tra cui l'eventualità che i dati personali siano raccolti all'insaputa dell'interessato, poiché tenerne conto sarebbe l'unico modo per consentire agli interessati di esercitare i loro diritti in modo efficace. Se il processo decisionale deve svolgersi esclusivamente sulla base della FRT, gli interessati devono essere informati riguardo alle caratteristiche del processo decisionale automatizzato.

Per quanto riguarda le **richieste di accesso**, quando i dati biometrici sono memorizzati e collegati a un'identità anche tramite dati alfanumerici, in linea con il principio della minimizzazione dei dati, ciò dovrebbe consentire all'autorità competente di confermare una richiesta di accesso basata su una ricerca tramite tali dati alfanumerici e senza avviare alcun ulteriore trattamento di dati biometrici altrui (ossia effettuando una ricerca con la FRT in una banca dati).

I rischi per gli interessati sono particolarmente gravi se in una banca dati della polizia sono conservati dati inesatti e/o questi ultimi vengono condivisi con altre entità. Il titolare del trattamento deve **correggere** i dati conservati e i sistemi FRT di conseguenza (cfr. anche considerando 47 della direttiva LED).

Il diritto alla **limitazione** di trattamento diventa particolarmente importante quando si ha che fare con la tecnologia di riconoscimento facciale (che, basandosi su uno o più algoritmi, non mostra mai un risultato definitivo) in situazioni in cui vengono acquisite grandi quantità di dati e l'accuratezza e la qualità dell'identificazione possono variare.

Una **valutazione d'impatto sulla protezione dei dati (DPIA)** prima di ricorrere alla FRT rappresenta un requisito obbligatorio (cfr. articolo 27 della direttiva LED). L'EDPB raccomanda di rendere pubblici i risultati di tali valutazioni, o almeno le principali risultanze e conclusioni della DPIA, come misura per rafforzare la fiducia e la trasparenza.

La maggior parte dei casi di diffusione e utilizzo della FRT comporta un rischio intrinseco elevato per i diritti e le libertà degli interessati. Pertanto, l'autorità che si avvale della FRT dovrebbe **consultare** l'autorità di controllo competente prima di implementare il sistema.

Data la natura univoca dei dati biometrici, l'autorità che attua e/o utilizza la FRT deve prestare particolare attenzione alla **sicurezza del trattamento**, in linea con l'articolo 29 della direttiva LED; in particolare, l'autorità di contrasto dovrebbe garantire che il sistema sia conforme alle norme pertinenti e attuare misure di protezione dei modelli biometrici. I principi e le garanzie in materia di protezione dei dati devono essere integrati nella tecnologia prima dell'avvio del trattamento dei dati personali. Pertanto, anche quando un'autorità di contrasto intende applicare e impiegare la FRT offerta da fornitori esterni, essa deve garantire (ad esempio mediante la procedura di appalto) che siano utilizzate solo tecnologie di riconoscimento facciale basate sui principi della **protezione dei dati fin dalla progettazione e per impostazione predefinita**.

La registrazione (cfr. articolo 25 della direttiva LED) è una garanzia importante per la verifica della liceità del trattamento, sia a livello interno (ossia l'autocontrollo da parte del titolare/responsabile del trattamento interessato) che da parte delle autorità di controllo esterne. Nel contesto dei sistemi di riconoscimento facciale, si raccomanda la registrazione anche per le modifiche della banca dati di riferimento e i tentativi di identificazione o verifica, ivi compreso per quanto riguarda l'utente, l'esito e il punteggio di confidenza. La registrazione, tuttavia, è solo uno degli elementi essenziali del **principio generale di responsabilità** (cfr. articolo 4, paragrafo 4, della direttiva LED). Il titolare del trattamento

deve essere in grado di comprovare la conformità del trattamento ai principi fondamentali di protezione dei dati di cui all'articolo 4, paragrafi da 1 a 3, della direttiva LED.

L'EDPB ricorda la **richiesta** congiunta, da parte sua e del GEPD, **di vietare** determinati tipi di trattamento in relazione 1) all'identificazione biometrica remota delle persone in spazi accessibili al pubblico, 2) ai sistemi di riconoscimento facciale basati sull'IA che classificano le persone, in funzione dei loro dati biometrici, in gruppi secondo l'etnia, il genere, l'orientamento politico o sessuale o altri motivi di discriminazione, 3) all'uso del riconoscimento facciale o di tecnologie analoghe per dedurre le emozioni di una persona fisica e 4) al trattamento dei dati personali in un contesto di applicazione della legge che si baserebbe su una banca dati popolata tramite la raccolta di dati personali su vasta scala e in modo indiscriminato, ad esempio attraverso lo «scraping» (l'estrazione dai siti web) di fotografie e immagini facciali accessibili online.

Una garanzia essenziale per i diritti fondamentali in gioco è costituita dalla **supervisione efficace** da parte delle autorità di controllo competenti per la protezione dei dati. Pertanto, gli Stati membri devono assicurare che le risorse delle autorità di controllo siano adeguate e sufficienti per consentire loro di svolgere il proprio mandato.

Le presenti **linee guida sono rivolte** ai legislatori a livello nazionale e dell'UE, nonché alle autorità di contrasto e ai rispettivi funzionari che attuano e utilizzano i sistemi FRT; sono altresì rivolte alle persone nella misura in cui le riguardano in generale o in qualità di interessati, in particolare per quanto riguarda i diritti degli interessati.

Le **linee guida intendono** fornire informazioni in merito a determinate caratteristiche della FRT e al quadro giuridico applicabile nel contesto dell'applicazione della legge (in particolare della direttiva LED).

- Inoltre offrono uno **strumento per agevolare una prima classificazione della sensibilità di un determinato caso d'uso** (allegato I).
- Contengono inoltre **orientamenti pratici per le autorità di contrasto che intendono acquistare e gestire un sistema FRT** (allegato II).
- Le linee guida descrivono inoltre vari **casi d'uso tipici ed elencano numerose considerazioni pertinenti**, specialmente per quanto riguarda la verifica della necessità e della proporzionalità (allegato III).

1 INTRODUZIONE

1. Si può ricorrere alla tecnologia di riconoscimento facciale (FRT) per riconoscere automaticamente le persone in base al loro volto; spesso la FRT si basa sull'intelligenza artificiale, come le tecnologie di apprendimento automatico. Le sue applicazioni vengono sperimentate e impiegate con frequenza sempre maggiore in vari settori, dall'utilizzo individuale fino al suo ricorso nelle organizzazioni private e nella pubblica amministrazione. Anche le autorità di contrasto contano di avvalersi vantaggiosamente della FRT, che promette soluzioni per risolvere problemi relativamente nuovi, come le indagini che coinvolgono una grande quantità di prove acquisite, ma anche problemi noti, in particolare per quanto riguarda la carenza di personale addetto ai compiti di osservazione e ricerca.

2. Una gran parte del crescente interesse per la FRT si deve alla sua efficienza e scalabilità, cui tuttavia si accompagnano gli svantaggi inerenti alla tecnologia e alla sua applicazione (anche su vasta scala). Benché si possano analizzare migliaia di insiemi di dati personali premendo semplicemente un

pulsante, gli effetti anche lievi della discriminazione algoritmica o dell'errata identificazione sono sufficienti per causare gravi danni alla condotta e alla vita quotidiana di un gran numero di persone. L'entità del trattamento dei dati personali, e in particolare dei dati biometrici, è di per sé un ulteriore elemento chiave della FRT, poiché il trattamento dei dati personali costituisce un'ingerenza nel diritto fondamentale alla protezione dei dati di carattere personale ai sensi dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (la Carta).

3. L'applicazione della FRT da parte delle autorità di contrasto produrrà (e in una certa misura già produce) ripercussioni significative su singoli individui e gruppi di persone, minoranze comprese. Tali ripercussioni avranno anche effetti considerevoli sul nostro modo di vivere insieme e sulla nostra stabilità politica sociale e democratica, valorizzando la grande rilevanza del pluralismo e dell'opposizione politica. Il diritto alla protezione dei dati personali è spesso un prerequisito chiave per garantire altri diritti fondamentali. L'applicazione della FRT tende sensibilmente a interferire con i diritti fondamentali, oltre che con il diritto alla protezione dei dati personali.

4. L'EDPB ritiene perciò importante contribuire all'integrazione in corso della FRT nel settore delle attività di contrasto, disciplinate rispettivamente dalla direttiva sulla protezione dei dati ([1]) nelle attività di polizia e giudiziarie e dalle leggi nazionali che la recepiscono, e fornire le presenti linee guida, che sono intese a offrire informazioni pertinenti ai legislatori a livello nazionale e dell'UE, nonché alle autorità di contrasto e ai rispettivi funzionari in fase di attuazione e utilizzo dei sistemi FRT. L'ambito di applicazione delle linee guida si limita alla tecnologia di riconoscimento facciale; tuttavia, altre forme di trattamento dei dati personali basate su dati biometrici e impiegate dalle autorità di contrasto, specialmente in caso di trattamento a distanza, possono comportare rischi analoghi o aggiuntivi per le persone, i gruppi e la società. In base alle rispettive circostanze, alcuni aspetti di queste linee guida possono costituire una fonte utile anche in questi casi. Infine, anche le persone che esse riguardano in generale o in qualità di interessati possono trovare informazioni importanti, in particolare per quanto riguarda i diritti degli interessati.

5. Le linee guida sono costituite dal documento principale e da tre allegati: il documento principale in questione presenta la tecnologia e il quadro giuridico applicabile; l'allegato I contiene un modello per aiutare a individuare alcuni degli aspetti principali per classificare la gravità dell'interferenza con i diritti fondamentali in un determinato settore di applicazione; nell'allegato II le autorità di contrasto che intendono acquisire e gestire un sistema FRT possono trovare orientamenti pratici. A seconda dell'ambito di applicazione della tecnologia di riconoscimento facciale, potrebbero essere opportune considerazioni diverse; l'allegato III presenta una serie di scenari ipotetici e considerazioni pertinenti.

2 TECNOLOGIA

2.1 Una tecnologia biometrica, due funzioni distinte

6. Il riconoscimento facciale è una tecnologia probabilistica che può riconoscere automaticamente le persone in base al loro volto al fine di autenticarle o identificarle.

7. La FRT rientra nella categoria più ampia della tecnologia biometrica. La biometria comprende tutti i processi automatizzati impiegati per riconoscere una persona attraverso la quantificazione di caratteristiche fisiche, fisiologiche o comportamentali (impronte digitali, struttura dell'iride, voce,

([1]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

andatura, modelli dei vasi sanguigni, ecc.) Tali caratteristiche sono definite come «dati biometrici» perché consentono o confermano l'identificazione univoca della persona in questione.

8. È il caso dei volti delle persone o, più specificamente, del loro trattamento tecnico effettuato mediante dispositivi di riconoscimento facciale: prendendo l'immagine di un volto (una fotografia o un video), detto «campione» biometrico, è possibile estrarre una rappresentazione digitale (che è detta «modello») delle caratteristiche distinte di quel volto.

9. Un modello biometrico è una rappresentazione digitale delle caratteristiche uniche estratte da un campione biometrico che possono essere memorizzate in una banca dati biometrica ([2]). Questo modello dovrebbe essere unico e specifico per ogni persona e, in linea di principio, è immutabile nel tempo ([3]). Nella fase di riconoscimento, il dispositivo confronta questo modello con altri precedentemente realizzati o calcolati direttamente a partire da campioni biometrici come i volti presenti in un'immagine, una foto o un video. Il «riconoscimento facciale» è dunque un processo strutturato in due fasi: l'acquisizione dell'immagine del volto e la sua trasformazione in un modello, seguita dal riconoscimento del volto in questione confrontando il modello corrispondente con uno o più altri modelli.

10. Come qualsiasi processo biometrico, il riconoscimento facciale può svolgere due funzioni distinte:

    - l'**autenticazione** di una persona, al fine di verificare che quest'ultima sia chi afferma di essere. In questo caso il sistema confronterà un modello o un campione biometrico preregistrato (memorizzato per esempio su una carta intelligente o su un passaporto biometrico) con un singolo volto, ad esempio quello di una persona che si presenta a un punto di controllo, per verificare se si tratti della stessa persona. Questa funzionalità si basa pertanto sul confronto di due modelli ed è anche detta **verifica** 1:1;

    - l'**identificazione** di una persona, al fine di trovarla in mezzo a un gruppo di persone, all'interno di una zona specifica, di un'immagine o di una banca dati. In questo caso, il sistema deve elaborare ogni volto acquisito per generare un modello biometrico e poi verificare se corrisponda o meno a una persona nota al sistema. Questa funzionalità si basa quindi sul confronto di un modello con una banca dati di modelli o campioni (riferimento); è detta anche identificazione 1:molti e, per esempio, può collegare a un volto un codice di prenotazione (cognome, nome) se si effettua il confronto con una banca dati di fotografie associate a nomi e cognomi, oppure comportare la possibilità di seguire una persona in mezzo a una folla, senza necessariamente creare il collegamento con l'identità civile della persona.

11. In entrambi i casi, le tecniche di riconoscimento facciale impiegate si basano su una corrispondenza stimata tra modelli: quello confrontato e quello/i di riferimento. Da questo punto di vista, si tratta di tecniche probabilistiche: dal confronto emerge una probabilità maggiore o minore che la persona sia effettivamente quella da autenticare o identificare; se questa probabilità supera un determinato valore soglia nel sistema, definito dal suo sviluppatore o dall'utente, il sistema presupporrà che vi sia una corrispondenza.

12. Benché ambedue le funzioni (autenticazione e identificazione) siano distinte, entrambe hanno a che fare con il trattamento di dati biometrici relativi a una persona fisica identificata o identificabile e

([2]) Linee guida sul riconoscimento facciale, Comitato consultivo della Convenzione 108, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, Consiglio d'Europa, giugno 2021.
([3]) Ciò potrebbe dipendere dal tipo di biometria e dall'età dell'interessato.

costituiscono dunque un trattamento di dati personali e, nello specifico, un trattamento di categorie particolari di dati personali.

13. Il riconoscimento facciale fa parte di uno spettro più ampio di tecniche di trattamento delle immagini video. Alcune videocamere possono filmare le persone all'interno di una zona definita, in particolare i loro volti, ma non possono essere utilizzate come tali per riconoscere automaticamente le persone. Lo stesso vale per una semplice foto: una telecamera non è un sistema di riconoscimento facciale perché le fotografie delle persone devono essere trattate in modo specifico per estrarre i dati biometrici.

14. Anche il mero rilevamento di volti da parte delle cosiddette telecamere «intelligenti» non costituisce necessariamente un sistema di riconoscimento facciale. Pur sollevando importanti questioni in termini di etica ed efficacia, le tecniche digitali per rilevare comportamenti anomali o episodi di violenza (oppure riconoscere emozioni facciali o addirittura sagome) non possono essere considerate sistemi biometrici che trattano categorie particolari di dati personali, a condizione che non siano intese a identificare in modo univoco una persona e che il trattamento dei dati personali in questione non comprenda altre categorie particolari di dati personali. Questi esempi non sono del tutto slegati dal riconoscimento facciale e sono ancora soggetti alle norme in materia di protezione dei dati personali ([4]). Inoltre, questo tipo di sistema di rilevamento può essere impiegato in combinazione con altri sistemi volti a identificare una persona e può quindi essere considerato una tecnologia di riconoscimento facciale.

15. A differenza dei sistemi di acquisizione ed elaborazione video, per esempio, che richiedono l'installazione di dispositivi fisici, il riconoscimento facciale è una funzionalità software che può essere implementata nell'ambito di sistemi preesistenti (telecamere, banche dati di immagini, ecc.) e pertanto si può collegare o interfacciare con una molteplicità di sistemi e combinare con altre funzionalità. Tale integrazione in un'infrastruttura già esistente richiede un'attenzione specifica perché comporta rischi intrinseci causati dalla possibilità che la tecnologia di riconoscimento facciale sia comoda e facilmente occultabile ([5]).

2.2 Un'ampia varietà di finalità e applicazioni

16. Oltre all'ambito di applicazione delle presenti linee guida e al di fuori di quello della direttiva LED, il riconoscimento facciale si può impiegare per un'ampia gamma di obiettivi, sia per uso commerciale che per affrontare problemi di sicurezza pubblica o di applicazione della legge. Vi si può ricorrere in molti contesti diversi: nel rapporto personale tra un utente e un servizio (accesso a un'applicazione), per l'accesso a un luogo specifico (filtraggio fisico) o senza particolari limitazioni nello spazio pubblico (riconoscimento facciale in diretta). Si può applicare nei confronti di qualsiasi tipo di interessato: un cliente di un servizio, un dipendente, un semplice spettatore, una persona ricercata o coinvolta in procedimenti giudiziari o amministrativi, ecc. Alcuni utilizzi sono già comuni e diffusi mentre altri, al momento, sono in fase sperimentale o esplorativa. Anche se le presenti linee guida non riguardano tutti gli usi e le applicazioni di questo tipo, l'EDPB ricorda che si possono attuare solo se sono conformi al quadro giuridico applicabile, e in particolare al RGPD e alle leggi nazionali pertinenti ([6]). Anche nel contesto della direttiva LED, oltre alle funzioni di autenticazione o identificazione, i dati trattati

([4]) Tuttavia, l'articolo 10 della direttiva LED (o l'articolo 9 del RGPD) si applica ai sistemi utilizzati per classificare le persone, in base ai loro dati biometrici, in gruppi in cluster secondo l'etnia, nonché secondo l'orientamento politico o sessuale o altre categorie particolari di dati personali.
([5]) Per esempio nelle videocamere indossabili, utilizzate sempre più spesso nella pratica.
([6]) Per ulteriori orientamenti, cfr. anche le Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020.

ricorrendo alla tecnologia di riconoscimento facciale si possono trattare ulteriormente anche per altre finalità, come la categorizzazione.

17. Nello specifico, si potrebbe prendere in considerazione una gamma di potenziali utilizzi a seconda del grado di controllo esercitato dalle persone sui propri dati personali, dei mezzi efficaci di cui dispongono per esercitarlo e del loro diritto di iniziativa per attivare e impiegare tale tecnologia, delle conseguenze per loro (in caso di riconoscimento o di mancato riconoscimento) e dell'entità del trattamento effettuato. Il riconoscimento facciale basato su un modello memorizzato su un dispositivo personale (carta intelligente, smartphone, ecc.) che appartiene alla persona, utilizzato a fini di autenticazione e per scopi strettamente personali attraverso un'interfaccia dedicata, non comporta gli stessi rischi, per esempio, dell'uso a fini di identificazione in un ambiente non controllato, senza il coinvolgimento attivo degli interessati, in cui il modello di ogni volto che entra nell'area di monitoraggio viene confrontato con i modelli di un'ampia sezione trasversale della popolazione, memorizzati in una banca dati. Tra questi due estremi esiste una gamma molto variegata di utilizzi e problemi associati che riguardano la protezione dei dati personali.

18. Per illustrare ulteriormente il contesto in cui le tecnologie di riconoscimento facciale vengono attualmente dibattute o attuate, a fini sia di autenticazione che di identificazione, l'EDPB ritiene pertinente citare una serie di esempi. Quelli che seguono sono puramente descrittivi e non dovrebbero essere considerati in alcun modo una valutazione preliminare della loro conformità all'acquis dell'UE nel settore della protezione dei dati.

Esempi di autenticazione tramite riconoscimento facciale

19. L'autenticazione può essere progettata in modo tale che gli utenti ne abbiano il pieno controllo, ad esempio per consentire l'accesso a servizi o applicazioni esclusivamente in un contesto domestico. In quanto tale, è ampiamente utilizzata dai proprietari di smartphone per sbloccare il loro dispositivo, al posto dell'autenticazione tramite password.

20. L'autenticazione tramite riconoscimento facciale può servire anche per verificare l'identità di una persona che intende beneficiare di servizi pubblici o privati di terzi. Tali processi offrono quindi la possibilità di creare un'identità digitale utilizzando un'app mobile (smartphone, tablet, ecc.) che si può poi impiegare per accedere a servizi amministrativi online.

