MANUALE

Evitare la profilazione illecita oggi e in futuro: una guida

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Numerose informazioni sull'Agenzia dell'Unione europea per i diritti fondamentali sono disponibili su Internet accedendo al sito della FRA all'indirizzo fra.europa.eu

Europe Direct è un servizio a vostra disposizione per aiutarvi a trovare le risposte ai vostri interrogativi sull'Unione europea.

Numero verde unico (*):

00 800 6 7 8 9 10 11

(*) Le informazioni sono fornite gratuitamente e le chiamate sono nella maggior parte dei casi gratuite (con alcuni operatori e in alcuni alberghi e cabine telefoniche il servizio potrebbe essere a pagamento).

Foto (copertina e interno, da sinistra a destra): © stock.adobe.com-Savvapanf Photo.

Numerose altre informazioni sull'Unione europea sono disponibili su Internet consultando il portale Europa (http://europa.eu).

Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2019

Print:	ISBN 978-92-9474-747-1	doi:10.2811/270869	TK-06-18-031-IT-C
PDF:	ISBN 978-92-9474-748-8	doi:10.2811/00732	TK-06-18-031-IT-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Evitare la profilazione illecita oggi e in futuro: una guida

Sommario

Immagini e tabelle

Sigle e abbreviazioni

CCC	Programma comune di base
CEDU	Convenzione europea dei diritti dell'uomo
CGUE	Corte di giustizia dell'Unione europea
Corte EDU	Corte europea dei diritti dell'uomo
EES	Sistema di ingressi/uscite
ETIAS	Sistema europeo di informazione e autorizzazione ai viaggi
FRA	Agenzia dell'Unione europea per i diritti fondamentali
Frontex	Agenzia europea della guardia di frontiera e costiera
GDPR	Regolamento generale sulla protezione dei dati
GEPD	Garante europeo della protezione dei dati
IT	Tecnologie dell'informazione
OHCHR	Ufficio dell'Alto commissario delle Nazioni Unite per i diritti umani
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
SIS II	Sistema d'informazione Schengen
TCN	Cittadino di un paese terzo
UE	Unione europea
UE-MIDIS	Indagine su minoranze e discriminazioni nell'Unione europea
VIS	Sistema di informazione visti

Introduzione

Con il progredire della tecnologia, il ricorso alla profilazione è andato diffondendosi in un'ampia gamma di contesti, quali il marketing, l'occupazione, la sanità, la finanza, le attività di contrasto, il controllo delle frontiere e la sicurezza. Da qualche anno a questa parte gli Stati membri dell'Unione europea (UE) prestano maggiore attenzione all'uso degli strumenti di profilazione per agevolare il lavoro dei funzionari delle autorità di contrasto e di gestione delle frontiere. La profilazione è comunemente — e legittimamente — utilizzata dalle forze dell'ordine e dalle guardie di frontiera a fini di prevenzione, indagine e perseguimento di reati, nonché di prevenzione e accertamento dell'immigrazione irregolare. D'altro canto, però, se viene effettuata in modo illecito può minare la fiducia nelle autorità, in particolare nella polizia (e con questo termine si indicano tutte le forze di polizia), e stigmatizzare alcune comunità, facendo crescere le tensioni tra le comunità e le autorità di contrasto in relazione all'uso della profilazione con modalità percepite come discriminatorie.

La presente guida spiega che cos'è la profilazione, illustra il quadro giuridico che la disciplina ed espone i motivi per cui l'applicazione della profilazione entro i limiti stabiliti dalla legge non soltanto è necessaria per rispettare i diritti fondamentali, ma è anche essenziale per un'efficace attività di polizia e gestione delle frontiere. La guida fornisce inoltre indicazioni pratiche su come evitare la profilazione illecita nelle operazioni di polizia e di gestione delle frontiere. I principi e le prassi della guida sono illustrati con l'aiuto di esempi, casi di studio e decisioni giurisprudenziali tratti da tutta l'UE e non solo.