21. Inoltre, l'autenticazione tramite riconoscimento facciale può essere finalizzata a controllare l'accesso fisico a uno o più luoghi predeterminati, come gli ingressi agli edifici o specifici punti di attraversamento. Questa funzionalità è attuata, per esempio, nell'ambito di determinati trattamenti ai fini dell'attraversamento di frontiera, in cui il volto della persona presso il dispositivo del punto di controllo viene confrontato con quello memorizzato nel suo documento d'identità (passaporto o permesso di soggiorno sicuro).

Esempi di identificazione tramite riconoscimento facciale

22. L'identificazione può essere applicata in molti modi, ancor più diversificati. Essi includono in particolare, ma non solo, gli utilizzi elencati di seguito, attualmente osservati, sperimentati o programmati nell'UE:

- ricerca, in una banca dati di fotografie, dell'identità di una persona non identificata (vittima, persona sospettata, ecc.);
- monitoraggio degli spostamenti di una persona nello spazio pubblico. Il suo volto viene confrontato con i modelli biometrici di persone che viaggiano o hanno viaggiato nella zona

monitorata, ad esempio quando un bagaglio viene dimenticato o dopo che è stato commesso un reato;

- ricostruzione del viaggio di una persona e delle sue successive interazioni con altre persone, mediante un confronto differito degli stessi elementi nell'intento di identificare, ad esempio, i suoi contatti;
- identificazione biometrica remota di persone ricercate negli spazi pubblici. Tutti i volti ripresi in diretta dalle videocamere di protezione sono sottoposti a un controllo incrociato, in tempo reale, con una banca dati in possesso delle forze di sicurezza;
- riconoscimento automatico delle persone in un'immagine per individuare, ad esempio, le loro relazioni su un social network che la utilizza. L'immagine viene confrontata con i modelli di tutti coloro che, in rete, hanno espresso il loro consenso all'uso di questa funzionalità, al fine di proporre l'identificazione nominativa di tali relazioni;
- accesso ai servizi, con alcuni bancomat che riconoscono i propri clienti confrontando il volto ripreso da una telecamera con la banca dati delle immagini facciali in possesso della banca;
- tracciamento del viaggio di un passeggero in una determinata fase del tragitto. Il modello, calcolato in tempo reale, di ogni persona che effettua il check-in ai gate previsti in determinate fasi del viaggio (punti di deposito bagagli, gate di imbarco, ecc.), viene confrontato con i modelli delle persone precedentemente registrate nel sistema.

23. Oltre all'uso della FRT nel settore delle attività di contrasto, l'ampia gamma di utilizzi osservati richiede certamente un dibattito e un approccio strategico globale al fine di garantire la coerenza e la conformità all'acquis dell'UE nel campo della protezione dei dati.

2.3 Affidabilità, accuratezza e rischi per gli interessati

24. Come ogni tecnologia, anche il riconoscimento facciale può incontrare difficoltà dal punto di vista dell'attuazione, in particolare per quanto riguarda la sua affidabilità ed efficienza in termini di autenticazione o identificazione, oltre alla questione generale della qualità e dell'accuratezza dei dati della «fonte» e dell'esito del trattamento con la tecnologia di riconoscimento facciale.

25. Tali difficoltà tecnologiche comportano rischi particolari per gli interessati, rischi che sono ancora più significativi o gravi nel settore delle attività di contrasto, considerando i possibili effetti di carattere giuridico per gli interessati o gli effetti di altro tipo che li riguardano in modo significativo. In tale contesto, sembra utile sottolineare che l'uso ex post della FRT non è di per sé più sicuro, poiché le persone possono essere tracciate nel tempo e nei luoghi; pertanto l'uso ex post comporta anche rischi specifici che occorre valutare caso per caso ([7]).

26. Come ha sottolineato l'Agenzia dell'Unione europea per i diritti fondamentali nella sua relazione del 2019, «determinare il livello necessario di accuratezza del software di riconoscimento facciale è impegnativo: esistono molti modi diversi per valutare e stimare l'accuratezza anche a seconda del compito, della finalità e del contesto del suo utilizzo. Quando si applica la tecnologia in luoghi frequentati da milioni di persone, come stazioni ferroviarie o aeroporti, una percentuale relativamente esigua di errori (ad esempio lo 0,01%) ([8]) implica comunque che centinaia di persone vengano segnalate erroneamente. Inoltre, per alcune categorie di persone possono esservi maggiori possibilità

([7]) Cfr. gli esempi riportati nell'allegato III.
([8]) Questo tasso di accuratezza è tratto dalla relazione citata e riflette un tasso di gran lunga migliore rispetto alle prestazioni attuali degli algoritmi adottati nelle applicazioni della FRT.

di un falso abbinamento rispetto ad altre, come descritto nella sezione 3. Dal momento che esistono diversi modi per calcolare e interpretare i tassi di errore, la cautela è necessaria. Inoltre, per quanto riguarda l'accuratezza e gli errori, gli aspetti relativi alla facilità con cui un sistema può essere ingannato, per esempio con immagini facciali false (il cosiddetto "spoofing"), sono rilevanti soprattutto a fini di contrasto» ([9]).

27. In tale contesto, l'EDPB ritiene importante ricordare che la tecnologia di riconoscimento facciale, indipendentemente dal fatto che venga impiegata a fini di autenticazione o di identificazione, non fornisce un risultato definitivo, ma si basa sulla probabilità che due volti, o immagini di volti, corrispondano alla stessa persona ([10]). Questo risultato peggiora ulteriormente quando è bassa la qualità dei campioni biometrici acquisiti per il riconoscimento facciale. La scarsa nitidezza delle immagini in ingresso, la bassa risoluzione della fotocamera, il movimento e la scarsa illuminazione possono concorrere a ridurre la qualità. Altri aspetti che incidono sensibilmente sui risultati sono la diffusione e lo *spoofing*, ad esempio quando i criminali cercano di evitare di passare davanti alle telecamere o di ingannare la FRT. Numerosi studi hanno inoltre evidenziato che questi risultati statistici derivanti dal trattamento algoritmico possono anche essere soggetti a distorsioni, in particolare a causa della qualità dei dati della fonte, nonché delle banche dati di formazione o di altri fattori, come la scelta della sede di attuazione. Occorre inoltre sottolineare l'impatto della tecnologia di riconoscimento facciale su altri diritti fondamentali, quali il rispetto della vita privata e familiare, la libertà di espressione e di informazione, la libertà di riunione e di associazione, ecc.

28. È dunque essenziale prendere in considerazione l'affidabilità e l'accuratezza della tecnologia di riconoscimento facciale in quanto criteri per valutare la conformità ai principi fondamentali di protezione dei dati, ai sensi dell'articolo 4 della direttiva LED, e in particolare per quanto riguarda la correttezza e l'accuratezza.

29. Pur evidenziando che la qualità elevata dei dati è fondamentale per algoritmi di alto livello, l'EDPB sottolinea altresì che i titolari del trattamento, nell'ambito del loro obbligo di responsabilità, devono effettuare una valutazione periodica e sistematica del trattamento algoritmico al fine di garantire, in particolare, l'accuratezza, la correttezza e l'affidabilità dei risultati di tale trattamento dei dati personali. Quelli utilizzati ai fini della valutazione, della formazione e dell'ulteriore sviluppo dei sistemi di FRT si possono trattare solo in funzione di una base giuridica sufficiente e conformemente ai principi comuni in materia di protezione dei dati.

3 QUADRO GIURIDICO APPLICABILE

30. Il ricorso alle tecnologie di riconoscimento facciale è intrinsecamente legato al trattamento dei dati personali, comprese categorie particolari di dati, oltre a incidere direttamente o indirettamente su alcuni diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea. Ciò è particolarmente pertinente nel settore delle attività di contrasto e della giustizia penale. Pertanto, qualsiasi ricorso alle tecnologie di riconoscimento facciale dovrebbe svolgersi nel rigoroso rispetto del quadro giuridico applicabile.

31. Le informazioni seguenti sono destinate all'utilizzo per valutare misure legislative e amministrative future, nonché per attuare la normativa vigente in ogni singolo caso in cui sia coinvolta la FRT. La

([9]) Facial recognition technology: fundamental rights considerations in the context of law enforcement [Tecnologia di riconoscimento facciale: considerazioni sui diritti fondamentali nell'ambito delle attività di polizia e giudiziarie], Agenzia dell'Unione europea per i diritti fondamentali, 21 novembre 2019.
([10]) Questa probabilità è detta «punteggio di confidenza».

pertinenza dei rispettivi requisiti varia a seconda delle circostanze specifiche; non essendo possibile prevedere tutte le circostanze future, si ritiene che tali informazioni servano solo a fornire assistenza e non debbano essere interpretate come un elenco esaustivo.

3.1 Quadro giuridico generale – La Carta dei diritti fondamentali dell'Unione europea e la Convenzione europea dei diritti dell'uomo (CEDU)

3.1.1 Applicabilità della Carta

32. La Carta dei diritti fondamentali dell'Unione europea (in prosieguo «la Carta») si rivolge alle istituzioni, agli organi e agli organismi dell'Unione e agli Stati membri nell'attuazione del diritto dell'Unione.

33. La disciplina del trattamento dei dati biometrici a fini di contrasto ai sensi dell'articolo 1, paragrafo 1, della direttiva LED solleva inevitabilmente la questione del rispetto dei diritti fondamentali, in particolare il rispetto della vita privata e delle comunicazioni ai sensi dell'articolo 7 della Carta e il diritto alla protezione dei dati di carattere personale ai sensi dell'articolo 8 della Carta.

34. L'acquisizione e l'analisi dei filmati di persone fisiche, ivi compresi i loro volti, implica il trattamento di dati personali. Quando viene effettuato, il trattamento tecnico dell'immagine si estende anche ai dati biometrici. Il trattamento tecnico dei dati afferenti al volto di una persona fisica in relazione al tempo e al luogo consente di trarre conclusioni sulla vita privata delle persone interessate, che possono riguardare l'origine razziale o etnica, la salute, la religione, le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali che frequentano. L'ampia gamma di informazioni che possono essere rivelate attraverso l'applicazione della FRT mostra chiaramente il possibile impatto sul diritto alla protezione dei dati personali di cui all'articolo 8 della Carta, ma anche sul diritto al rispetto della vita privata di cui all'articolo 7 della Carta.

35. In tali circostanze, inoltre, non è inconcepibile che la raccolta, l'analisi e l'ulteriore elaborazione dei dati biometrici (facciali) in questione possano incidere sul modo in cui le persone si sentono libere di agire, anche se il loro agire sarebbe pienamente conforme a una società libera e aperta. Ciò potrebbe avere altresì gravi ripercussioni sull'esercizio dei loro diritti fondamentali, come il diritto alla libertà di pensiero, di coscienza e di religione, di espressione, di riunione pacifica e alla libertà di associazione ai sensi degli articoli 1, 10, 11 e 12 della Carta. Un trattamento di questo tipo comporta anche altri rischi, come quello di abuso delle informazioni personali raccolte dalle autorità competenti in seguito all'accesso e all'uso illeciti dei dati personali, alla violazione della sicurezza, ecc. I rischi dipendono spesso dal trattamento e dalle circostanze in cui avviene, come ad esempio il rischio di accesso e utilizzo illeciti per mano di agenti di polizia o di altre parti non autorizzate. Tuttavia, alcuni rischi sono semplicemente intrinseci alla natura univoca dei dati biometrici; a differenza di un indirizzo o di un numero di telefono, è impossibile che un interessato modifichi le proprie caratteristiche uniche, come il volto o l'iride. In caso di accesso non autorizzato o di pubblicazione accidentale di dati biometrici, il loro utilizzo come password o chiavi crittografiche sarebbe compromesso o i suddetti dati potrebbero essere impiegati per ulteriori attività di sorveglianza non autorizzata a danno dell'interessato.

3.1.2 Ingerenza nei diritti sanciti dalla Carta

36. In tutte le circostanze il trattamento dei dati biometrici costituisce di per sé una grave ingerenza indipendentemente dal risultato (per esempio un confronto con esito positivo). Il trattamento costituisce un'ingerenza anche se il modello biometrico viene immediatamente cancellato una volta che il confronto con una banca dati della polizia non abbia dato luogo a un riscontro positivo.

37. L'ingerenza nei diritti fondamentali degli interessati può derivare da un testo legislativo che ha la finalità o l'effetto di limitare il rispettivo diritto fondamentale ([11]), nonché dall'atto di un'autorità pubblica con la stessa finalità o gli stessi effetti, oppure anche di un'entità privata incaricata per legge di esercitare l'autorità pubblica e i poteri pubblici.

38. Una misura legislativa che funga da base giuridica per il trattamento dei dati personali interferisce direttamente con i diritti garantiti dagli articoli 7 e 8 della Carta ([12]).

39. In molti casi l'utilizzo dei dati biometrici e della FRT in particolare incide anche sul diritto alla dignità umana, garantito dall'articolo 1 della Carta. La dignità umana richiede che gli individui non siano trattati come semplici oggetti. La FRT calcola caratteristiche esistenziali ed estremamente personali (i tratti del viso) tramite lettura elettronica, al fine di utilizzarle come una targa umana o una carta d'identità, oggettivando così il volto.

40. Questo tipo di trattamento può anche interferire con altri diritti fondamentali, come quelli di cui agli articoli 10, 11 e 12 della Carta, nella misura in cui gli effetti inibitori sono previsti o derivano dalla relativa videosorveglianza da parte delle agenzie di contrasto.

41. Inoltre si dovrebbero considerare con attenzione anche i potenziali rischi generati dal ricorso alle tecnologie di riconoscimento facciale da parte delle forze dell'ordine per quanto riguarda il diritto a un giudice imparziale e la presunzione di innocenza ai sensi degli articoli 47 e 48 della Carta. L'esito dell'applicazione della FRT, per esempio una corrispondenza, può non solo comportare che una persona sia sottoposta a ulteriori controlli, ma anche costituire una prova determinante in un procedimento giudiziario. Eventuali carenze della FRT, quali possibili distorsioni, discriminazioni o errori di identificazione («falsi positivi»), possono quindi causare gravi ripercussioni anche a livello di procedimenti penali. Inoltre, nella valutazione delle prove, è possibile che venga data priorità all'esito dell'applicazione della FRT, anche in presenza di prove contraddittorie («distorsione dell'automazione»).

3.1.3 Giustificazione dell'ingerenza

42. Ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui.

3.1.3.1 Limitazioni previste dalla legge

43. L'articolo 52, paragrafo 1, della Carta stabilisce il requisito di una base giuridica specifica, che deve essere sufficientemente chiara nella sua formulazione per fornire ai cittadini un'indicazione adeguata in merito alle condizioni e alle circostanze in cui le autorità possono ricorrere a qualsiasi misura di raccolta di dati e di sorveglianza segreta ([13]). Tale base giuridica deve indicare con ragionevole chiarezza l'ambito e le modalità di esercizio del pertinente potere discrezionale conferito alle autorità pubbliche, in modo da garantire alle persone il livello minimo di tutela previsto dallo Stato di diritto in una società democratica ([14]). Inoltre la liceità richiede garanzie adeguate per assicurare, in particolare, l'osservanza del diritto spettante ai singoli ai sensi dell'articolo 8 della Carta. Questi principi si

([11]) CGUE, C-219/91 – Ter Voort, Racc. 1992 I-05485, punto 36 e segg.; CGUE, C-200/96 – Metronome, Racc. 1998 I-1953, punto 28.
([12]) CGUE, C-594/12, punto 36; CGUE, C-291/12, punto 23 e seguenti.
([13]) Corte EDU, Shimovolos c. Russia, § 68; Vukota-Bojić c. Svizzera.
([14]) Corte EDU, Piechowicz c. Polonia, § 212.

applicano anche al trattamento dei dati personali ai fini della valutazione, della formazione e dell'ulteriore sviluppo dei sistemi FRT.

44. Poiché, quando vengono trattati al fine di identificare una persona fisica in modo univoco, i dati biometrici costituiscono categorie particolari di dati elencate all'articolo 10 della direttiva LED, nella maggior parte dei casi le diverse applicazioni della FRT richiederebbero una legge specifica che descriva con precisione l'applicazione e le condizioni per il suo utilizzo. Ciò comprende in particolare i tipi di reato e, se del caso, la soglia adeguata della loro gravità al fine, tra l'altro, di escludere di fatto la microcriminalità ([15]).

3.1.3.2 Il contenuto essenziale del diritto fondamentale al rispetto della vita privata e alla protezione dei dati di carattere personale sancito dagli articoli 7 e 8 della Carta

45. Le limitazioni dei diritti fondamentali, imminenti per ciascuna situazione, devono comunque prevedere che sia rispettato il contenuto essenziale del diritto specifico. Per contenuto essenziale si intende la sostanza stessa del diritto fondamentale in questione ([16]). Parimenti, la dignità umana non può subire pregiudizio, neanche in caso di limitazione di un diritto ([17]).

46. Sono segnali di una possibile violazione della sostanza stessa di un diritto:

- una disposizione che imponga limitazioni indipendentemente dal comportamento individuale di una persona o dalla presenza di circostanze eccezionali ([18]);
- l'impossibilità o la difficoltà di rivolgersi ai giudici ([19]);
- prima di applicare una grave limitazione, non si tiene conto delle circostanze della persona interessata ([20]);
- per quanto riguarda i diritti di cui agli articoli 7 e 8 della Carta: oltre all'acquisizione di una vasta quantità di metadati delle comunicazioni, il fatto di venire a conoscenza del contenuto delle comunicazioni elettroniche potrebbe violare il contenuto essenziale di tali diritti ([21]);
- per quanto riguarda i diritti di cui agli articoli 7, 8 e 11 della Carta: una normativa che imponga ai fornitori di accesso a servizi di comunicazione al pubblico online e ai fornitori di servizi di hosting la conservazione generalizzata e indifferenziata, in particolare, dei dati personali relativi a tali servizi ([22]);
- in merito ai diritti di cui all'articolo 8 della Carta: anche l'assenza di principi basilari di protezione e sicurezza dei dati potrebbe violare la sostanza del diritto ([23]).

3.1.3.3 Finalità legittima

47. Come è stato già spiegato nel punto 3.1.3, le limitazioni dei diritti fondamentali devono rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui.

([15]) Cfr., per esempio, le sentenze della CGUE nelle cause C-817/19 Ligue des droits humains, punto 151 e seguenti, C-207/16 Ministerio Fiscal, punto 56.
([16]) CGUE, C-279/09, Racc. 2010 I-13849, punto 60.
([17]) Spiegazioni relative alla Carta dei diritti fondamentali, titolo I, spiegazione relativa all'articolo 1, GU C 303 del 14.12.2007, pagg. 17-35.
([18]) CGUE C-601/15, punto 52.
([19]) CGUE C-400/10, Racc. 2010 I-08965, punto 55.
([20]) CGUE C-408/03, Racc. 2006 I-02647, punto 68.
([21]) CGUE - 203/15 - Tele2 Sverige, punto 101 con riferimento a CGUE - C-293/12 e C-594/12, punto 39.
([22]) CGUE C-512/18, La Quadrature du Net, punto 209 e segg.
([23]) CGUE - C-594/12, punto 40.

48. L'Unione riconosce sia gli obiettivi citati nell'articolo 3 del trattato sull'Unione europea, sia altri interessi tutelati da disposizioni specifiche dei trattati ([24]), ossia, tra l'altro, uno spazio di libertà, sicurezza e giustizia, la prevenzione e la lotta contro la criminalità. Nelle sue relazioni con il resto del mondo, l'Unione dovrebbe contribuire alla pace, alla sicurezza e alla tutela dei diritti umani.

49. L'esigenza di proteggere i diritti e le libertà altrui si riferisce ai diritti di persone che sono tutelati dal diritto dell'Unione europea o dei suoi Stati membri. La valutazione deve essere svolta con la finalità di conciliare i requisiti della protezione dei rispettivi diritti e di conseguire un giusto equilibrio tra gli stessi ([25]).

3.1.3.4 Verifica della necessità e della proporzionalità

50. Allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore nazionale e dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano il settore interessato, la natura del diritto in questione garantito dalla Carta, la natura e la gravità dell'ingerenza nonché l'obiettivo di quest'ultima ([26]). Le misure legislative devono essere idonee a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi. Inoltre, la misura non deve superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi ([27]). Un obiettivo di interesse generale, per quanto essenziale, non può giustificare di per sé la limitazione di un diritto fondamentale ([28]).