Perché c'è bisogno di questa guida?

La profilazione desta una serie di preoccupazioni in merito ai diritti fondamentali ([1]). Le prassi di profilazione rischiano di violare principi giuridici consolidati quali l'uguaglianza, la non discriminazione e il diritto al rispetto della vita privata e alla protezione dei dati. Inoltre, sono state sollevate riserve circa la loro efficacia nel contrasto all'illegalità e le possibili conseguenze negative sulle relazioni tra le autorità (tra cui la polizia e le autorità di gestione delle frontiere) e le comunità al cui servizio esse operano.

In risposta a tali preoccupazioni, nel 2010 l'Agenzia dell'Unione europea per i diritti fondamentali (FRA) ha pubblicato un documento intitolato *Per una maggiore efficacia delle operazioni di polizia — Una guida per comprendere ed evitare la definizione discriminatoria di profili etnici*. Tale documento, che riguardava in modo specifico l'utilizzo della profilazione da parte della polizia, era incentrato in particolare sull'esercizio dei poteri di fermo e perquisizione e mirava a fornire ai funzionari di livello intermedio strumenti per evitare la profilazione discriminatoria fondata sull'origine etnica.

Da allora, gli sviluppi tecnologici hanno notevolmente modificato la natura della profilazione. Attualmente, gran parte dell'attività di profilazione si basa sui risultati dell'analisi informatica di ampi set di dati. Sul piano giuridico, le disposizioni più rigorose in materia di protezione dei dati, frutto della riforma che trova applicazione in tutta l'UE da maggio 2018, stabiliscono nuove norme per la raccolta, l'analisi e l'uso dei dati personali.

La presente guida aggiornata tiene conto dei cambiamenti rilevanti intervenuti, riprendendo e ampliando la guida del 2010 per tenere conto delle novità giuridiche e pratiche. In particolare, adotta un approccio più esaustivo alla profilazione illecita includendo:

- la profilazione nell'ambito della gestione delle frontiere;
- la profilazione discriminatoria fondata su qualsiasi motivo, tra cui la nazionalità, l'età e il genere, oltre all'origine etnica;
- la profilazione algoritmica o informatica.

La versione del 2018 contiene anche nuovi esempi e casi di studio che riflettono gli sviluppi e le innovazioni riguardanti la profilazione.

([1]) Cfr. FRA (2018e), pagg. 85-87; FRA (2017c), pagg. 88-89; e FRA (2016), pagg. 83-85.

Chi dovrebbe utilizzare questa guida?

La presente guida è destinata principalmente ai responsabili della formazione del personale delle autorità di contrasto e di gestione delle frontiere. Può inoltre avere un'utilità diretta per i funzionari di livello intermedio aiutandoli ad applicare le tecniche di profilazione in modo lecito. Mira a migliorare la comprensione della teoria e della prassi della profilazione e a illustrare concretamente in che modo la profilazione può essere condotta nel rispetto dei diritti fondamentali.

La guida riguarda la profilazione effettuata dai funzionari di polizia in prima linea, ad esempio durante le operazioni di fermo e perquisizione, e i controlli eseguiti dalle guardie di frontiera ai valichi, in particolare quando si decide di sottoporre una persona a una «verifica in seconda linea» più approfondita. Nella gestione delle frontiere, è un ausilio alla formazione per i soggetti che impartiscono il programma comune di base per la formazione delle guardie di frontiera ai sensi dell'articolo 36, paragrafo 5, del regolamento relativo alla guardia di frontiera e costiera europea [regolamento (UE) 2016/1624].

La guida tratta anche la profilazione basata sull'analisi di set di dati di grandi dimensioni, compresi quelli disciplinati dalle norme dell'Unione europea; non analizza invece la profilazione effettuata in altre situazioni, ad esempio nel settore privato a fini commerciali. La FRA sta conducendo ulteriori ricerche in quest'ambito ([2]).

Come si utilizza questa guida?