51. Secondo una costante giurisprudenza della CGUE, le deroghe e le restrizioni alla tutela dei dati personali devono operare entro i limiti dello stretto necessario ([29]). Ne consegue inoltre che non sono disponibili mezzi meno intrusivi per conseguire la finalità; occorre individuare e valutare attentamente possibili alternative, quali ad esempio (a seconda della finalità specifica) l'aumento del personale, controlli più frequenti o un'illuminazione stradale maggiore. Le misure legislative dovrebbero distinguere e riguardare le persone interessate dall'obiettivo, per esempio la lotta contro le forme gravi di criminalità. Se riguarda l'insieme delle persone in maniera globale, senza alcuna distinzione, limitazione o eccezione, essa intensifica l'ingerenza ([30]), anche nel caso in cui il trattamento dei dati riguardi una parte considerevole della popolazione ([31]).

52. La tutela dei dati personali, risultante dall'obbligo esplicito previsto dall'articolo 8, paragrafo 1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita privata sancito dall'articolo 7 della Carta ([32]). La normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e imporre requisiti in modo che le persone i cui dati sono stati trattati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali

([24]) Spiegazioni relative alla Carta dei diritti fondamentali, titolo I, spiegazione relativa all'articolo 52, GU C 303 del 14.12.2007, pagg. 17–35.
([25]) Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.
([26]) CGUE - C-594/12, punto 47 con le seguenti fonti: v., per analogia, per quanto riguarda l'articolo 8 della CEDU, sentenza Corte EDU, S. e Marper c. Regno Unito [GC], nn. 30562/04 e 30566/04, § 102, CEDU 2008-V.
([27]) CGUE - C-594/12, punto 46 con le seguenti fonti: sentenze Afton Chemical, C-343/09, EU:C:2010:419, punto 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, punto 74; Nelson e a., C-581/10 e C-629/10, EU:C:2012:657, punto 71; Sky Österreich, C-283/11 EU:C:2013:28, punto 50; nonché Schaible, C-101/12, EU:C:2013:661, punto 29.
([28]) CGUE - C-594/12, punto 51.
([29]) CGUE - C-594/12, punto 52, con le seguenti fonti: sentenza IPI, C-473/12, EU:C:2013:715, punto 39 e giurisprudenza ivi citata.
([30]) CGUE - C-594/12, punto 57.
([31]) CGUE - C-594/12, punto 56.
([32]) CGUE - C-594/12, punto 53.

contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati ([33]). La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi ([34]). Inoltre, anche l'autorizzazione interna o esterna (per esempio giudiziaria) all'impiego della FRT può contribuire come garanzia e rivelarsi necessaria in determinati casi di grave ingerenza ([35]).

53. Le norme previste devono essere adatte alla situazione specifica, per esempio alla quantità dei dati trattati, al loro carattere ([36]) nonché al rischio di accesso illecito a questi ultimi. Ciò richiede norme che servirebbero, in particolare, a regolare in maniera chiara e precisa la protezione e la sicurezza dei dati di cui trattasi, al fine di garantirne la piena integrità e riservatezza ([37]).

54. Per quanto riguarda il rapporto tra il titolare e il responsabile del trattamento, non si dovrebbero autorizzare i responsabili del trattamento a tenere conto solo di considerazioni economiche nel determinare il livello di sicurezza da essi applicato ai dati personali; ciò potrebbe mettere a repentaglio un livello di protezione sufficientemente elevato ([38]).

55. Un testo legislativo deve stabilire condizioni sostanziali e procedurali e criteri oggettivi che permettano di delimitare l'accesso delle autorità competenti ai dati e il loro uso ulteriore. A fini di prevenzione, di accertamento o di indagini penali, i reati in questione dovrebbero essere considerati sufficientemente gravi da giustificare la portata e la gravità di tali ingerenze nei diritti fondamentali sanciti, ad esempio, dagli articoli 7 e 8 della Carta ([39]).

56. I dati devono essere trattati in modo da garantire l'applicabilità e l'efficacia delle norme dell'UE in materia di protezione dei dati, in particolare di quelle previste dall'articolo 8 della Carta, in base a cui il rispetto dei requisiti di protezione e di sicurezza è soggetto al controllo di un'autorità indipendente. Il luogo geografico in cui avviene il trattamento può essere pertinente in tale situazione ([40]).

57. Per quanto riguarda le diverse fasi del trattamento dei dati personali, occorre effettuare una distinzione tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate ([41]). La determinazione delle condizioni del trattamento, ad esempio quella della durata di conservazione, deve basarsi su criteri obiettivi al fine di garantire che l'ingerenza sia limitata allo stretto necessario ([42]).

58. In base a ciascuna situazione, la valutazione della necessità e della proporzionalità deve individuare e considerare tutte le ripercussioni che rientrano nell'ambito di altri diritti fondamentali, come la dignità umana ai sensi dell'articolo 1 della Carta, la libertà di pensiero, coscienza e religione ai sensi

([33]) CGUE - C-594/12, punto 54, con le seguenti fonti: v., per analogia, per quanto riguarda l'articolo 8 della CEDU, sentenze Corte EDU, Liberty e altri c. Regno Unito, 1° luglio 2008, n. 58243/00, §§ 62 e 63; Rotaru c. Romania, cit. §§ da 57 a 59, nonché S. e Marper c. Regno Unito, cit. § 99.
([34]) CGUE - C-594/12, punto 55, con le seguenti fonti: v., per analogia, con riguardo all'articolo 8 della CEDU, sentenze Corte EDU, S. e Marper c. Regno Unito, cit. § 103, nonché M. K. c. Francia, 18 aprile 2013, n. 19522/09, § 35.
([35]) Corte EDU, Szabó e Vissy c. Ungheria, §§ da 73 a 77.
([36]) Cfr. anche i requisiti più rigorosi per le misure tecniche e organizzative in sede di trattamento di categorie particolari di dati, articolo 29, paragrafo 1, della direttiva LED.
([37]) CGUE - C-594/12, punto 66.
([38]) CGUE - C-594/12, punto 67.
([39]) CGUE - C-594/12, punti 60 e 61.
([40]) CGUE - C-594/12, punto 68.
([41]) CGUE - C-594/12, punto 63.
([42]) CGUE - C-594/12, punto 64.

dell'articolo 10 della Carta, la libertà di espressione ai sensi dell'articolo 11 della Carta e la libertà di riunione e di associazione ai sensi dell'articolo 12 della Carta.

59. Inoltre è da ritenersi grave il fatto che, se i dati vengono trattati sistematicamente all'insaputa degli interessati, ciò possa ingenerare una sensazione generale di costante sorveglianza ([43]), col rischio di causare effetti inibitori relativamente ad alcuni o a tutti i diritti fondamentali interessati.

60. Al fine di agevolare e rendere operativa la valutazione della necessità e della proporzionalità nelle misure legislative connesse al riconoscimento facciale nel settore delle attività di contrasto, i legislatori nazionali e dell'Unione potrebbero avvalersi degli strumenti pratici disponibili appositamente concepiti per tale compito. In particolare, potrebbero utilizzare il kit di strumenti per la necessità e la proporzionalità ([44]) messo a disposizione dal Garante europeo della protezione dei dati.

3.1.3.5 Articolo 52, paragrafo 3, e articolo 53 della Carta (livello di protezione, anche rispetto alla CEDU)

61. Ai sensi dell'articolo 52, paragrafo 3, e dell'articolo 53 della Carta, il significato e la portata dei diritti della Carta corrispondenti a quelli garantiti dalla CEDU devono essere uguali a quelli conferiti da quest'ultima. Benché, in particolare, per l'articolo 7 della Carta si possa trovare un equivalente nella CEDU, non avviene altrettanto per l'articolo 8 della Carta ([45]). L'articolo 52, paragrafo 3, della Carta non impedisce al diritto dell'Unione di prevedere una protezione più ampia. Poiché la CEDU non costituisce un atto giuridico formalmente integrato nel diritto dell'UE, l'esame della validità degli atti dell'UE deve essere effettuato alla luce dei diritti fondamentali della Carta ([46]).

62. Ai sensi dell'articolo 8 della CEDU, non può esservi ingerenza di un'autorità pubblica nell'esercizio del diritto al rispetto della vita privata e familiare, tranne quando tale ingerenza è prevista dalla legge e, in una società democratica, ciò è necessario alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

63. La CEDU definisce anche norme sulle modalità con cui si possono adottare limitazioni. Al di là dello Stato di diritto. un requisito fondamentale è costituito dalla prevedibilità e, al fine di soddisfarlo, il diritto nazionale deve essere sufficientemente chiaro da fornire ai cittadini un'indicazione adeguata in merito alle circostanze in cui e alle condizioni alle quali le autorità possono ricorrere a tali misure ([47]). Tale requisito è riconosciuto dalla CGUE e dalla normativa dell'UE sulla protezione dei dati (cfr. sezione 3.2.1.1).

64. Specificando ulteriormente i diritti di cui all'articolo 8 della CEDU, devono essere pienamente rispettate anche le disposizioni della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale ([48]). Occorre comunque tenere presente che

([43]) CGUE - C-594/12, punto 37.
([44]) Garante europeo della protezione dei dati: «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit» (11.4.2017) [Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: un kit di strumenti (11.4.2017)], Garante europeo della protezione dei dati: GEPD: «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19.12.2019).
([45]) CGUE - C-203/15 - Tele2 Sverige, punto 129.
([46]) CGUE – C-311/18, punto 99.
([47]) Corte europea dei diritti dell'uomo, sentenza nella causa COPLAND c. REGNO UNITO, 03/04/2007, ricorso n. 62617/00, punto 46.
([48]) Serie dei trattati europei n. 108.

queste disposizioni rappresentano solo una norma minima, considerando il diritto dell'Unione prevalente.

3.2 Quadro giuridico specifico: la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie

65. La direttiva LED prevede un determinato quadro relativo all'utilizzo della FRT. In primo luogo, l'articolo 3, paragrafo 13, della direttiva LED definisce l'espressione «dati biometrici» ([49]). Per maggiori dettagli, cfr. la precedente sezione 2.1. In secondo luogo, l'articolo 8, paragrafo 2, chiarisce che, affinché sia lecito, un qualsiasi trattamento deve (oltre a essere necessario per le finalità di cui all'articolo 1, paragrafo 1, della direttiva LED) essere disciplinato dal diritto nazionale e occorre che quest'ultimo specifichi quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità dello stesso. Ulteriori disposizioni particolarmente pertinenti in merito ai dati biometrici sono gli articoli 10 e 11 della direttiva LED; l'articolo 10 e l'articolo 8 di quest'ultima devono essere letti in combinato disposto ([50]). Occorre sempre rispettare i principi per il trattamento dei dati personali di cui all'articolo 4 della direttiva LED, principi che dovrebbero orientare qualsiasi valutazione di un eventuale trattamento biometrico tramite FRT.

3.2.1 Trattamento di categorie particolari di dati per finalità di contrasto

66. Ai sensi dell'articolo 10 della direttiva LED, il trattamento di categorie particolari di dati, quali i dati biometrici, è autorizzato solo se strettamente necessario e soggetto a garanzie adeguate per i diritti e le libertà dell'interessato. Inoltre, è consentito solo se autorizzato dal diritto dell'Unione o dello Stato membro, per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato. Questa clausola generale sottolinea il carattere sensibile del trattamento di categorie particolari di dati.

3.2.1.1 Autorizzato dal diritto dell'Unione o dello Stato membro

67. In merito al tipo necessario di misura legislativa, il considerando 33 della direttiva LED enuncia che «[q]ualora la presente direttiva faccia riferimento al diritto dello Stato membro, a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato» ([51]).

68. Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta sono «previste dalla legge». Ciò richiama l'espressione «conformemente alla legge» di cui all'articolo 8, paragrafo 2, della CEDU, il che significa non soltanto rispetto del diritto applicabile, ma riguarda anche la qualità di tale diritto lasciando impregiudicata la natura dell'atto, cui è richiesto di essere compatibile con lo Stato di diritto.

69. Il considerando 33 della direttiva LED stabilisce inoltre che «(t)uttavia, tale diritto dello Stato membro, base giuridica o misura legislativa dovrebbero essere chiari e precisi, e la loro applicazione prevedibile, per coloro che vi sono sottoposti, come richiesto dalla giurisprudenza della Corte di giustizia e della

([49]) Articolo 3, paragrafo 13, della direttiva LED: «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine del volto o i dati dattiloscopici.
([50]) WP258, Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie, pag. 7.
([51]) Il tipo di misure legislative considerate deve essere conforme al diritto dell'UE o a quello nazionale. A seconda del grado di ingerenza della restrizione, potrebbe rendersi necessaria una particolare misura legislativa a livello nazionale, tenendo conto del livello della norma.

Corte europea dei diritti dell'uomo. Il diritto dello Stato membro che disciplina il trattamento dei dati personali nell'ambito di applicazione della presente direttiva dovrebbe specificare quanto meno gli obiettivi, i dati personali da trattare, le finalità del trattamento e le procedure per preservare l'integrità e la riservatezza dei dati personali come pure le procedure per la loro distruzione».

70. Il diritto nazionale deve essere sufficientemente chiaro nella sua formulazione da fornire agli interessati un'indicazione adeguata in merito alle circostanze e alle condizioni in cui i titolari del trattamento possono ricorrere a tali misure, comprendendo eventuali prerequisiti per il trattamento, come tipi specifici di prove, nonché la necessità di un'autorizzazione giudiziaria o interna. Il diritto in questione può essere neutrale dal punto di vista tecnologico, nella misura in cui le caratteristiche e i rischi specifici del trattamento dei dati personali da parte dei sistemi FRT sono sufficientemente trattati. In linea con la direttiva LED e la giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) nonché della Corte europea dei diritti dell'uomo (CEDU), è di fatto essenziale che le misure legislative, volte a fornire una base giuridica per una misura di riconoscimento facciale, siano prevedibili per gli interessati.

71. Una misura legislativa non può essere invocata come una legge che autorizzi il trattamento dei dati biometrici mediante la FRT a fini di contrasto se si limita a recepire la clausola generale di cui all'articolo 10 della direttiva LED.

72. Oltre ai dati biometrici, l'articolo 10 della direttiva LED disciplina il trattamento di altre categorie particolari di dati, quali l'orientamento sessuale, le opinioni politiche e le convinzioni religiose, contemplando in tal modo un'ampia gamma di trattamenti. Inoltre, tale disposizione sarebbe priva di requisiti specifici che indichino le circostanze e le condizioni in cui le autorità di contrasto sarebbero autorizzate a ricorrere alla tecnologia di riconoscimento facciale. A causa del riferimento ad altri tipi di dati e alla necessità esplicita di garanzie speciali senza ulteriori indicazioni, la disposizione nazionale che recepisce l'articolo 10 della direttiva LED nel diritto nazionale (con una formulazione altrettanto generale e astratta) non può essere invocata come base giuridica per il trattamento dei dati biometrici in cui sia coinvolto il riconoscimento facciale, in quanto difetterebbe di precisione e prevedibilità. Conformemente all'articolo 28, paragrafo 2, o all'articolo 46, paragrafo 1, lettera c), della direttiva LED, prima che il legislatore crei una nuova base giuridica per qualsiasi forma di trattamento dei dati biometrici che si avvalga del riconoscimento facciale, dovrebbe essere consultata l'autorità di controllo nazionale per la protezione dei dati.

3.2.1.2 Strettamente necessario

73. Il trattamento può essere considerato «strettamente necessario» solo se l'ingerenza nella protezione dei dati personali e le sue limitazioni non eccedono la misura assolutamente necessaria ([52]). L'aggiunta del termine «rigorosamente» significa che il legislatore intendeva che il trattamento di categorie particolari di dati dovesse svolgersi solo in condizioni ancora più rigorose rispetto a quelle di necessità (cfr. sopra, punto 3.1.3.4); tale requisito dovrebbe essere interpretato come indispensabile, limitando a un minimo assoluto il margine di valutazione consentito all'autorità di contrasto nella verifica della necessità. Conformemente alla giurisprudenza costante della Corte di giustizia dell'Unione europea, anche la condizione del «carattere strettamente necessario» è particolarmente legata al requisito dei criteri oggettivi per definire le circostanze e le condizioni in cui si può effettuare il trattamento, escludendo così qualsiasi trattamento di carattere generale o sistematico ([53]).

([52]) Giurisprudenza costante sul diritto fondamentale al rispetto della vita privata: cfr. CGUE, causa C-73/07, punto 56 (Satakunnan Markkinapörssi e Satamedia); CGUE, cause C-92/09 e C-93/09, punto 77 (Schecke e Eifert); CGUE - C-594/12, punto 52 (Digital Rights); CGUE, causa C-362/14, punto 92 (Schrems).
([53]) CGUE, causa C- 623/17, punto 78.

3.2.1.3 Dati resi manifestamente reso pubblici

74. Nel valutare se il trattamento si riferisca o meno a dati resi manifestamente pubblici da un interessato, occorre ricordare che una fotografia in quanto tale non è considerata sistematicamente un dato biometrico ([54]). Pertanto, il fatto che una fotografia sia stata resa manifestamente pubblica dall'interessato non implica che i relativi dati biometrici, ricavabili dalla fotografia con mezzi tecnici specifici, si considerino resi manifestamente pubblici.

75. Come avviene per i dati personali in generale, affinché quelli biometrici siano considerati manifestamente resi pubblici dall'interessato, quest'ultimo deve avere volontariamente reso liberamente accessibile e pubblico il modello biometrico (e non semplicemente un'immagine del volto) attraverso una fonte aperta. Se un terzo divulga i dati biometrici, questi ultimi non si possono considerare manifestamente resi pubblici dall'interessato.

76. Inoltre non è sufficiente interpretare il comportamento di un interessato per ritenere che i dati biometrici siano stati manifestamente resi pubblici. Ad esempio, nel caso dei social network o delle piattaforme online, l'EDPB sostiene che, se l'interessato non ha attivato né stabilito funzionalità di privacy specifiche, ciò non sia sufficiente per ritenere che l'interessato abbia manifestamente reso pubblici i propri dati personali e che questi ultimi (per esempio fotografie) possano essere trasformati in modelli biometrici e utilizzati a fini di identificazione senza il consenso dell'interessato. Più in generale, le impostazioni predefinite di un servizio (per esempio la messa a disposizione del pubblico di modelli o l'assenza di scelta, come quando i modelli vengono resi pubblici senza che l'utente possa modificare tale impostazione) non dovrebbero in alcun modo essere interpretate come dati resi manifestamente pubblici.

3.2.2 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

77. L'articolo 11, paragrafo 1, della direttiva LED prevede l'obbligo per gli Stati membri di vietare in generale le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato. In deroga a tale divieto generale, tale trattamento è possibile solo se è autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e tale diritto prevede garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento. La deroga può essere utilizzata solo in modo restrittivo. Questa soglia si applica alle categorie ordinarie (ossia non speciali) di dati personali. Per la deroga di cui all'articolo 11, paragrafo 2, della direttiva LED, si applica una soglia ancora più elevata e un utilizzo ancora più restrittivo. Essa ribadisce che le decisioni di cui al paragrafo 1 non si basano sulle categorie particolari di dati, ossia in particolare sui dati biometrici intesi a identificare in modo univoco una persona fisica. Una deroga può essere prevista solo se sono in vigore misure adeguate a salvaguardia dei diritti e delle libertà dell'interessato e dei legittimi interessi della persona fisica in questione. Tale deroga deve essere letta a supplemento e alla luce delle premesse dell'articolo 10 della direttiva LED.

78. In base al sistema FRT, persino l'intervento umano cui è affidata la valutazione dei risultati della FRT potrebbe non fornire necessariamente una garanzia sufficiente di per sé in merito al rispetto dei diritti delle persone e, in particolare, del diritto alla protezione dei dati personali (considerando gli eventuali

([54]) Cfr. il considerando 51 del RGPD: «Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.»

errori e le distorsioni derivanti dal trattamento stesso), e inoltre si può ritenere che rappresenti una garanzia solo se la persona che interviene può contestare criticamente i risultati della FRT durante l'intervento umano. È fondamentale permetterle di comprendere il sistema FRT e i suoi limiti, nonché di interpretarne correttamente i risultati; è altresì necessario predisporre un ambiente di lavoro e un'organizzazione tali da controbilanciare gli effetti della distorsione dell'automazione, evitando di favorire l'accettazione acritica dei risultati, per esempio a causa delle ristrettezze di tempo, di procedure onerose, di potenziali effetti negativi sulla carriera, ecc.

79. Ai sensi dell'articolo 11, paragrafo 3, della direttiva LED, la profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali come i dati biometrici è vietata, conformemente al diritto dell'Unione. Ai sensi dell'articolo 3, paragrafo 4, della direttiva LED, per «profilazione» si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. Nel valutare se siano previste misure adeguate a salvaguardia dei diritti e delle libertà dell'interessato e dei legittimi interessi della persona fisica in questione, occorre tenere presente che il ricorso alla FRT può implicare la profilazione, a seconda della modalità e delle finalità per cui la FRT viene applicata. In ogni caso, ai sensi del diritto dell'Unione e dell'articolo 11, paragrafo 3, della direttiva LED, la profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali è vietata.

3.2.3 Categorie di interessati

80. L'articolo 6 della direttiva LED riguarda la necessità di distinguere tra diverse categorie di interessati; tale distinzione deve essere operata se del caso e nella misura del possibile, producendo effetti sulla modalità di trattamento dei dati. Dagli esempi forniti all'articolo 6 della direttiva LED si può dedurre che, di norma, il trattamento dei dati personali deve soddisfare i criteri di necessità e proporzionalità anche per quanto riguarda la categoria di interessati ([55]). Si può evincere inoltre che, per quanto riguarda gli interessati per i quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o remoto, con l'obiettivo legittimo secondo la direttiva LED, è assai probabile che non si possa giustificare un'ingerenza ([56]). Se non è applicabile né possibile alcuna distinzione ai sensi dell'articolo 6 della direttiva LED, nella valutazione della necessità e della proporzionalità dell'ingerenza occorre tenere rigorosamente conto dell'eccezione alla regola di cui all'articolo suddetto. Sembra che la distinzione tra diverse categorie di interessati costituisca un requisito essenziale per quanto riguarda il trattamento dei dati personali che comporta il riconoscimento facciale, anche considerando i possibili falsi riscontri positivi o negativi, che possono avere impatti considerevoli per gli interessati anche nel corso di un'indagine.

81. Come detto, nell'attuazione del diritto dell'Unione devono essere rispettate le disposizioni della Carta dei diritti fondamentali dell'Unione europea (cfr. articolo 52 della Carta). Il quadro e i criteri previsti dalla direttiva LED devono pertanto essere letti alla luce della Carta. I testi legislativi dell'UE e dei suoi Stati membri non devono essere da meno rispetto a questa misura e devono garantire la piena efficacia della Carta.

([55]) Cfr. anche CGUE - C-594/12, punti da 56 a 59.
([56]) Cfr. anche CGUE - C-594/12, punto 58.

3.2.4 Diritti dell'interessato

82. L'EDPB ha già fornito orientamenti sui diritti degli interessati a norma del RGPD sotto diversi aspetti ([57]). La direttiva LED prevede diritti analoghi per gli interessati e il gruppo di lavoro «articolo 29» ha fornito orientamenti generali al riguardo in un parere che è stato approvato dall'EDPB ([58]). In determinate circostanze, la direttiva LED consente di porre alcune limitazioni a questi diritti; i parametri per tali limitazioni saranno ulteriormente elaborati nella sezione 3.2.4.6. «Limitazioni legittime ai diritti degli interessati».

83. Benché tutti i diritti dell'interessato elencati nel capo III della direttiva LED si applichino naturalmente anche al trattamento dei dati personali mediante la tecnologia di riconoscimento facciale (FRT), il capitolo seguente si concentrerà su alcuni diritti e aspetti su cui si potrebbero ricevere indicazioni di particolare interesse. Inoltre, questo capitolo e la relativa analisi indicano se il trattamento mediante FRT in questione abbia soddisfatto i requisiti giuridici descritti nel capitolo precedente.

84. Data la natura del trattamento dei dati personali effettuato tramite FRT (trattamento di categorie particolari di dati personali, spesso senza alcuna interazione apparente con l'interessato), il titolare del trattamento deve valutare accuratamente come (o se possa) soddisfare i requisiti della direttiva LED prima di avviare qualsiasi trattamento mediante FRT, in particolare analizzando attentamente:

- chi sono gli interessati (spesso non solo il destinatario o i destinatari principali ai fini del trattamento);
- le modalità con cui gli interessati vengono informati del trattamento mediante FRT (cfr. sezione 3.2.4.1);
- le modalità con cui gli interessati possono esercitare i propri diritti (in questo caso, può risultare particolarmente difficile tutelare sia i diritti di informazione e di accesso che quelli di rettifica o di limitazione del trattamento, nel caso in cui si ricorra alla FRT per effettuare tutte le verifiche tranne quella 1:1 a contatto diretto con l'interessato).

3.2.4.1 Comunicare agli interessati i diritti e le informazioni in forma concisa, intelligibile e facilmente accessibile.

85. La FRT comporta alcuni problemi per quanto riguarda il fatto di garantire che gli interessati siano informati del trattamento dei loro dati biometrici. Ciò è particolarmente difficile se un'autorità di contrasto analizza tramite la FRT materiale video proveniente da terzi o fornito da questi ultimi poiché è improbabile, e il più delle volte impossibile, che detta autorità possa informare l'interessato al momento dell'acquisizione dei dati (ad esempio tramite un cartello in loco). Qualsiasi materiale video non pertinente per l'indagine (o per la finalità del trattamento) dovrebbe sempre essere cancellato o anonimizzato (per esempio offuscando l'immagine senza alcuna possibilità retroattiva di recuperare i dati) prima di effettuare qualsiasi trattamento di dati biometrici, al fine di evitare il rischio di inosservanza del principio di minimizzazione di cui all'articolo 4, paragrafo 1, lettera e), della direttiva LED e gli obblighi di informazione di cui all'articolo 13, paragrafo 2, della direttiva LED. Compete al titolare del trattamento valutare quali informazioni siano importanti per l'interessato nell'esercizio dei suoi diritti e garantire che vengano fornite le informazioni necessarie. L'effettivo esercizio dei diritti dell'interessato dipende dall'adempimento, da parte del titolare del trattamento, dei propri obblighi di informazione.

([57]) Cfr. per esempio le Linee guida EDPB 1/2022 sui diritti dell'interessato - Diritto di accesso e le Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video.
([58]) WP258, Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie.

86. L'articolo 13, paragrafo 1, della direttiva LED stabilisce quali informazioni minime debbano essere fornite in generale all'interessato. Tali informazioni possono essere comunicate tramite il sito web del titolare del trattamento, in forma cartacea (per esempio un opuscolo disponibile su richiesta) o con altre fonti di facile accesso per l'interessato. Il titolare del trattamento deve in ogni caso garantire che vengano effettivamente fornite informazioni almeno in merito ai seguenti elementi:

- identità e dati di contatto del titolare del trattamento, incluso il responsabile della protezione dei dati;
- la finalità del trattamento e il fatto che esso avvenga mediante FRT;
- il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità;
- il diritto di chiedere l'accesso, la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali.

87. Inoltre, in casi specifici definiti dal diritto nazionale che dovrebbero essere in linea con l'articolo 13, paragrafo 2, della direttiva LED ([59]), come ad esempio nel caso di un trattamento basato sulla FRT, occorre fornire direttamente all'interessato le seguenti informazioni:

- la base giuridica per il trattamento;
- informazioni sul luogo in cui i dati personali sono stati raccolti all'insaputa dell'interessato;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- se del caso, le categorie di destinatari dei dati personali (anche in paesi terzi o in seno a organizzazioni internazionali).

88. Mentre l'articolo 13, paragrafo 1, della direttiva LED riguarda informazioni generali rese disponibili al pubblico, l'articolo 13, paragrafo 2, riguarda le ulteriori informazioni che devono essere fornite a un determinato interessato in casi specifici, per esempio qualora i dati siano raccolti direttamente presso l'interessato o indirettamente a sua insaputa ([60]). Benché non esista una definizione chiara di cosa si intenda per «casi specifici» all'articolo 13, paragrafo 2, della direttiva LED, l'espressione si riferisce a situazioni in cui gli interessati devono essere informati del trattamento che li riguarda specificamente e ricevere informazioni adeguate per poter esercitare i loro diritti in modo efficace. L'EDPB ritiene che, nel valutare l'esistenza di un «caso specifico», si debba tenere conto di diversi fattori, tra cui l'eventualità che i dati personali siano raccolti all'insaputa dell'interessato, poiché questo sarebbe l'unico modo per consentire agli interessati di esercitare i loro diritti in modo efficace. Altri esempi di «casi specifici» potrebbero essere quelli in cui i dati personali vengono ulteriormente trattati in quanto soggetti a una procedura internazionale di cooperazione giudiziaria penale o quelli in cui i dati personali sono trattati nell'ambito di operazioni sotto copertura, come specificato nel diritto nazionale. Inoltre, risulta dal considerando 38 della direttiva LED che, qualora il processo decisionale debba svolgersi esclusivamente sulla base della FRT, gli interessati devono essere informati in merito alle caratteristiche del processo decisionale automatizzato. Ciò indicherebbe inoltre che si tratta di un caso

([59]) Ad esempio, l'articolo 56, paragrafo 1, della legge federale tedesca sulla protezione dei dati che, tra l'altro, indica quali informazioni debbano essere fornite agli interessati nell'ambito di operazioni sotto copertura.
([60]) WP258 Parere su alcune questioni chiave della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (UE 2016/680), pagg. 17-18.

specifico in cui dovrebbero essere fornite all'interessato ulteriori informazioni ai sensi dell'articolo 13, paragrafo 2, della direttiva LED ([61]).

89. Infine occorre osservare che, ai sensi dell'articolo 13, paragrafo 3, della direttiva LED, gli Stati membri possono adottare misure legislative che limitano l'obbligo di comunicare informazioni in casi specifici per determinati obiettivi. Ciò si applica nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi dell'interessato.

3.2.4.2 Diritto di accesso

90. In generale, l'interessato ha il diritto di ottenere la conferma positiva o negativa di qualsiasi trattamento dei suoi dati personali e, in caso di risposta positiva, di ottenere l'accesso ai dati personali in quanto tali, nonché alle informazioni supplementari elencate all'articolo 14 della direttiva LED. Per quanto riguarda la FRT, quando i dati biometrici vengono memorizzati e collegati a un'identità (anche tramite dati alfanumerici), ciò dovrebbe consentire all'autorità competente di confermare una richiesta di accesso basata sulla ricerca di tali dati alfanumerici, senza avviare alcun ulteriore trattamento di dati biometrici altrui (per esempio effettuando una ricerca con la FRT in una banca dati). Occorre rispettare il principio della minimizzazione dei dati e non si dovrebbe conservare una quantità di dati maggiore del necessario in relazione alla finalità del trattamento.

3.2.4.3 Diritto di rettifica dei dati personali

91. Poiché la FRT non garantisce l'accuratezza assoluta, è particolarmente importante che i titolari del trattamento siano attenti alle richieste di rettifica dei dati personali, anche nel caso in cui un interessato, in base alla FRT, sia stato inserito erroneamente in una categoria inesatta (per esempio nella categoria delle persone sospette) perché inizialmente era stata ipotizzata una sua serie di azioni in un filmato. I rischi per gli interessati sono particolarmente gravi se tali dati inesatti sono conservati in una banca dati della polizia e/o vengono condivisi con altre entità. Il titolare del trattamento deve pertanto correggere i dati conservati e i sistemi FRT di conseguenza (cfr. il considerando 47 della direttiva LED).

3.2.4.4 Diritto di cancellazione

92. Nella maggior parte delle circostanze, se non viene utilizzata a fini di autenticazione/verifica 1:1, la FRT equivarrà al trattamento di un gran numero di dati biometrici degli interessati; perciò è importante che il titolare del trattamento valuti preventivamente quali siano i limiti della sua finalità e necessità, affinché sia possibile trattare una richiesta di cancellazione ai sensi dell'articolo 16 della direttiva LED senza indebito ritardo (poiché il titolare del trattamento deve, tra l'altro, cancellare dati personali trattati al di là della misura consentita dalla normativa applicabile ai sensi degli articoli 4, 8 e 10 della direttiva LED).

3.2.4.5 Diritto alla limitazione

93. Nel caso in cui l'interessato contesti l'accuratezza dei dati e non sia possibile accertarla (o qualora i dati personali debbano essere conservati per futuri fini probatori), il titolare è tenuto a limitare il trattamento dei dati personali del suddetto interessato ai sensi dell'articolo 16 della direttiva LED. Ciò diventa particolarmente importante quando si ha che fare con la tecnologia di riconoscimento facciale (che, basandosi su uno o più algoritmi, non mostra mai un risultato definitivo) in situazioni in cui vengono acquisite grandi quantità di dati e l'accuratezza e la qualità dell'identificazione possono

([61]) Si noti bene la differenza tra «rendere disponibili all'interessato» nell'articolo 13, paragrafo 1, della direttiva LED e «fornire all'interessato» nell'articolo 13, paragrafo 2, della medesima direttiva. Ai sensi dell'articolo 13, paragrafo 2, della direttiva LED, il titolare del trattamento deve garantire che le informazioni pervengano all'interessato, qualora non siano sufficienti le informazioni pubblicate su un sito web.

variare; con materiale video di scarsa qualità (per esempio quello tratto dal luogo del reato) aumenta il rischio di falsi positivi. Inoltre, se in una lista di controllo le immagini facciali non vengono aggiornate periodicamente, è maggiore anche il rischio di falsi positivi o falsi negativi. In casi specifici in cui i dati non possono essere cancellati perché vi sono motivi ragionevoli di ritenere che la cancellazione possa compromettere gli interessi legittimi dell'interessato, i dati dovrebbero invece essere limitati e trattati solo per la finalità che ne ha impedito la cancellazione (cfr. considerando 47 della direttiva LED).

3.2.4.6 Limitazioni legittime ai diritti degli interessati

94. Per quanto riguarda gli obblighi di informazione del titolare del trattamento e il diritto di accesso degli interessati, sono consentite limitazioni soltanto a condizione che queste ultime siano stabilite dalla legge che, a sua volta, deve costituire una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata (cfr. articolo 13, paragrafi 3 e 4, articolo 15 e articolo 16, paragrafo 4, della direttiva LED). Quando si ricorre alla FRT a fini di contrasto, ci si può aspettare che venga utilizzata in circostanze in cui sarebbe dannoso per la finalità perseguita informare l'interessato o consentire l'accesso ai dati; ciò varrebbe, ad esempio, per un'indagine di polizia su un reato o a fini di tutela della sicurezza nazionale o pubblica.

95. Il diritto di accesso non comporta automaticamente l'accesso a tutte le informazioni, per esempio nell'ambito di un caso penale in cui sono coinvolti i propri dati personali. Un altro esempio valido di caso in cui sono ammissibili limitazioni a questo diritto potrebbe essere costituito da un'indagine penale in corso.

3.2.4.7 Esercizio dei diritti tramite l'autorità di controllo

96. Nei casi in cui sussistono limitazioni legittime all'esercizio dei diritti ai sensi del capo III della direttiva LED, l'interessato può chiedere che l'autorità di protezione dei dati di esercitare i diritti dello stesso per suo conto, verificando la legittimità del trattamento da parte del relativo titolare. Spetta al responsabile del trattamento informare l'interessato della possibilità di esercitare i suoi diritti in tal modo [cfr. articolo 17 e articolo 46, paragrafo 1, lettera g), della direttiva LED]. Per quanto concerne la FRT, ciò significa che il titolare del trattamento deve garantire che siano in vigore misure adeguate affinché sia possibile trattare tale richiesta, per esempio consentendo la ricerca di materiale registrato, a condizione che l'interessato fornisca informazioni sufficienti per localizzare i dati personali che lo riguardano.

3.2.5 Altri requisiti giuridici e garanzie

3.2.5.1 Articolo 27 - Valutazione d'impatto sulla protezione dei dati

97. Una valutazione d'impatto sulla protezione dei dati (DPIA) prima di avvalersi della FRT è un requisito obbligatorio in quanto il tipo di trattamento, prevedendo in particolare l'uso di nuove tecnologie e considerando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Poiché il ricorso alla FRT comporta il trattamento automatizzato sistematico di categorie particolari di dati, si potrebbe ipotizzare che in tali casi il titolare del trattamento sia di norma tenuto a condurre una DPIA. Quest'ultima dovrebbe contenere almeno una descrizione generale dei trattamenti previsti, una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità. L'EDPB raccomanda di rendere pubblici i risultati di tali

valutazioni, o almeno quelli principali e le conclusioni della DPIA, come misura per rafforzare la fiducia e la trasparenza ([62]).

3.2.5.2 Articolo 28 - Consultazione preventiva dell'autorità di controllo

98. Ai sensi dell'articolo 28 della direttiva LED, il titolare del trattamento o il responsabile del trattamento deve consultare l'autorità di controllo prima del trattamento se: a) una valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure b) il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati. Come già spiegato nella sezione 2.3 delle presenti linee guida, l'EDPB ritiene che la maggior parte dei casi di diffusione e utilizzo della FRT comporti un rischio intrinseco elevato per i diritti e le libertà degli interessati. Pertanto, oltre alla valutazione d'impatto sulla protezione dei dati, l'autorità che ricorre alla FRT dovrebbe consultare l'autorità di controllo competente prima di implementare il sistema.

3.2.5.3 Articolo 29 - Sicurezza del trattamento

99. La natura univoca dei dati biometrici fa sì che per l'interessato sia impossibile modificarli nel caso in cui vengano compromessi, per esempio in seguito a una violazione dei dati. Pertanto l'autorità competente che attua e/o utilizza la FRT dovrebbe prestare particolare attenzione alla sicurezza del trattamento, in linea con l'articolo 29 della direttiva LED. In particolare, l'autorità di contrasto dovrebbe garantire che il sistema sia conforme alle norme pertinenti e attuare misure di protezione dei modelli biometrici ([63]). Tale obbligo è ancora più pertinente se l'autorità di contrasto si avvale di un fornitore terzo di servizi (responsabile del trattamento).

3.2.5.4 Articolo 20 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

100. La protezione dei dati fin dalla progettazione e per impostazione predefinita, conformemente all'articolo 20 della direttiva LED, mira a garantire che i principi e le garanzie in materia di protezione dei dati, quali la loro minimizzazione e la limitazione della conservazione, siano integrati nella tecnologia attraverso misure tecniche e organizzative adeguate, quali la pseudonimizzazione, anche prima dell'inizio del trattamento dei dati personali, e siano applicati durante tutto il suo ciclo di vita. Dato l'elevato rischio intrinseco per i diritti e le libertà delle persone fisiche, la scelta di tali misure non dovrebbe dipendere unicamente da considerazioni economiche ([64]), ma dovrebbe avere piuttosto la finalità di attuare le tecnologie di protezione dei dati all'avanguardia. Analogamente, se intende applicare e impiegare la FRT messa a disposizione da fornitori esterni, un'autorità di contrasto deve garantire, ad esempio mediante la procedura di appalto, che siano utilizzate solo tecnologie di riconoscimento facciale basate sui principi della protezione dei dati fin dalla progettazione e per impostazione predefinita ([65]). Ciò implica anche che la trasparenza in merito al funzionamento della FRT non venga limitata da rivendicazioni di segreti commerciali o di diritti di proprietà intellettuale.

([62]) Per ulteriori informazioni, cfr. WP248 rev.01, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato».

([63]) Cfr. per esempio: ISO/IEC 24745 Information security, cybersecurity and privacy protection - Biometric information protection [Sicurezza delle informazioni, cybersicurezza e protezione della privacy - Protezione delle informazioni biometriche].

([64]) Cfr. il considerando 53 della direttiva LED.