La presente guida fornisce una panoramica dei principi e delle prassi principali della profilazione nell'ambito delle attività di contrasto e gestione delle frontiere. Può essere letta nella sua interezza o utilizzata come riferimento a sostegno delle attività di formazione.

La guida si compone di tre capitoli. Il capitolo 1 illustra il concetto di profilazione, chiarisce quando la profilazione diventa illecita e descrive l'impatto negativo che può avere sulle persone, sulle comunità e sull'esercizio dei poteri di polizia e di gestione delle frontiere. Il capitolo 2 illustra in dettaglio i principi e le prassi che dovrebbero guidare i funzionari delle autorità di contrasto e le guardie di frontiera nello svolgimento di attività lecite di profilazione. Il capitolo 3, infine, è dedicato alla profilazione algoritmica. Poiché in questo ambito la prassi non è ancora molto sviluppata, questa sezione contiene meno esempi concreti; presenta invece i rischi principali per i diritti fondamentali associati alla profilazione informatica e definisce i principali requisiti

([2]) Cfr. il progetto della FRA su intelligenza artificiale, megadati e diritti fondamentali.

giuridici stabiliti dal regolamento generale sulla protezione dei dati (GDPR) e dalla direttiva di polizia.

Una serie di elementi visivi pone in risalto i diversi aspetti della guida. I messaggi principali sono riassunti in punti salienti, evidenziati in riquadri gialli. Gli aspetti fondamentali del quadro giuridico sono evidenziati in riquadri azzurri, mentre gli esempi pratici sono contenuti in riquadri verdi. Altri riquadri contengono punti importanti a cui prestare attenzione, casi di studio ed esempi di decisioni giurisprudenziali. Sebbene si sia cercato di diversificare i casi di studio, gli esempi riportati si riferiscono in grande maggioranza al Regno Unito. Il motivo di tale sproporzione va ricercato nel fatto che il Regno Unito si occupa della profilazione illecita sin dagli anni Ottanta, mentre negli altri Stati membri la consapevolezza delle prassi di profilazione illecita è maturata solo in tempi recenti. Per questo motivo, il Regno Unito ha elaborato politiche e prassi più ampie e consolidate a cui si è attinto per presentare esempi.

Come è stata elaborata questa guida?

La FRA ha organizzato una riunione con esperti di vari settori per discutere una prima bozza della guida ed avere assistenza nella stesura della versione finale.

A questo proposito, la FRA desidera ringraziare gli esperti dell'Ufficio dell'Alto commissario delle Nazioni Unite per i diritti umani (OHCHR), dell'Agenzia europea della guardia di frontiera e costiera (Frontex), dell'Ufficio per le istituzioni democratiche e i diritti umani (ODIHR), dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), di Amnesty International, della Rete europea contro il razzismo (ENAR), del Centro internazionale per lo sviluppo delle politiche migratorie (ICMPD), del FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, European Digital Rights, Open Society Initiative for Europe, nonché i rappresentanti del difensore civico francese, delle forze di polizia olandesi, danesi e austriache e le guardie di frontiera polacche per i contributi preziosi che hanno fornito durante l'elaborazione della guida.

Sintesi dei punti principali

1. Le caratteristiche protette non possono in nessun caso essere l'unica base per la profilazione

- La profilazione comporta la **classificazione degli individui** in base alle loro caratteristiche.
- Per raccogliere e trattare **dati personali**, le autorità di contrasto e di gestione delle frontiere devono garantire che la raccolta e il trattamento dei dati abbiano una base giuridica, perseguano uno scopo valido e legittimo e siano necessari e proporzionati.
- Le **caratteristiche protette** quali la razza, l'origine etnica, il genere o la religione possono essere tra i fattori presi in considerazione dalle autorità di contrasto e dalle guardie di frontiera nell'esercizio delle loro competenze, ma **non possono essere l'unica o principale ragione per concentrare l'attenzione su un soggetto** (per ulteriori informazioni sulle «caratteristiche protette», cfr. sezione 1.2.1).
- La profilazione basata esclusivamente o principalmente su una o più caratteristiche protette equivale a una discriminazione diretta e pertanto **viola i diritti e le libertà della persona** ed è **illecita**.