([65]) Per maggiori informazioni cfr. le Linee guida dell'EDPB sulla protezione dei dati fin dalla progettazione e sulla protezione per impostazione predefinita, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

3.2.5.5 Articolo 25 - Registrazione

101. La direttiva LED prevede diversi metodi con cui il titolare o il responsabile del trattamento può dimostrare la liceità del trattamento e assicurare l'integrità e la sicurezza dei dati. A questo proposito, le registrazioni dei sistemi rappresentano uno strumento molto utile e una garanzia importante per verificare la liceità del trattamento, sia a livello interno (ossia attraverso l'autocontrollo) che da parte di autorità di controllo esterne quali le autorità di protezione dei dati. Ai sensi dell'articolo 25 della direttiva LED, devono essere registrati in sistemi di trattamento automatizzato i seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione. Inoltre le registrazioni delle consultazioni e delle comunicazioni dovrebbero consentire di stabilire la motivazione, la data e l'ora di tali operazioni e, nella misura del possibile, di identificare la persona che ha consultato o comunicato i dati personali, nonché di stabilire l'identità dei destinatari di tali dati personali. Per di più, nel contesto dei sistemi di riconoscimento facciale, si raccomanda di registrare anche le seguenti operazioni di trattamento (che esulano in parte dall'ambito dell'articolo 25 della direttiva LED):

- modifiche della banca dati di riferimento (aggiunta, cancellazione o aggiornamento). La registrazione dovrebbe conservare una copia dell'immagine pertinente (aggiunta, cancellata o aggiornata) quando non è altrimenti possibile verificare la liceità o l'esito delle operazioni di trattamento;

- tentativi di identificazione o di verifica, incluso l'esito e il punteggio di confidenza. Si dovrebbe applicare rigorosamente il principio di minimizzazione, affinché sia conservato nelle registrazioni soltanto l'identificativo dell'immagine proveniente dalla banca dati di riferimento, anziché l'immagine di riferimento. Occorre evitare la registrazione dei dati biometrici in ingresso, a meno che non sia necessaria (ad esempio solo in casi di corrispondenza);

- l'ID dell'utente che ha richiesto l'identificazione o il tentativo di verifica;

- tutti i dati personali conservati nelle registrazioni dei sistemi sono soggetti a rigorose limitazioni di finalità (ad esempio gli audit) e non dovrebbero essere utilizzati per altri scopi (ad esempio per poter effettuare ancora un riconoscimento/una verifica che riguardi un'immagine che è stata cancellata dalle banche dati di riferimento). Occorre applicare misure di sicurezza per garantire l'integrità delle registrazioni, mentre sono vivamente raccomandati sistemi di monitoraggio automatico per rilevare l'abuso delle registrazioni. Per quanto riguarda le registrazioni della banca dati di riferimento, si dovrebbero attuare misure di sicurezza equivalenti a quelle della banca dati di riferimento, in caso di conservazione delle immagini facciali. Si dovrebbero inoltre attuare procedure automatiche per garantire che venga applicato il periodo di conservazione dei dati per le registrazioni.

3.2.5.6 Articolo 4, paragrafo 4 - Responsabilità

102. Il titolare del trattamento deve essere in grado di comprovare la conformità del trattamento ai principi di cui all'articolo 4, paragrafi da 1 a 3 (cfr. l'articolo 4, paragrafo 4, della direttiva LED). A questo riguardo, è fondamentale una documentazione sistematica e aggiornata del sistema (comprendente aggiornamenti, miglioramenti e la formazione algoritmica), delle misure tecniche e organizzative (inclusi il monitoraggio delle prestazioni del sistema e il potenziale intervento umano) e del trattamento dei dati personali. Per dimostrare la liceità del trattamento, un aspetto particolarmente importante è costituito dalla registrazione ai sensi dell'articolo 25 della direttiva LED (cfr. sezione 3.2.5.5). Il principio di responsabilità riguarda non soltanto il sistema e il trattamento, ma anche la documentazione di garanzie procedurali come le valutazioni della necessità e della proporzionalità, le DPIA nonché le consultazioni interne (per esempio l'approvazione del progetto da

parte della dirigenza o le decisioni interne in merito ai valori dei punteggi di confidenza) e le consultazioni esterne (per esempio con l'autorità competente per la protezione dei dati). L'allegato II comprende alcuni elementi a questo proposito.

3.2.5.7 Articolo 47 - Controllo efficace

103. Il controllo efficace da parte delle autorità competenti per la protezione dei dati è una delle garanzie più importanti per i diritti e le libertà fondamentali delle persone interessate dal ricorso alla FRT. Contestualmente, dotare ciascuna autorità di controllo delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari costituisce un presupposto per l'effettivo adempimento dei loro compiti e l'esercizio dei loro poteri ([66]). Più importanti ancora del numero di membri del personale disponibili sono le competenze degli esperti, che dovrebbero trattare una gamma molto ampia di questioni, dalle indagini penali e dalla cooperazione di polizia all'analisi dei megadati e all'IA. Pertanto, gli Stati membri dovrebbero garantire che le risorse delle autorità di controllo siano adeguate e sufficienti per consentire loro di svolgere il loro mandato, ossia tutelare i diritti degli interessati e seguire da vicino gli sviluppi al riguardo ([67]).

4 CONCLUSIONI

104. Il ricorso alle tecnologie di riconoscimento facciale è intrinsecamente legato al trattamento di quantità considerevoli di dati personali, comprese categorie particolari di dati. Il volto e, più in generale, i dati biometrici sono legati in modo permanente e irrevocabile all'identità di una persona. Pertanto l'utilizzo del riconoscimento facciale ha un impatto diretto o indiretto su una serie di diritti e libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE che non sempre si limitano alla privacy e alla protezione dei dati, come la dignità umana, la libertà di movimento, la libertà di riunione e altri, cosa particolarmente pertinente nel settore delle attività di contrasto e della giustizia penale.

105. L'EDPB riconosce che le autorità di contrasto hanno l'esigenza di accedere ai migliori strumenti possibili in modo da identificare rapidamente gli autori di atti terroristici e altri reati gravi. Tuttavia, tali strumenti devono essere utilizzati nel rigoroso rispetto del quadro giuridico applicabile e solo nei casi in cui soddisfano i requisiti di necessità e proporzionalità, come stabilito dall'articolo 52, paragrafo 1, della Carta. Inoltre, anche se le moderne tecnologie possono far parte della soluzione, non costituiscono affatto una «formula magica».

106. Esistono alcuni casi d'uso delle tecnologie di riconoscimento facciale che comportano rischi inaccettabilmente elevati per le persone e la società («limiti invalicabili»). Per questi motivi l'EDPB e il GEPD hanno richiesto il divieto generale di tali usi ([68]).

107. In particolare, l'identificazione biometrica remota delle persone in spazi accessibili al pubblico implica un rischio elevato di intrusione nella vita privata delle persone e non è ammissibile in una società democratica poiché comporta, per sua natura, una sorveglianza di massa. Analogamente, l'EDPB ritiene che i sistemi di riconoscimento facciale basati sull'IA che classificano le persone, in funzione dei

([66]) Cfr. la comunicazione della Commissione «Prima relazione sull'applicazione e sul funzionamento della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di contrasto», COM(2022) 364 final, punto 3.4.1.
([67]) Cfr. Contributo dell'EDPB alla valutazione della LED da parte della Commissione europea ai sensi dell'articolo 62, paragrafo 14., https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf
([68]) Cfr. EDPB-GEPD Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale): https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

loro dati biometrici, in gruppi secondo l'etnia, il genere, l'orientamento politico o sessuale non siano compatibili con la Carta. Per di più, l'EDPB è convinto che l'uso del riconoscimento facciale o di tecnologie analoghe per dedurre le emozioni di una persona fisica sia particolarmente indesiderabile e dovrebbe essere vietato, possibilmente con poche eccezioni debitamente giustificate. Inoltre l'EDPB ritiene che il trattamento dei dati personali in un contesto di applicazione della legge che si baserebbe su una banca dati popolata tramite la raccolta di dati personali su vasta scala e in modo indiscriminato, ad esempio attraverso lo «scraping» di fotografie e immagini facciali accessibili online, in particolare quelle rese disponibili attraverso i social network, non sarebbe conforme, in quanto tale, al requisito di stretta necessità previsto dal diritto dell'Unione.

5 ALLEGATI

Allegato I: Modello di supporto

Allegato II: Orientamenti pratici per la gestione dei progetti FRT presso le autorità di contrasto

Allegato III: Esempi pratici

ALLEGATO I - MODELLO PER LA DESCRIZIONE DEGLI SCENARI

(con infobox per gli aspetti trattati nello scenario)

Descrizione del trattamento

- Descrizione del trattamento, contesto (relazione con il reato), finalità

Fonte delle informazioni:

- Tipi di interessati: ☐ tutti i cittadini ☐ detenuti ☐ indagati ☐ minori ☐ altri interessati vulnerabili
- Fonte dell'immagine: ☐ spazi accessibili al pubblico ☐ internet ☐ entità privata ☐ altre persone ☐ altro .....
- Collegamento con il reato: ☐ Temporale diretto ☐ Temporale non diretto ☐ Geografico diretto ☐ Geografico non diretto ☐ Non necessario
- Modalità di acquisizione delle informazioni: ☐ remota ☐ in una cabina o in un ambiente controllato
- Contesto: incidenza su altri diritti fondamentali:
  ☐ No
  Sì, in particolare sulla ☐ libertà di riunione
  ☐ libertà di espressione
  ☐ varie:.....
- Possibili ulteriori fonti di informazioni sull'interessato:
  ☐ Documento d'identità☐ uso del telefono pubblico ☐ targa del veicolo
  ☐ altro .....

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità: ☐ banche dati per finalità generali ☐ banche dati specifiche relative alla zona in cui è avvenuto il reato
- Descrizione della modalità con cui sono state popolate tali banche dati di riferimento (e base giuridica)
- Modifica della finalità della banca dati (per esempio, l'obiettivo principale era la sicurezza della proprietà privata): ☐ Sì ☐ NO

Algoritmo:

- Tipo di trattamento: ☐ verifica (autenticazione) 1:1 ☐ identificazione 1:molti
- Considerazioni sull'accuratezza
- Garanzie tecniche

Esito:

- Impatto ☐ diretto (per esempio l'interessato può essere arrestato, interrogato, comportamento discriminatorio)

  ☐ Non diretto (utilizzato per modelli statistici, nessuna conseguenza legale grave per gli interessati)

- Decisione automatizzata:☐ SÌ☐ NO
- Durata della conservazione

Analisi giuridica:

- Analisi della necessità e della proporzionalità - finalità/gravità del reato/numero di persone non coinvolte ma interessate dal trattamento
- Tipo di informazione preliminare all'interessato: ☐ Al momento dell'ingresso nella zona specifica

  ☐ Sul sito web dell'autorità di contrasto in generale

  ☐ Sul sito web dell'autorità di contrasto per il trattamento specifico

  ☐ Altro .....
- Quadro giuridico applicabile:

  ☐ Direttiva LED, ripresa in gran parte nel diritto nazionale

  ☐ Normativa nazionale generica per l'utilizzo di dati biometrici da parte delle autorità di contrasto

  ☐ Normativa nazionale specifica per questo trattamento (riconoscimento facciale) per l'autorità competente in questione

  ☐ Normativa nazionale specifica per questo trattamento (decisione automatizzata)

Conclusione:

Considerazioni generali sull'eventualità che il trattamento descritto sia compatibile con il diritto dell'UE (e alcuni riferimenti ai presupposti di legge)

ALLEGATO II - ORIENTAMENTI PRATICI PER LA GESTIONE DEI PROGETTI FRT PRESSO LE AUTORITÀ DI CONTRASTO

Il presente allegato fornisce ulteriori orientamenti pratici per le autorità di contrasto («LEA») che intendono avviare un progetto in cui è previsto il ricorso alla tecnologia di riconoscimento facciale («FRT»), nonché maggiori informazioni sulle misure organizzative e tecniche di cui tenere conto durante l'implementazione del progetto, e non deve essere considerato un elenco esaustivo di passaggi/misure da adottare. Dovrebbe essere considerato anche unitamente alle Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video ([69]) e a qualsiasi regolamento UE/SEE, nonché alle Linee guida dell'EDPB relative all'uso dell'intelligenza artificiale.

Il presente allegato fornisce orientamenti basati sul presupposto che le autorità di contrasto acquisiscano la tecnologia di riconoscimento facciale (come prodotto in serie). Se la LEA prevede di sviluppare (addestrare ulteriormente) la FRT, si applicano ulteriori requisiti per la selezione degli insiemi di dati necessari per l'addestramento, la prova e la convalida da usare durante lo sviluppo e dei ruoli/misure per l'ambiente di sviluppo. Analogamente, un prodotto in serie può richiedere ulteriori adeguamenti per l'uso previsto, nel qual caso occorre soddisfare i requisiti summenzionati per la selezione degli insiemi di dati per la prova, la convalida e l'addestramento.

L'appartenenza alla stessa LEA non implica di per sé il pieno accesso ai dati biometrici. Come avviene con qualsiasi altra categoria di dati personali, i dati biometrici raccolti per una determinata finalità di contrasto secondo una specifica base giuridica non si possono utilizzare senza un'adeguata base giuridica per una finalità di contrasto diversa [articolo 4, paragrafo 2, della direttiva (UE) 2016/680 (direttiva LED)]. Inoltre si ritiene che lo sviluppo/l'addestramento di uno strumento FRT costituisca una finalità diversa e si dovrebbe valutare se il trattamento dei dati biometrici per misurare le prestazioni/addestrare la tecnologia in modo da evitare un impatto sugli interessati a causa di prestazioni scadenti sia necessario e proporzionato, tenendo conto della finalità iniziale del trattamento.

1. RUOLI E RESPONSABILITÀ

Quando un'autorità di contrasto ricorre alla FRT per svolgere i propri compiti che rientrano nell'ambito di applicazione della direttiva LED (prevenzione, indagine, accertamento o perseguimento di reati, ecc., a norma dell'articolo 3 della direttiva LED), può essere considerata titolare del trattamento per la FRT. Tuttavia, le autorità di contrasto sono composte da diverse unità/dipartimenti che possono essere coinvolti nel trattamento, sia definendo il processo di applicazione della FRT, sia applicandolo nella pratica. A causa delle specificità di questa tecnologia, potrebbe rendersi necessario coinvolgere diverse unità per fornire assistenza nelle misurazioni delle sue prestazioni o per addestrare ulteriormente la tecnologia stessa.

In un progetto in cui è previsto il ricorso alla FRT è possibile che siano coinvolte diverse parti interessate ([70]) all'interno delle LEA:

([69]) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

([70]) I ruoli seguenti sono indicativi delle diverse parti interessate e delle loro responsabilità in un progetto FRT. Benché il linguaggio utilizzato per descrivere i ruoli nel presente allegato non sia consolidato, ciascuna autorità

- Alta dirigenza: per approvare il progetto dopo aver soppesato i rischi rispetto ai potenziali benefici.
- Responsabile della protezione dei dati e/o ufficio legale dell'autorità di contrasto: per fornire assistenza nella valutazione della legittimità dell'attuazione di un determinato progetto FRT e nell'esecuzione della DPIA, nonché per garantire il rispetto e l'esercizio dei diritti degli interessati.
- Titolare del processo: agisce in veste di unità specifica all'interno dell'autorità di contrasto competente per sviluppare il progetto FRT e stabilirne i dettagli, tra cui i requisiti di prestazione del sistema, decidere in merito all'adeguata metrica di equità, definire il punteggio di confidenza ([71]); fissa soglie accettabili per le distorsioni, individua i potenziali rischi posti dal progetto FRT per i diritti e le libertà delle persone (consultando anche il responsabile della protezione dei dati e il dipartimento informatico di IA e/o di scienza dei dati, cfr. infra) e li sottopone all'alta dirigenza. Il titolare del processo consulterà anche il gestore della banca dati di riferimento, prima di decidere in merito ai dettagli del progetto FRT, per comprendere sia la finalità d'uso della banca dati di riferimento che i relativi dettagli tecnici. In caso di riaddestramento di una tecnologia di riconoscimento facciale (FRT) acquisita tramite appalto, anche il titolare del processo sarà responsabile della selezione dell'insieme di dati per l'addestramento. Il titolare del processo, essendo l'unità incaricata di elaborare e stabilire i dettagli del progetto, è altresì responsabile della conduzione della DPIA.
- Dipartimento informatico di IA e/o di scienza dei dati: per fornire assistenza nell'esecuzione di una DPIA, spiegare i parametri disponibili per misurare la prestazione, l'equità ([72]) e le potenziali distorsioni del sistema, attuare la tecnologia e le garanzie tecniche, al fine di impedire l'accesso non autorizzato ai dati raccolti, gli attacchi informatici, ecc. In caso di riaddestramento di una FRT acquisita tramite appalto, il dipartimento informatico di IA o di scienza dei dati addestrerà il sistema in base all'insieme di dati fornito dal titolare del processo. Questo dipartimento sarà inoltre incaricato di definire le misure volte a mitigare i rischi individuati congiuntamente dai titolari dei processi (ad esempio, rischi specifici dell'IA, come gli attacchi di deduzione ai modelli).
- Utenti finali (quali agenti di polizia sul campo o in laboratori forensi): per effettuare un confronto con la banca dati, esaminare criticamente i risultati tenendo conto degli elementi di prova raccolti in precedenza e fornire un riscontro al titolare del processo in merito ai falsi positivi e alle indicazioni di possibili discriminazioni.
- Gestore della banca dati di riferimento: è l'unità specifica in seno all'autorità di contrasto competente incaricata di popolare e gestire la banca dati di riferimento (ossia quella con cui saranno confrontate le immagini), nonché di cancellare di immagini facciali dopo il periodo di conservazione definito. La banca dati in questione può essere creata specificamente per il progetto FRT previsto o essere preesistente per finalità compatibili; Il suo gestore ha il compito di definire quando e in quali circostanze le immagini facciali possano essere conservate, nonché di stabilire i propri requisiti di conservazione dei dati (in base al tempo o ad altri criteri).

Poiché la maggior parte dei casi di diffusione e utilizzo della FRT comporta un rischio intrinseco elevato per i diritti e le libertà degli interessati, dovrebbe essere coinvolta anche l'autorità di controllo della

di contrasto deve definire e assegnare ruoli simili a seconda della propria organizzazione. Potrebbe accadere che un'unità assommi più di un ruolo, ad esempio il titolare del processo e il gestore della banca dati di riferimento, o il titolare del processo e il dipartimento informatico di IA e/o di scienza dei dati (nel caso in cui l'unità del titolare del processo disponga di tutte le conoscenze tecniche necessarie).

([71]) Il punteggio di confidenza è l'intervallo di confidenza della previsione (riscontro), espresso sotto forma di probabilità: per esempio, confrontando due modelli, c'è una probabilità del 90 % che appartengano alla stessa persona. Il punteggio di confidenza è diverso dalla prestazione della FRT, ma la influenza. Più alta è la soglia di confidenza, minore è il numero di falsi positivi e di falsi negativi presenti nei risultati della FRT.

([72]) L'equità può essere definita come l'assenza di discriminazioni ingiuste e illecite, quali distorsioni di genere o di razza.

protezione dei dati nel contesto della consultazione preventiva prescritta dall'articolo 28 della direttiva LED.

2. AVVIO/FASE PRECEDENTE ALL'ACQUISIZIONE DEL SISTEMA FRT

Il titolare del processo nell'ambito di un'autorità di contrasto dovrebbe innanzitutto conoscere in modo chiaro il processo o i processi che perseguono il ricorso all'FTT (il caso/i casi d'uso) e garantire l'esistenza di una base giuridica per giustificare il caso d'uso previsto. In base a ciò, il titolare del processo è tenuto a svolgere i compiti che seguono.

- Descrivere formalmente il caso d'uso. Occorre descrivere il problema da risolvere e il modo in cui la FRT fornirà una soluzione, nonché una panoramica della procedura (compito) in cui la tecnologia sarà applicata. A questo proposito, le autorità di contrasto dovrebbero documentare quanto meno gli aspetti seguenti ([73]):
  - le categorie di dati personali registrati nella procedura;
  - gli obiettivi e le finalità concrete per cui si ricorrerà alla FRT, comprese le potenziali conseguenze per l'interessato dopo un riscontro;
  - le tempistiche e le modalità di acquisizione delle immagini facciali (comprese le informazioni sul contesto di tale acquisizione, ad esempio presso il gate dell'aeroporto, i video delle telecamere di sicurezza fuori da un negozio in cui è stato commesso un reato, ecc. e le categorie di interessati dei quali saranno trattati i dati biometrici);
  - la banca dati con cui verranno confrontate le immagini (banca dati di riferimento), nonché informazioni su come è stata realizzata, sulle sue dimensioni e sulla qualità dei dati biometrici che contiene;
  - gli attori delle LEA che saranno autorizzati a utilizzare il sistema FRT e ad agire di conseguenza nell'ambito delle attività di contrasto (i loro profili e diritti di accesso devono essere definiti dal titolare del processo);
  - il periodo di conservazione previsto per i dati in ingresso o il momento in cui si concluderà tale periodo (come la chiusura o la cessazione del procedimento penale, in conformità al diritto procedurale nazionale, per cui i dati sono stati inizialmente raccolti), nonché qualsiasi azione successiva (cancellazione di tali dati, anonimizzazione e utilizzo a fini statistici o di ricerca, ecc.);
  - implementazione delle registrazioni e accessibilità dei registri e delle registrazioni conservate;
  - le metriche di prestazione (ad esempio accuratezza, precisione, recupero, F1 score) e le loro soglie minime accettabili ([74]);
  - una stima del numero di persone che saranno sottoposte alla FRT e in quale periodo di tempo/circostanza.

([73]) L'allegato I fornisce un elenco di elementi per aiutare il titolare del trattamento a descrivere un caso d'uso della FRT.

([74]) Esistono diverse metriche per valutare le prestazioni di un sistema FRT. Ogni fornisce una visione diversa dei risultati del sistema e la sua capacità di indicare adeguatamente se il sistema FRT funzioni bene dipende dal caso d'uso della FRT. Se si pone l'accento sul raggiungimento di percentuali elevate di corrispondenza corretta di un volto, si potrebbero utilizzare metriche quali la precisione e il recupero; tuttavia, tali metriche non misurano la qualità di gestione degli esempi negativi da parte della FRT (ossia il numero di corrispondenze errate effettuate dal sistema). Il titolare del processo, assistito dal dipartimento informatico di IA e di scienza dei dati, deve essere in grado di stabilire i requisiti di prestazione e di esprimerli nella metrica più adatta in base al caso d'uso della FRT.

- Eseguire una valutazione della necessità e della proporzionalità ([75]). l'esistenza di questa tecnologia non giustifica necessariamente la sua applicazione: il titolare del processo deve innanzitutto valutare se esista una base giuridica adeguata per il trattamento previsto; a tal fine, è necessario consultare il responsabile della protezione dei dati e il servizio giuridico. Il motivo per avvalersi della FRT dovrebbe essere principalmente il fatto che questa tecnologia è una soluzione necessaria e proporzionata a un problema specificamente definito delle autorità di contrasto e questo aspetto deve essere valutato in base alla finalità/alla gravità del reato/al numero di persone non coinvolte ma interessate dal sistema FRT. Ai fini della valutazione della liceità occorre considerare almeno i seguenti elementi: la direttiva LED ([76]), il RGPD ([77]) ([78]), qualsiasi quadro giuridico esistente in materia di IA ([79]) e tutti gli orientamenti di accompagnamento forniti dalle autorità di controllo della protezione dei dati [come ad esempio le Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video ([80])]. Questi atti legislativi dell'UE dovrebbero sempre essere corroborati dai requisiti nazionali applicabili, specialmente nell'ambito del diritto procedurale penale. La valutazione della proporzionalità dovrebbe individuare i diritti fondamentali degli interessati che rischiano di essere lesi (al di là della privacy e della protezione dei dati), oltre a descrivere e considerare eventuali limiti (o la loro assenza) imposti nel caso d'uso al sistema FRT, indicando per esempio se il sistema funzionerà in modo continuo o temporaneo e se si limiterà a una zona geografica.
- Effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) ([81]). Su dovrebbe eseguire una DPIA poiché il ricorso alla FRT nel settore delle attività di contrasto comporta tendenzialmente un rischio elevato per i diritti e le libertà delle persone ([82]). La DPIA dovrebbe includere in particolare una descrizione generale dei trattamenti previsti ([83]), una valutazione dei

([75]) Per tenere conto della necessità si possono prendere in considerazione ulteriori provvedimenti in merito all'adattamento e all'utilizzo del sistema, affinché si possa modificare lievemente anche la descrizione del caso d'uso durante la valutazione della necessità e della proporzionalità.
([76]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
([77]) Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
([78]) Qualora un progetto scientifico inteso a condurre ricerche sull'uso della FRT debba trattare dati personali, ma tale trattamento non rientri nell'ambito di applicazione dell'articolo 4, paragrafo 3, della direttiva LED, sarebbe applicabile in generale il RGPD (articolo 9, paragrafo 2, della direttiva LED). Nel caso di progetti pilota eventualmente seguiti da operazioni di contrasto, la direttiva LED sarebbe comunque applicabile.
([79]) Esiste per esempio una proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE, che tuttavia non è ancora stata approvata.
([80]) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
([81]) Ulteriori orientamenti sulle DPIA sono disponibili nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679, WP 248 rev.01, disponibile all'indirizzo: https://ec.europa.eu/newsroom/article29/items/611236 e nel kit di strumenti del GEPD Responsabilità sul campo (parte II), disponibile all'indirizzo: https://edps.europa.eu/node/4582_en
([82]) La FRT, a seconda del caso d'uso, può rientrare nei seguenti criteri che determinano il trattamento a rischio elevato (tratti dalle Linee guida in materia di valutazione d'impatto sulla protezione dei dati, WP 248 rev.01): monitoraggio sistematico, trattamento di dati su vasta scala, creazione di corrispondenze o combinazione di insiemi di dati, uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative.
([83]) Anche la descrizione del trattamento e la valutazione della necessità e della proporzionalità, come già descritto nelle fasi precedenti, fanno parte della DPIA, eccezion fatta per la valutazione del rischio. Se necessario, nella DPIA sarà fornita una descrizione più dettagliata dei flussi di dati personali.

rischi per i diritti e le libertà degli interessati ([84]), le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità. Poiché la DPIA è un processo continuo, occorre aggiungere qualsiasi nuovo elemento del trattamento e aggiornare la valutazione del rischio in ogni fase del progetto.

- Ottenere l'approvazione dell'alta dirigenza spiegando i rischi per i diritti e le libertà degli interessati (dovuti al caso d'uso e alla tecnologia) e i rispettivi piani di trattamento dei rischi.

3. DURANTE L'APPALTO E PRIMA DELL'UTILIZZO DELLA FRT

- Decidere i criteri per selezionare la FRT (algoritmo). Il titolare del processo dovrebbe decidere i criteri di selezione di un algoritmo con l'aiuto del dipartimento informatico di IA e/o di scienza dei dati. In pratica, tali criteri includerebbero l'equità e le metriche di prestazione stabilite nella descrizione del caso d'uso e dovrebbero includere anche informazioni relative ai dati con cui è stato addestrato l'algoritmo. Gli insiemi di dati per l'addestramento, la prova e la convalida devono includere campioni sufficienti di tutte le caratteristiche degli interessati da sottoporre alla FRT (tenendo conto per esempio dell'età, del genere e della razza) per ridurre eventuali distorsioni. Il fornitore della FRT dovrebbe rendere disponibili informazioni e metriche sugli insiemi di dati per l'addestramento, la prova e la convalida della FRT, nonché descrivere le misure adottate per misurare e mitigare potenziali discriminazioni e distorsioni illecite. Il titolare del processo, ove possibile, è tenuto a verificare se esista una base giuridica tale da consentire al fornitore di utilizzare l'insieme di dati in questione al fine di addestrare gli algoritmi (in base alle informazioni che il fornitore metterà a disposizione). Inoltre il titolare del processo dovrebbe garantire che il fornitore della FRT applichi norme di sicurezza relative ai dati biometrici (per esempio ISO/IEC 24745), che forniscono orientamenti per la protezione delle informazioni biometriche in base a vari requisiti di riservatezza, integrità e rinnovabilità/revocabilità in fase di conservazione e trasmissione, nonché requisiti e linee guida affinché le informazioni biometriche vengano gestite e trattate in modo sicuro e rispettoso della vita privata.

- Riaddestrare l'algoritmo (se necessario). Il titolare del processo dovrebbe garantire che i servizi acquisiti in appalto comprendano anche la messa a punto del sistema FRT per conseguire un'accuratezza maggiore prima del suo utilizzo. Qualora si renda un addestramento supplementare del sistema FRT acquisito per soddisfare i parametri di accuratezza, il titolare del processo, oltre a prendere la decisione di procedere al riaddestramento, deve stabilire, con l'aiuto del dipartimento informatico di IA e/o di scienza dei dati, l'insieme di dati adeguato e rappresentativo da impiegare e verificare la liceità di tale utilizzo in relazione ai dati.
- Definire le opportune garanzie per far fronte ai rischi connessi alla sicurezza, alle distorsioni e alle basse prestazioni. Tale compito comprende l'istituzione di una procedura per monitorare la FRT una volta in uso (registrazione e feedback sull'accuratezza e la correttezza dei risultati). Inoltre occorre garantire che siano individuati, misurati e mitigati i rischi specifici di alcuni sistemi di apprendimento automatico e sistemi FRT (per esempio l'avvelenamento dei dati, esempi antagonistici, l'inversione del modello, attacchi white-box). Il titolare del processo dovrebbe inoltre stabilire garanzie adeguate per assicurare il rispetto dei requisiti di conservazione dei dati biometrici inclusi nell'insieme di dati per il riaddestramento.

([84]) L'analisi dei rischi per gli interessati dovrebbe includere i rischi relativi al luogo in cui devono essere confrontate le immagini facciali (locale/remoto), i rischi relativi ai responsabili/sub-responsabili del trattamento, nonché quelli specifici per l'apprendimento automatico nei casi in cui viene applicato (tra cui l'avvelenamento dei dati e gli esempi antagonistici).

- Documentare il sistema FRT. Questo compito dovrebbe includere una descrizione generale del sistema FRT, una descrizione dettagliata degli elementi dei suoi elementi e del processo per istituirlo, informazioni particolareggiate sul monitoraggio, sul funzionamento e sul controllo del sistema FRT nonché una descrizione dettagliata dei rischi e delle misure di attenuazione. Gli elementi inclusi in questa documentazione comprenderanno quelli principali della descrizione del sistema FRT desunta dalle fasi precedenti (cfr. supra), che tuttavia saranno arricchiti con informazioni relative al monitoraggio delle prestazioni e all'applicazione di modifiche al sistema, inclusi eventuali aggiornamenti della versione e/o del riaddestramento.
- Redigere manuali utente per spiegare la tecnologia e i casi d'uso. I manuali devono spiegare in modo chiaro tutti gli scenari e i prerequisiti nell'ambito dei quali si ricorrerà alla FRT.
- Impartire una formazione agli utenti finali sulle modalità di utilizzo della tecnologia. Tali corsi di formazione devono spiegare le capacità e i limiti della tecnologia, affinché gli utenti possano comprendere le circostanze in cui è necessario applicarla e i casi in cui può essere inaccurata, e contribuiranno altresì a mitigare i rischi connessi alla mancata verifica/analisi critica dell'esito dell'algoritmo.
- Consultare l'autorità di controllo della protezione dei dati, a norma dell'articolo 28, paragrafo 1, lettera b), della direttiva LED. Fornire informazioni, ai sensi dell'articolo 13 della direttiva LED, per informare gli interessati in merito al trattamento e ai loro diritti. Occorre trasmettere queste comunicazioni agli interessati in un linguaggio appropriato, affinché possano comprendere il trattamento, spiegando gli elementi di base della tecnologia tra cui i tassi di accuratezza, gli insiemi di dati per l'addestramento e le misure adottate per evitare la discriminazione e la scarsa accuratezza dell'algoritmo.

4. RACCOMANDAZIONI DOPO L'UTILIZZO DELLA FRT

- Garantire l'intervento umano e la sorveglianza dei risultati. Non adottare mai alcuna misura relativa a una persona fisica esclusivamente sulla base dell'esito della FRT (ciò implicherebbe una violazione dell'articolo 11 della direttiva LED - Processo decisionale automatizzato relativo alle persone fisiche con effetti giuridici o di altro tipo sull'interessato). Garantire che un funzionario delle autorità di contrasto esamini i risultati della FRT e che gli utenti di tali autorità evitino di incorrere nelle distorsioni dell'automazione, indagando su informazioni contraddittorie e contestando criticamente i risultati della tecnologia. A tal fine, la formazione permanente e la sensibilizzazione degli utenti finali sono importanti, ma l'alta dirigenza dovrebbe garantire la presenza di risorse umane adeguate per svolgere una sorveglianza efficace: ne consegue che si deve concedere a ciascun agente tempo a sufficienza per contestare criticamente i risultati della tecnologia. Registrare, misurare e valutare in quale misura la sorveglianza umana modifichi la decisione originaria della FRT.
- Monitorare e contrastare la deriva del modello FRT (degradazione delle prestazioni) una volta che il modello sia in fase di produzione.
- Istituire una procedura per valutare nuovamente i rischi e le misure di sicurezza periodicamente e ogni volta in cui la tecnologia o il caso d'uso sono sottoposti a modifiche.
- Documentare qualsiasi modifica apportata al sistema nel corso di tutto il suo ciclo di vita (per esempio aggiornamenti, riqualificazione).
- Istituire una procedura e le relative capacità tecniche per soddisfare le richieste di accesso degli interessati. Occorre predisporre la capacità tecnica per l'estrazione dei dati, qualora fosse necessario fornirli agli interessati, prima che venga presentata qualsiasi richiesta.
- Garantire che siano previste procedure in caso di violazione dei dati. Se si verifica una violazione dei dati personali che riguarda dati biometrici, i rischi sono probabilmente elevati. In tal caso, tutti gli utenti coinvolti dovrebbero conoscere le pertinenti procedure da seguire e il responsabile della protezione dei dati dovrebbe essere immediatamente informato, al pari degli interessati.

ALLEGATO III - ESEMPI PRATICI

Esistono molti contesti pratici e finalità differenti per l'utilizzo del riconoscimento facciale, per esempio in ambienti controllati come quelli dei valichi di frontiera, controlli incrociati con dati provenienti dalle banche dati della polizia o dati personali resi manifestamente pubblici dall'interessato, flussi video dal vivo (riconoscimento facciale in diretta), ecc. Di conseguenza, i rischi per la protezione dei dati personali e di altri diritti e libertà fondamentali variano considerevolmente a seconda dei vari casi d'uso. Al fine di agevolare la valutazione della necessità e della proporzionalità, che dovrebbe precedere la decisione in merito all'eventuale impiego del riconoscimento facciale, le attuali linee guida forniscono un elenco non esaustivo delle possibili applicazioni della FRT nel settore delle attività di contrasto.

Gli scenari presentati e valutati si basano su situazioni **ipotetiche** e hanno la finalità di illustrare alcuni usi concreti della FRT, fornire assistenza per gli esami caso per caso nonché definire un quadro generale; non hanno la pretesa di essere esaustivi né pregiudicano eventuali procedimenti in corso o futuri avviati da un'autorità nazionale di controllo in merito alla progettazione, alla sperimentazione o all'implementazione di tecnologie di riconoscimento facciale. La presentazione di questi scenari dovrebbe servire soltanto allo scopo di esemplificare gli orientamenti per i responsabili politici, i legislatori e le autorità di contrasto, già forniti nel presente documento, nel momento in cui si concepisce e si prevede l'attuazione di tecnologie di riconoscimento facciale per garantire la piena conformità all'acquis dell'UE in materia di protezione dei dati personali. In tale contesto occorre tenere presente che, anche in situazioni analoghe in cui si ricorre alla FRT, la presenza o l'assenza di alcuni elementi può determinare un esito diverso per la valutazione della necessità e della proporzionalità.

1 SCENARIO 1

1.1. Descrizione

Un sistema di controllo automatizzato delle frontiere che, autenticando l'immagine biometrica memorizzata nel documento di viaggio elettronico dei cittadini dell'UE e di altri viaggiatori che varcano il confine e accertando che il passeggero è il legittimo titolare del documento, consente l'attraversamento automatizzato della frontiera.

Tale verifica/autenticazione prevede solo il riconoscimento facciale 1:1 e viene effettuata in un ambiente controllato (ad esempio presso i varchi automatici degli aeroporti). I dati biometrici del viaggiatore che attraversa la frontiera vengono acquisiti quando questi viene esplicitamente invitato a guardare la telecamera del varco automatico e i dati suddetti vengono confrontati con quelli del documento presentato (passaporto, carta d'identità, ecc.), che viene rilasciato in base a specifici requisiti tecnici.

Contestualmente, benché in tali casi il trattamento esuli in linea di principio dall'ambito di applicazione della direttiva LED, l'esito della verifica può servire anche per confrontare i dati (alfanumerici) della persona con le banche dati delle autorità di contrasto nel quadro del controllo di frontiera e, pertanto, può comportare provvedimenti con effetti giuridici significativi per l'interessato, per esempio l'arresto in seguito a una segnalazione nel SIS (sistema d'informazione Schengen). In determinate circostanze, i dati biometrici possono essere utilizzati anche per la ricerca di corrispondenze nelle banche dati delle autorità di contrasto (in tal caso, in questa fase si effettuerebbe l'identificazione 1:molti).

L'esito del trattamento biometrico dell'immagine ha un impatto diretto sull'interessato, perché gli consente di varcare la frontiera soltanto se la verifica ha esito positivo. In caso di mancata

identificazione, le guardie di frontiera devono effettuare un secondo controllo per accertare che l'interessato non sia la persona indicata nel documento di identificazione.

Se viene individuata una segnalazione nel SIS o a livello nazionale, le guardie di frontiera devono effettuare una seconda verifica e gli ulteriori controlli necessari e, successivamente, adottare tutti i provvedimenti del caso, per esempio arrestare la persona e informare le autorità interessate.

Fonte delle informazioni:

- Tipi di interessati: ☒ tutte le persone che attraversano le frontiere
- Fonte dell'immagine:☒ altro (documento d'identità)
- Collegamento con il reato: ☒ non necessario
- Modalità di acquisizione delle informazioni: ☒ in una cabina o in un ambiente controllato
- Contesto: incidenza su altri diritti fondamentali: sì, in particolare: ☒ diritto di libera circolazione ☒ diritto di asilo

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità: ☒ banche dati specifiche relative al controllo delle frontiere

Algoritmo:

- Tipo di verifica: ☒ verifica (autenticazione) 1:1

Esito:

- Impatto ☒ diretto (si consente o si nega l'ingresso all'interessato)
- Decisione automatizzata: ☒ sì

1.2. Quadro giuridico applicabile

Dal 2004, ai sensi del regolamento (CE) n. 2252/2004 del Consiglio ([85]), i passaporti e gli altri documenti di viaggio rilasciati dagli Stati membri devono contenere un'immagine biometrica del volto memorizzata in un chip elettronico incorporato nel documento.

Il codice frontiere Schengen (CFS) ([86]) stabilisce i requisiti per i controlli sulle persone alle frontiere esterne. Per i cittadini dell'UE e le altre persone che godono del diritto di libera circolazione ai sensi del diritto dell'Unione, i controlli minimi dovrebbero consistere in una verifica dei documenti di viaggio, se del caso tramite dispositivi tecnici. Il codice frontiere Schengen è stato successivamente modificato con il regolamento (UE) 2017/2225 ([87]), che ha introdotto, tra l'altro, le definizioni di «varchi automatici», «sistema di controllo di frontiera automatizzato» e «sistema self-service», nonché la possibilità di trattare i dati biometrici per effettuare le verifiche di frontiera.

Si può quindi presumere che esista una base giuridica chiara e prevedibile che autorizza questa forma di trattamento dei dati personali. Inoltre il quadro giuridico è adottato a livello dell'Unione ed è direttamente applicabile agli Stati membri.

([85]) REGOLAMENTO (CE) N. 2252/2004 DEL CONSIGLIO, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri.

([86]) Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen).

([87]) Regolamento (UE) 2017/2225 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che modifica il regolamento (UE) 2016/399 per quanto riguarda l'uso del sistema di ingressi/uscite.

1.3. Necessità e proporzionalità: finalità/gravità del reato

Nell'ambito di un controllo di frontiera automatizzato, la verifica dell'identità dei cittadini dell'UE tramite la loro immagine biometrica è un elemento dei controlli alle frontiere esterne dell'UE e di conseguenza è collegato direttamente alla sicurezza delle frontiere, perseguendo un obiettivo di interesse generale riconosciuto dall'Unione. In aggiunta, le porte di controllo automatizzate alle frontiere contribuiscono a velocizzare le operazioni relative ai passeggeri e a ridurre il rischio di errori umani. Inoltre l'ambito, la portata e l'intensità dell'ingerenza in questo scenario sono molto più limitati rispetto ad altre forme di riconoscimento facciale. Tuttavia, il trattamento dei dati biometrici genera ulteriori rischi per gli interessati, rischi che devono essere affrontati e attenuati in modo adeguato dall'autorità competente che utilizza e gestisce la FRT.

1.4. Conclusioni

La verifica dell'identità dei cittadini dell'UE nel contesto di un controllo automatizzato alle frontiere è una misura necessaria e proporzionata, a condizione che siano in atto garanzie adeguate, in particolare l'applicazione dei principi di limitazione delle finalità, qualità dei dati, trasparenza e un elevato livello di sicurezza.

2 SCENARIO 2

2.1. Descrizione

Le autorità di contrasto istituiscono un sistema di identificazione delle vittime di sottrazione di minori. Un agente di polizia autorizzato può confrontare, a condizioni rigorose, i dati biometrici di un minore (del quale si sospetta il rapimento) con una banca dati delle vittime di sottrazione di minori, al solo fine di identificare quelli che possono corrispondere alla descrizione del minore scomparso per il quale è stata avviata un'indagine ed è stata effettuata la segnalazione.

Il trattamento in questione consisterebbe nel confronto tra il volto o l'immagine di una persona, che può corrispondere alla descrizione di un minore scomparso, e le immagini memorizzate nella banca dati; tale trattamento si effettuerebbe in casi specifici e non in modo sistematico.

La banca dati con cui si eseguirà il confronto è popolata da immagini di minori scomparsi in relazione a cui è stato segnalato il sospetto che siano stati rapiti o sia stata minacciata la loro vita o la loro integrità fisica, è stata avviata un'indagine penale sotto la supervisione di un'autorità giudiziaria ed è stata emessa una segnalazione di sottrazione di minore. I dati vengono acquisiti nel quadro delle procedure istituite dall'autorità di contrasto competente, ossia gli agenti di polizia autorizzati a svolgere missioni di polizia giudiziaria. Le categorie di dati personali registrati sono:

- identità, soprannome, alias, filiazione, nazionalità, indirizzi, indirizzi di posta elettronica, numeri di telefono;
- data e luogo di nascita;
- informazioni sulla parentela;
- fotografia con caratteristiche tecniche che consentono di utilizzare un dispositivo di riconoscimento facciale e altre fotografie.

I risultati del confronto devono inoltre essere esaminati e verificati da un funzionario autorizzato, al fine di confermare le prove precedenti con l'esito del confronto ed escludere eventuali risultati falsi positivi.

Le immagini e i dati personali dei minori possono essere conservati solo per la durata della segnalazione e devono essere cancellati immediatamente dopo la chiusura o la conclusione del procedimento penale, conformemente alle procedure nazionali per cui sono stati inseriti nella banca dati.

Per quanto si possa preventivare un periodo di durata relativamente lunga e definito in conformità del diritto nazionale per la conservazione dei dati biometrici nella banca dati, l'esercizio dei diritti degli interessati, in particolare del diritto di rettifica e cancellazione, prevede un'ulteriore garanzia per limitare l'ingerenza nel diritto alla protezione dei dati personali degli interessati.

Fonte delle informazioni:

- Tipi di interessati: ☒ Minori
- Fonte dell'immagine ☒ altro: non predefinita, presunta vittima di rapimento di minore
- Collegamento con il reato ☒ Temporale non diretto ☒ Geografico non diretto
- Modalità di acquisizione delle informazioni: ☒ in una cabina o in un ambiente controllato
- Contesto: incidenza su altri diritti fondamentali☒ Sì, in particolare:☒ vari

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità ☒ banca dati specifica

Algoritmo:

- Tipo di verifica: ☒ identificazione 1:molti

Esito:

- Impatto ☒ Diretto
- Decisione automatizzata: ☒ NO, revisione obbligatoria a cura di un funzionario autorizzato

Analisi giuridica:

- Quadro giuridico applicabile:☒ Normativa nazionale specifica per questo trattamento (riconoscimento facciale)

2.2. Quadro giuridico applicabile

Il diritto nazionale prevede un quadro giuridico ad hoc che istituisce la banca dati e determina le finalità del trattamento, nonché i criteri per il popolamento, l'accesso e l'utilizzo della banca dati. Le misure legislative necessarie per la sua attuazione prevedono anche la determinazione di un periodo di conservazione e il riferimento ai principi applicabili di integrità e riservatezza, oltre alle modalità per la fornitura di informazioni all'interessato (e, in tal caso, al titolare o ai titolari della responsabilità genitoriale) nonché quelle per l'esercizio dei diritti dell'interessato e, se del caso, l'eventuale limitazione. Durante la preparazione della proposta della rispettiva misura legislativa, è stato necessario consultare l'autorità nazionale di controllo.

2.3. Necessità e proporzionalità: finalità/gravità del reato/numero di persone non coinvolte ma interessate dal trattamento

Condizioni e garanzie per il trattamento

Il confronto per il riconoscimento facciale può essere effettuato da un funzionario autorizzato solo in ultima istanza, a meno che non siano disponibili altri mezzi meno intrusivi e solo se strettamente necessario, per esempio nel caso in cui sussista un dubbio sull'autenticità del documento di identità di un minore in viaggio e/o in seguito all'esame di prove e materiale acquisiti in precedenza che indichino

una possibile corrispondenza con la descrizione di un minore scomparso in relazione a cui è in corso un'indagine penale.

La revisione e la verifica obbligatorie del confronto per il riconoscimento facciale, eseguite da un funzionario autorizzato, costituiscono un'ulteriore garanzia al fine di confermare le prove precedenti con l'esito del confronto ed escludere eventuali risultati falsi positivi.

Obiettivo perseguito

L'istituzione della banca dati serve a conseguire importanti obiettivi di interesse pubblico generale, in particolare la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali, nonché la tutela dei diritti e delle libertà altrui. A quanto sembra, l'istituzione della banca dati e il trattamento previsto contribuiscono all'identificazione dei minori vittime di rapimento e si possono considerare misure idonee a sostenere l'obiettivo legittimo di indagare e perseguire tali reati.

Finalità e popolazione della banca dati

Le finalità del trattamento sono chiaramente definite dalla legge e la banca dati verrà utilizzata solo per identificare minori scomparsi per i quali è stato segnalato il sospetto che siano stati rapiti ed è stata avviata un'indagine penale sotto la supervisione di un'autorità giudiziaria e per cui è stata emessa una segnalazione di sottrazione di minore. Le condizioni stabilite dalla legge per la popolazione della banca dati mirano a limitare rigorosamente il numero degli interessati e dei dati personali da includere nella stessa. Il titolare della responsabilità genitoriale nei confronti del minore deve essere informato in merito al trattamento effettuato e alle condizioni per l'esercizio dei diritti del minore relativamente al trattamento biometrico previsto ai fini dell'identificazione o ai dati personali del minore memorizzati nella banca dati.

2.4. Conclusioni

Tenuto conto della necessità e della proporzionalità del trattamento previsto, nonché dell'interesse superiore del minore nel corso del trattamento in questione dei dati personali, e purché vi siano garanzie sufficienti per assicurare in particolare l'esercizio dei diritti degli interessati (considerando in particolare che devono essere trattati dati di minori), tale applicazione del trattamento del riconoscimento facciale può essere ritenuta probabilmente compatibile con il diritto dell'UE.

Inoltre, dato il tipo di trattamento e la tecnologia utilizzata, da cui deriva un rischio elevato per i diritti e le libertà degli interessati, l'EDPB ritiene che l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare, basata su tale atto legislativo relativamente al trattamento previsto, debba includere una consultazione preventiva dell'autorità di controllo per garantire la coerenza e la conformità con il quadro giuridico applicabile (cfr. articolo 28, paragrafo 2, della direttiva LED).

3 SCENARIO 3

3.1. Descrizione

Nel corso degli interventi di polizia in occasione di disordini e delle successive indagini, alcune persone sono state identificate come sospette, ad esempio grazie a indagini precedenti svolte mediante telecamere a circuito chiuso o testimoni, e le loro immagini vengono confrontate con altre immagini di persone che sono state riprese da telecamere a circuito chiuso o da dispositivi mobili sul luogo del reato o nelle zone circostanti.

Al fine di ottenere prove più dettagliate sulle persone sospettate di aver partecipato ai disordini che accompagnano una manifestazione, la polizia crea una banca dati costituita da immagini che hanno un nesso labile, dal punto di vista locale e temporale, con gli scontri avvenuti. La banca dati comprende registrazioni private caricate dai cittadini a beneficio della polizia, materiale proveniente dalle telecamere a circuito chiuso all'interno di trasporti pubblici, filmati di videosorveglianza di proprietà della polizia e materiale pubblicato dai media senza limitazioni né tutele specifiche di sorta. La presenza nelle immagini di comportamenti criminali gravi non è un prerequisito per la raccolta dei file nella banca dati. Pertanto, sono registrate nella banca dati immagini di persone non coinvolte nei disordini (una percentuale significativa della popolazione locale che passava di lì al momento della manifestazione o ha partecipato alla manifestazione, ma non ai disordini), per un totale di migliaia di file di video e immagini.

Usando un software di riconoscimento facciale, tutti i volti che compaiono in questi file vengono assegnati a ID facciali univoci. I volti di ogni persona sospetta vengono quindi confrontati automaticamente con questi ID e la banca dati costituita da tutti i modelli biometrici presenti nelle migliaia di file di video e immagini viene conservata fino a quando non si concludono tutte le possibili indagini. I funzionari responsabili esaminano le corrispondenze positive e in seguito decidono in merito a ulteriori provvedimenti da adottare, che possono includere l'attribuzione del file reperito nella banca dati al fascicolo penale della persona in questione nonché ulteriori misure, quali il suo interrogatorio o il suo arresto.

Una normativa nazionale prevede una disposizione generica in base a cui il trattamento dei dati biometrici al fine di identificare in modo univoco una persona fisica è ammissibile solo se è strettamente necessario ed è soggetto a garanzie adeguate per i diritti e le libertà della persona interessata.

Fonte delle informazioni:

- Tipi di interessati: ☒ tutte le persone
- Fonte dell'immagine: ☒ spazi accessibili al pubblico ☒ entità privata ☒ altre persone ☒ altro: media
- Collegamento con il reato: ☒ non necessariamente un collegamento geografico o temporale diretto
- Modalità di acquisizione delle informazioni: ☒ remota
- Contesto: incidenza su altri diritti fondamentali: sì, in particolare sulla ☒ libertà di riunione
- Ulteriori fonti di informazioni disponibili sull'interessato:
  ☒ altro: non si escludono (per esempio l'uso di bancomat o negozi in cui è entrato l'interessato), poiché non si può esercitare un controllo sulle intenzioni nelle immagini

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità: ☒ banche dati specifiche relative alla zona in cui è avvenuto il reato

Algoritmo:

- Tipo di trattamento: ☒ identificazione 1:molti

Esito:

- Impatto: ☒ diretto (ad es. l'interessato può essere arrestato, interrogato)
- Decisione automatizzata: ☒ NO
- Durata della conservazione: fino alla conclusione di tutte le possibili indagini

Analisi giuridica:

- Tipo di informazione preliminare all'interessato:☒ Sul sito web dell'autorità di contrasto in generale

- Quadro giuridico applicabile: ☒ Direttiva LED, ripresa in gran parte nel diritto nazionale ☒ Normativa nazionale generica per l'utilizzo di dati biometrici da parte delle autorità di contrasto

3.2. Quadro giuridico applicabile

Come spiegato più sopra, le basi giuridiche che si limitano a ripetere la clausola generale dell'articolo 10 della direttiva LED non sono sufficientemente chiare nella loro formulazione per fornire alle persone un'indicazione adeguata in merito alle condizioni e alle circostanze in cui le autorità di contrasto sono autorizzate a usare registrazioni, effettuate in spazi pubblici, di telecamere a circuito chiuso per creare un modello biometrico dei loro volti e confrontarlo con le banche dati della polizia, altre telecamere a circuito chiuso disponibili o registrazioni private, ecc. Pertanto il quadro giuridico istituito in questo scenario non soddisfa i requisiti minimi per costituire una base giuridica.

3.3. Necessità e proporzionalità

In questo esempio il trattamento suscita vari dubbi in base ai principi di necessità e proporzionalità per diversi motivi.

Le persone non sono sospettate di aver commesso un reato grave e la presenza nelle immagini di comportamenti criminali gravi non è un prerequisito per l'utilizzo dei file conservati nella banca dati che le contiene. Inoltre, un collegamento temporale e geografico diretto con il reato non è a sua volta un prerequisito per l'utilizzo dei file presenti nella banca dati; ne consegue che una percentuale considerevole della popolazione locale è registrata in una banca dati biometrica per una durata potenzialmente pluriennale, fino alla conclusione di tutte le indagini.

Poiché la banca dati relativa al luogo del reato non si limita alle immagini conformi ai requisiti di proporzionalità, ciò comporta una quantità illimitata di immagini da confrontare, in contrasto con il principio della minimizzazione dei dati. Una quantità inferiore di immagini consentirebbe inoltre di prendere in considerazione metodi non algoritmici e meno invasivi, come i super riconoscitori ([88]).

Poiché l'esempio è tratto da una zona in cui si è svolta una manifestazione e dai suoi dintorni, è altresì probabile che le immagini rivelino le opinioni politiche dei partecipanti, ossia la seconda categoria speciale di dati potenzialmente interessati in questo scenario, nel quale non è chiaro come si possa impedire l'acquisizione di tali dati e con quali garanzie. Inoltre, quando gli interessati apprendono di essere stati inseriti in una banca dati biometrica della polizia per aver partecipato a una manifestazione, ciò può comportare gravi effetti inibitori in futuro sull'esercizio del loro diritto di riunione.

Anche i modelli biometrici presenti nella banca dati si possono confrontare tra loro, consentendo alla polizia non solo di cercare una persona specifica all'interno di tutto il materiale di cui dispone, ma anche di ricreare il modello comportamentale di una persona nell'arco di diversi giorni, nonché di acquisire ulteriori informazioni sul suo conto, quali i contatti sociali e il coinvolgimento politico.

([88]) Ossia persone dotate di una straordinaria capacità di riconoscimento facciale. Cfr. anche: Face Recognition by Metropolitan Police Super-Recognisers, 26 febbraio 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

L'ingerenza è ulteriormente accentuata perché il trattamento dei dati avviene all'insaputa degli interessati.

Considerando che la gente scatta fotografie e registra video in continuazione, e che anche le riprese onnipresenti delle telecamere a circuito chiuso si possono analizzare sotto il profilo biometrico, ciò può causare gravi effetti inibitori.

Un altro motivo di preoccupazione è costituito dall'ampio utilizzo di fotografie e video privati, comprendente potenziali abusi come la delazione. Poiché gli abusi di questo tipo rappresentano un rischio inerente anche ai procedimenti penali in generale, tale rischio è considerevolmente più elevato per quanto concerne la scalabilità dei dati trattati e il numero delle persone coinvolte, poiché la gente potrebbe caricare anche materiale relativo a una persona specifica o a un gruppo di persone per cui prova antipatia. Il fatto che la polizia richieda alla gente di caricare fotografie e video può comportare soglie molto basse per la trasmissione del materiale da parte del pubblico, soprattutto perché il materiale potrebbe essere caricato in forma anonima o, quanto meno, senza che ci si debba presentare e identificare presso una stazione di polizia.

3.4. Conclusioni

Nel caso dell'esempio non esiste alcuna disposizione specifica che possa fungere da base giuridica. Tuttavia, anche in presenza di una base giuridica sufficiente, i requisiti di necessità e proporzionalità non sarebbero soddisfatti, comportando così un'ingerenza sproporzionata nei diritti dell'interessato al rispetto della vita privata e alla protezione dei dati personali ai sensi della Carta.

4 SCENARIO 4

4.1. Descrizione

La polizia adotta un metodo per identificare, mediante l'uso retrospettivo della FRT, le persone sospette che commettono un reato grave ripreso dalle telecamere a circuito chiuso. Nell'ambito di un'indagine preliminare, un funzionario seleziona manualmente l'immagine o le immagini di persone sospette nel materiale video che è stato raccolto sul luogo del reato o altrove e invia successivamente l'immagine o le immagini al dipartimento di medicina legale, che si avvale della FRT per abbinarle a immagini di persone che la polizia ha acquisito in precedenza in una banca dati (la cosiddetta banca dati descrittiva, costituita da persone sospette ed ex indagati). Quest'ultima viene analizzata con la FRT ai fini di questa procedura (temporaneamente e in un ambiente isolato) al fine di poter effettuare il processo di abbinamento. Per ridurre al minimo l'ingerenza nei diritti e negli interessi delle persone abbinate, solo un numero molto ridotto di dipendenti del dipartimento di medicina legale è autorizzato a condurre il processo di abbinamento effettivo, l'accesso ai dati è limitato ai funzionari cui è stato affidato il fascicolo specifico e si esegue un controllo manuale dei risultati prima di trasmettere qualsiasi risultato al funzionario incaricato delle indagini. I dati biometrici non vengono trasmessi al di fuori dell'ambiente controllato e isolato. Vengono ulteriormente utilizzati nell'indagine solo il risultato e l'immagine (non il modello biometrico). I dipendenti ricevono una formazione specifica sulle norme e sulle procedure per questa operazione e tutto il trattamento di dati personali e biometrici è sufficientemente trattato nel diritto nazionale.

Fonte delle informazioni:

- Tipi di interessati: ☒ persone sospette identificate attraverso le registrazioni di telecamere a circuito chiuso
- Fonte dell'immagine: ☒ spazi accessibili al pubblico ☒ internet

- Collegamento con il reato: ☒ temporale diretto
  ☒ Geografico diretto

- Modalità di acquisizione delle informazioni: ☒ remota
- Contesto: incidenza su altri diritti fondamentali: Sì, in particolare: ☒ Libertà di riunione ☒ Libertà di parola ☒ vari: __

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità: ☒ banche dati specifiche relative alla zona in cui è avvenuto il reato

Algoritmo:

- Tipo di trattamento☒ identificazione 1:molti

Esito:

- Impatto: ☒ diretto (per esempio l'interessato viene arrestato e interrogato)
- Decisione automatizzata: ☒ NO

Analisi giuridica:

- Quadro giuridico applicabile:☒ Normativa nazionale specifica per questo trattamento (riconoscimento facciale) per l'autorità competente in questione

4.2. Quadro giuridico applicabile

In questo scenario, la normativa nazionale specifica che i dati biometrici si possono utilizzare per condurre analisi forensi quando ciò è strettamente necessario per conseguire la finalità di identificare, tramite l'abbinamento delle immagini nella banca dati descrittiva, le persone sospette che commettono un reato grave. La normativa nazionale indica inoltre quali dati possano essere trattati, nonché le procedure per preservare l'integrità e la riservatezza dei dati personali e quelle per la loro distruzione, fornendo in tal modo sufficienti garanzie contro il rischio di abuso e arbitrarietà.

4.3. Necessità e proporzionalità

Il ricorso al riconoscimento facciale è chiaramente più efficiente in termini di tempo rispetto all'abbinamento manuale a livello forense. La selezione manuale delle immagini in anticipo limita l'ingerenza rispetto alla riproduzione dell'intero materiale video per confrontarlo con una banca dati, distinguendo e riguardando solo le persone interessate dall'obiettivo, ossia la lotta contro le forme gravi di criminalità. Tuttavia, è comunque importante valutare se l'abbinamento sia eseguibile manualmente in un lasso di tempo ragionevole, a seconda del caso in questione. La limitazione del numero di persone che hanno accesso alla tecnologia e ai dati personali riduce l'impatto sul diritto alla vita privata e alla protezione dei dati, nonché sui modelli biometrici che non verranno conservati né utilizzati in seguito nel corso dell'indagine. Il controllo manuale del risultato comporta anche un minor rischio di falsi positivi.

4.4. Conclusioni

È bene che la legislazione nazionale preveda una base giuridica adeguata per il trattamento dei dati biometrici e per la banca dati nazionale con cui si effettua l'abbinamento. In questo scenario sono state attuate diverse misure al fine di limitare l'ingerenza nei diritti di protezione dei dati, come le condizioni per il ricorso alla FRT specificate nella base giuridica, il numero di persone aventi accesso alla tecnologia e ai dati biometrici, ai controlli manuali, ecc. La FRT migliora sensibilmente l'efficienza delle indagini del dipartimento di medicina legale della polizia, si basa sulla normativa che autorizza la polizia a trattare dati biometrici solo quando è assolutamente necessario e, pertanto, entro questi limiti può essere considerata un'ingerenza legittima nei diritti della persona.

5 SCENARIO 5

5.1. Descrizione

L'identificazione biometrica remota serve a determinare l'identità di più persone utilizzando identificatori biometrici (immagine del volto, andatura, iride, ecc.) a distanza, in uno spazio pubblico e in modo continuo o permanente confrontandoli con i dati (biometrici) contenuti in una banca dati ([89]). L'identificazione biometrica remota viene effettuata in tempo reale se il rilevamento delle immagini, il confronto e l'identificazione avvengono senza ritardi significativi.

Prima di ricorrere all'identificazione biometrica remota in tempo reale, la polizia compila ogni volta una lista di controllo di soggetti di interesse nell'ambito di un'indagine, popolata da immagini facciali delle persone. Sulla base di informazioni che suggeriscono la presenza di individui in una zona specifica, come un centro commerciale o una piazza pubblica, la polizia decide quando, dove e per quanto tempo utilizzare l'identificazione biometrica a distanza.

Nel giorno in cui interviene, la polizia invia sul posto un suo furgone con la funzione di centro di controllo, con un alto funzionario di polizia a bordo. Il furgone contiene alcuni monitor che visualizzano le immagini riprese dalle telecamere a circuito chiuso situate nelle vicinanze, installate ad hoc o collegate ai flussi video di telecamere già installate. Quando i pedoni passano davanti alle telecamere, la tecnologia isola le immagini facciali, le converte in un modello biometrico e le confronta con i modelli biometrici delle persone inserite nella lista di controllo.

Se si rileva una potenziale corrispondenza tra la lista di controllo e le persone che passano davanti alle telecamere, viene inviata una segnalazione agli agenti nel furgone, che avvisano quindi gli agenti sul posto se la segnalazione è positiva, ad esempio attraverso un dispositivo radio; questi ultimi decideranno allora se intervenire, entrare in contatto con la persona segnalata o, in ultima analisi, arrestarla. Le misure adottate dagli agenti sul posto vengono registrate. Nel caso di un controllo discreto, vengono memorizzate le informazioni acquisite (per esempio con chi si trova la persona segnalata, che cosa indossa e dove è diretta).

Una normativa nazionale citata prevede una disposizione generica in base a cui il trattamento dei dati biometrici al fine di identificare in modo univoco una persona fisica è ammissibile solo se è strettamente necessario ed è soggetto ad adeguate garanzie per i diritti e le libertà della persona interessata.

Fonte delle informazioni:

- Tipi di interessati: ☒ tutte le persone
- Fonte dell'immagine: ☒ spazi accessibili al pubblico
- Collegamento con il reato: ☒ non necessariamente un collegamento geografico o temporale diretto
- Modalità di acquisizione delle informazioni: ☒ remota
- Contesto: incidenza su altri diritti fondamentali: sì, in particolare: ☒ Libertà di riunione ☒ Libertà di parola ☒ varie
- Ulteriori fonti di informazioni disponibili sull'interessato:
  ☒ altro: non si escludono (per esempio l'uso di bancomat o negozi in cui è entrato l'interessato)

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

([89]) https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

- Specificità: ☒ banche dati specifiche relative alla zona in cui è avvenuto il reato

Algoritmo:

- Tipo di trattamento:☒ identificazione 1:molti

Esito:

- Impatto: ☒ diretto (per esempio l'interessato viene arrestato o interrogato)
- Decisione automatizzata: ☒ NO
- Durata della conservazione: fino alla conclusione di tutte le possibili indagini

Analisi giuridica:

- Tipo di informazione preliminare all'interessato:☒ Sul sito web dell'autorità di contrasto in generale
- Quadro giuridico applicabile: ☒ Direttiva LED, ripresa in gran parte nel diritto nazionale ☒ Normativa nazionale generica per l'utilizzo di dati biometrici da parte delle autorità di contrasto

5.2. Quadro giuridico applicabile

Le basi giuridiche che si limitano a ripetere la clausola generale dell'articolo 10 della direttiva LED non sono sufficientemente chiare nella loro formulazione per fornire alle persone un'indicazione adeguata in merito alle condizioni e alle circostanze in cui le autorità di contrasto sono autorizzate a usare registrazioni, effettuate in spazi pubblici, di telecamere a circuito chiuso per creare un modello biometrico dei loro volti e confrontarlo con le banche dati della polizia. Pertanto il quadro giuridico istituito in questo scenario non soddisfa i requisiti minimi per costituire una base giuridica ([90]).

5.3. Necessità e proporzionalità

Quanto più è profonda l'ingerenza, tanto più in alto si sposta l'asticella relativa alla necessità e alla proporzionalità. L'identificazione biometrica remota negli spazi pubblici comporta diverse ripercussioni per i diritti fondamentali.

Gli scenari implicano il monitoraggio di tutti i passanti nello spazio pubblico in questione; pertanto l'identificazione pregiudica pesantemente la ragionevole aspettativa delle persone di avere diritto all'anonimato negli spazi pubblici ([91]). Questo è un prerequisito per molti aspetti del processo democratico, come la decisione di aderire a un'associazione civica, partecipare a raduni e incontrare persone di ogni estrazione sociale e culturale, prendere parte a una protesta politica e visitare luoghi di ogni tipo. Il concetto di anonimato negli spazi pubblici è essenziale per raccogliere e scambiare liberamente informazioni e idee: preserva la pluralità delle opinioni, la libertà di riunione pacifica e la libertà di associazione nonché la tutela delle minoranze, oltre a sostenere i principi della separazione dei poteri e del bilanciamento dei poteri. Minare la nozione di anonimato negli spazi pubblici può causare un grave effetto inibitorio ai danni dei cittadini, i quali rischiano di astenersi da alcuni comportamenti che rientrano nei limiti di una società libera e aperta. Questo inciderebbe sull'interesse

([90]) Qualora un progetto scientifico finalizzato a condurre ricerche sull'uso della FRT debba trattare dati personali, ma tale trattamento non rientri nell'ambito di applicazione dell'articolo 4, paragrafo 3, della direttiva LED o esuli dell'ambito di applicazione del diritto dell'Unione, sarebbe applicabile il RGPD. Nel caso di progetti pilota eventualmente seguiti da operazioni di contrasto, la direttiva LED sarebbe comunque applicabile.

([91]) Risposta dell'EDPB ai deputati al Parlamento europeo in merito all'app di riconoscimento facciale sviluppata da Clearview AI, 10 giugno 2020, rif.: OUT2020-0052.

pubblico, poiché una società democratica richiede l'autodeterminazione e la partecipazione dei suoi cittadini al processo democratico.

Se si applica una simile tecnologia, il semplice fatto di camminare per strada, andare in metropolitana o in panetteria nella zona interessata comporterà la raccolta di dati personali, anche biometrici, da parte delle autorità di contrasto e, nel primo scenario, il confronto con le banche dati della polizia. Una situazione in cui si facesse altrettanto attraverso il rilevamento delle impronte digitali sarebbe chiaramente sproporzionata.

Il numero degli interessati coinvolti è estremamente elevato, poiché vi rientra chiunque passi davanti all'area pubblica in questione. Inoltre gli scenari comporterebbero il trattamento automatizzato di massa dei dati biometrici e un confronto di massa di questi ultimi con le banche dati della polizia.

Nella giurisprudenza europea, la sorveglianza di massa è vietata (per esempio, la Corte europea dei diritti dell'uomo nella causa S. e Marper c. Regno Unito ha ritenuto che la conservazione indiscriminata di dati biometrici rappresenti un'«ingerenza sproporzionata» nel diritto alla privacy, in quanto ciò non si può considerare «necessario in una società democratica»).

L'identificazione biometrica remota presenta un rischio talmente elevato di sfociare nella sorveglianza di massa che non esistono mezzi di limitazione affidabili; è sostanzialmente diversa dalla videosorveglianza in quanto tale, poiché l'eventuale utilizzo di riprese video senza l'identificazione biometrica costituisce già una forte ingerenza, ma al tempo stesso limitata, mentre se si applica la FRT il sistema di videosorveglianza già ampiamente diffuso come fonte principale dei dati subirà un cambiamento qualitativo. Inoltre, specialmente per quanto riguarda gli effetti inibitori impliciti, le eventuali restrizioni nell'applicazione degli impianti di videosorveglianza già esistenti non risulteranno visibili e pertanto non saranno ritenute affidabili dal pubblico.

L'identificazione biometrica remota attuata dalle autorità di polizia tratta tutti come persone potenzialmente sospette. In uno Stato di diritto, tuttavia, si presume che i cittadini siano innocenti fino a prova contraria. Tale principio si rispecchia anche in parte nella direttiva LED, che sottolinea la necessità di operare una distinzione, per quanto possibile, tra il trattamento delle persone condannate o indiziate, nel qual caso le autorità di contrasto devono avere «*fondati motivi di ritenere che [le persone] abbiano commesso o stiano per commettere un reato*» [articolo 6, lettera a), della direttiva LED] rispetto alle persone condannate o indiziate.

L'applicazione ai punti nodali dei trasporti o agli spazi pubblici, con le agenzie di contrasto che si avvalgono di una tecnologia in grado di identificare in modo univoco una singola persona e di rintracciarne e analizzarne la posizione e gli spostamenti, rivelerà anche le informazioni più sensibili sul suo conto (ivi comprese preferenze sessuali, religione, problemi di salute), comportando il rischio enorme di un accesso e un utilizzo illeciti dei dati.

L'installazione di un sistema che permetta di scoprire l'essenza stessa del comportamento e delle caratteristiche delle persone provoca forti effetti inibitori, spingendo i cittadini a chiedersi se partecipare o meno a una determinata manifestazione e nuocendo in tal modo al processo democratico. Potrebbe essere considerato critico anche il fatto di incontrare e farsi vedere in pubblico con un amico noto per i suoi problemi con la polizia o il suo comportamento particolare, poiché tutto ciò attirerebbe l'attenzione dell'algoritmo del sistema e quindi delle forze dell'ordine.

È impossibile proteggere interessati vulnerabili come i minori; questo vale anche per chi, come i giornalisti, gli avvocati e i membri del clero, ha un interesse professionale (e spesso è corrispondentemente tenuto per legge) a mantenere la riservatezza dei propri contatti, con il

conseguente rischio, per esempio, che vengano rivelati la fonte e il nome del giornalista o il fatto che una persona consulti un avvocato penale. Il problema non riguarda solo luoghi pubblici casuali, dove si incontrano per esempio i giornalisti e le loro fonti, ma naturalmente anche spazi pubblici necessari per venire in contatto con le istituzioni o i professionisti del settore e accedervi.

Inoltre, il disagio delle persone nei confronti della FRT può indurle a modificare il proprio comportamento, evitando i luoghi in cui viene utilizzata tale tecnologia e rinunciando quindi alla vita sociale e agli eventi culturali. A seconda della portata del ricorso alla FRT, l'impatto sulle persone può essere talmente significativo da incidere sulla loro capacità di vivere una vita dignitosa ([92]).

Vi è dunque una forte probabilità che venga violato il contenuto essenziale – il nucleo intoccabile – del diritto alla protezione dei dati personali. Ne sono forti indizi (cfr. sezione 3.1.3.2 delle linee guida) in particolare i seguenti: su vasta scala, le caratteristiche biologiche uniche delle persone vengono trattate automaticamente dalle autorità di contrasto con algoritmi basati sulla plausibilità, con risultati solo parzialmente spiegabili; le limitazioni ai diritti alla vita privata e alla protezione dei dati sono imposte indipendentemente dal comportamento individuale della persona o dalle circostanze che la riguardano; statisticamente, quasi tutti gli interessati che subiscono questa ingerenza sono persone rispettose delle leggi; le possibilità di fornire informazioni all'interessato sono limitate e, nella maggior parte dei casi, sarà possibile ricorrere alle vie giudiziarie solo in un secondo momento.

L'affidamento a un sistema basato sulla plausibilità e con una spiegabilità limitata può comportare una diffusione di responsabilità e una lacuna nel campo dei mezzi di ricorso, oltre al rischio di incentivare la disattenzione.

Una volta che un sistema di questo tipo, che può essere applicato anche alle telecamere a circuito chiuso esistenti, venga attuato con pochissimo sforzo e senza essere visibile alle persone, tale sistema può essere utilizzato in modo improprio e consentire la rapida e sistematica stesura di elenchi di persone in base all'origine etnica, al sesso, alla religione, ecc. Il principio del trattamento dei dati personali in base a criteri predeterminati, come il luogo in cui una persona si trova e l'itinerario percorso, viene già messo in pratica ([93]) ed è suscettibile di causare discriminazioni.

In base alla sensibilità, all'espressività e alla quantità dei dati trattati, i sistemi di riconoscimento facciale a distanza in luoghi accessibili al pubblico sono soggetti a un utilizzo improprio, con effetti nocivi per le persone interessate. Tali dati possono anche essere facilmente acquisiti e utilizzati in modo abusivo per esercitare pressioni sui principali soggetti attivi nell'ambito del principio del bilanciamento dei poteri, quali l'opposizione politica, i funzionari e i giornalisti.

Infine, i sistemi FRT implicano tendenzialmente forti effetti distorsivi in relazione alla razza e al genere: i risultati falsi positivi riguardano in misura sproporzionata le persone di colore e le donne ([94]), con conseguenti discriminazioni. Le misure di polizia adottate a seguito di un risultato falso positivo, quali perquisizioni e arresti, stigmatizzano ulteriormente tali gruppi.

([92]) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, pag. 20.

([93]) Cfr. articolo 6 della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e articolo 33 del regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226.

([94]) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

5.4. Conclusioni

Gli scenari summenzionati, riguardanti il trattamento a distanza dei dati biometrici negli spazi pubblici a fini di identificazione, denotano il mancato raggiungimento di un giusto equilibrio tra gli interessi privati e pubblici concorrenti, costituendo perciò un'ingerenza sproporzionata nei diritti degli interessati ai sensi degli articoli 7 e 8 della Carta.

6 SCENARIO 6

6.1. Descrizione

Un'entità privata sviluppa un'applicazione con cui si estraggono immagini facciali da internet per creare una banca dati. L'utente, per esempio la polizia, può quindi caricare una foto e, mediante l'identificazione biometrica, l'applicazione tenterà di abbinarla alle immagini facciali o ai modelli biometrici presenti nella sua banca dati.

Un dipartimento di polizia locale sta svolgendo un'indagine su un reato ripreso in un video e non è in grado di identificare alcuni potenziali testimoni e persone sospette attraverso il confronto delle informazioni acquisite con le banche dati interne o l'intelligence. In base alle informazioni raccolte, le persone fisiche non sono registrate in alcuna banca dati di polizia esistente. La polizia decide di utilizzare uno strumento come quello sopra descritto, messo a disposizione da un'azienda privata, per individuare le persone attraverso l'identificazione biometrica.

Fonte delle informazioni:

- Tipi di interessati: ☒ tutti i cittadini (testimoni) ☒ detenuti ☒ indagati
- Fonte dell'immagine: ☒ Riprese video provenienti da un luogo pubblico o acquisite altrove nell'ambito di un'indagine preliminare.
- Collegamento con il reato: ☒ non necessario
- Modalità di acquisizione delle informazioni: ☒ remota
- Contesto: incidenza su altri diritti fondamentali: sì, in particolare: ☒ Libertà di riunione ☒ Libertà di parola ☒ varie: __

Banca dati di riferimento (con cui si confrontano le informazioni acquisite):

- Specificità: ☒ banche dati per finalità generali popolate tramite internet

Algoritmo:

- Tipo di trattamento: ☒ identificazione 1:molti

Esito:

- Impatto ☒ diretto (per esempio l'interessato viene arrestato, interrogato, comportamento discriminatorio)
- Decisione automatizzata: ☒ NO

Analisi giuridica:

- Tipo di informazione preliminare all'interessato: ☒ No

6.2. Quadro giuridico applicabile

Quando un'entità privata presta un servizio che prevede il trattamento di dati personali, di cui determina la finalità e i mezzi (in questo caso l'estrazione di immagini da internet per creare una banca dati), tale entità deve disporre di una base giuridica per questo trattamento. Inoltre, anche l'autorità

di contrasto che decide di avvalersi di questo servizio per le proprie finalità deve disporre di una base giuridica per il trattamento di cui determina le finalità e i mezzi. Affinché l'autorità di contrasto possa trattare dati biometrici, deve esistere un quadro giuridico che specifichi l'obiettivo, i dati personali da trattare, le finalità del trattamento e le procedure per preservare l'integrità e la riservatezza dei dati personali, nonché le procedure per la loro distruzione.

Questo scenario implica l'acquisizione su vasta scala di dati personali all'insaputa dei relativi interessati; un trattamento di questo tipo potrebbe essere legittimo solo in circostanze del tutto eccezionali. A seconda del luogo in cui si trova la banca dati, il ricorso a tale servizio può comportare il trasferimento di dati personali e/o di categorie particolari di dati personali al di fuori dell'Unione europea (da parte della polizia, che ad esempio «invia» l'immagine del volto ripresa dalla videosorveglianza o altrimenti acquisita), richiedendo quindi condizioni specifiche per il suddetto trasferimento (cfr. articolo 39 della direttiva LED).

In questo scenario non esistono norme specifiche che autorizzino le autorità di contrasto a effettuare questo trattamento.

6.3. Necessità e proporzionalità

L'utilizzo del servizio da parte dell'autorità di contrasto comporta che i dati personali vengano condivisi con un'entità privata che si avvale di una banca dati in cui i dati personali sono raccolti su vasta scala e senza limitazioni. Non vi è alcun collegamento tra i dati personali acquisiti e l'obiettivo perseguito dall'autorità di contrasto; il fatto che quest'ultima condivida dati con l'entità privata implica anche una mancanza di controllo dell'autorità sui dati trattati dall'entità privata e grandi difficoltà per gli interessati nell'esercitare i loro diritti, poiché non sapranno che i loro dati vengono trattati in questo modo. Questo definisce una soglia molto elevata per le situazioni in cui potrebbe anche essere effettuato un trattamento di questo tipo; è opinabile che i requisiti stabiliti dalla direttiva siano soddisfatti da qualsiasi finalità, poiché eventuali deroghe e limitazioni al diritto alla vita privata e alla protezione dei dati sono applicabili solo quando è strettamente necessario. L'interesse generale che riveste l'efficacia nella lotta contro le forme gravi di criminalità non può di per sé giustificare il trattamento nel caso in cui vengano acquisite indiscriminatamente quantità di dati tanto vaste; pertanto questo trattamento non sarebbe conforme ai requisiti di necessità e proporzionalità.

6.4. Conclusioni

L'assenza di norme chiare, precise e prevedibili che soddisfino i requisiti di cui agli articoli 4 e 10 della direttiva e la mancanza di prove del fatto che tale trattamento sia strettamente necessario per conseguire gli obiettivi prefissati portano a concludere che l'uso di tale applicazione non sarebbe conforme ai requisiti di necessità e proporzionalità e implicherebbe un'ingerenza sproporzionata nei diritti degli interessati al rispetto della vita privata e alla protezione dei dati personali ai sensi della Carta.