2. Qualsiasi interazione con le persone dovrebbe essere improntata al rispetto, alla professionalità e all'informazione

- Un'**interazione di buona qualità** di per sé non elimina la profilazione basata su preconcetti, ma con buona probabilità migliora il risultato dell'interazione e riduce il possibile impatto negativo del fermo effettuato da un agente di polizia o una guardia di frontiera. Nella gestione delle frontiere, un comportamento professionale e rispettoso è espressamente indicato come un obbligo giuridico.
- Un **comportamento professionale e rispettoso** in genere aumenta la soddisfazione relativa all'interazione.
- **Offrendo spiegazioni sui motivi per cui si ferma** una persona, si contribuisce a rafforzare la fiducia nelle operazioni di polizia e gestione delle frontiere e a ridurre la sensazione che la profilazione sia basata su preconcetti.
- Il rispetto e la cortesia, tuttavia, **non rendono in nessun caso giustificabili verifiche di frontiera o fermi e perquisizioni illeciti**.

3. La profilazione dovrebbe essere fondata su motivazioni oggettive e ragionevoli

- Per essere leciti, i fermi e il rinvio a verifiche in seconda linea devono **essere fondati su motivi ragionevoli e oggettivi** che inducano a nutrire sospetti.
- Le caratteristiche personali possono essere utilizzate come fattori legittimi per la profilazione, ma per evitare che si configuri una discriminazione **devono esservi *anche* ragionevoli motivi di sospetto** basati su informazioni diverse dalle caratteristiche protette.
- Quando le attività di contrasto e gestione delle frontiere sono basate su **informazioni di intelligence specifiche e aggiornate**, è più probabile che siano **oggettive**.
- L'essenziale è che la decisione di fermare una persona o sottoporla a verifiche di frontiera in seconda linea **non si basi esclusivamente sulle *sensazioni* di un funzionario** nei confronti di tale persona, perché tali sensazioni rischiano di essere basate su preconcetti, stereotipi e/o pregiudizi.

4. La profilazione illecita ha un impatto negativo sulle attività di polizia e gestione delle frontiere

- **La profilazione illecita mina la fiducia nella polizia e nelle guardie di frontiera.** Può causare un deterioramento dei rapporti tra la polizia/le guardie di frontiera e i membri di minoranze e altre comunità che possono sentirsi presi di mira. Questo senso di ingiustizia può far sì che alcuni individui e gruppi perdano fiducia nelle forze di polizia e in altre autorità, il che può portare a una riduzione delle denunce di reati alla polizia e della cooperazione con le autorità. Ciò, a sua volta, può indurre le autorità a considerare alcuni gruppi con sospetto, il che può ulteriormente accrescere il ricorso a prassi di profilazione illecite.
- **La profilazione illecita compromette l'efficacia della profilazione**, in quanto il tasso di fermi di persone appartenenti ai diversi gruppi da parte della polizia o alle frontiere non corrisponde necessariamente al tasso di commissione di illeciti registrato in tali gruppi.
- Quando un gruppo di minoranza è oggetto di un'attenzione spropositata da parte del personale di polizia o di gestione delle frontiere, vi è il rischio che si crei una **profezia che si autoavvera** causando un maggior numero di arresti o verifiche alle frontiere.

5. La profilazione illecita ha conseguenze giuridiche e finanziarie e i funzionari sono tenuti a risponderne

- I funzionari delle autorità di contrasto e di gestione delle frontiere hanno la responsabilità di mantenere la profilazione nell'ambito della legalità e sono tenuti a **renderne conto**.
- La **raccolta di dati affidabili, accurati e tempestivi** è fondamentale per garantire l'assunzione di responsabilità.
- L'istituzione di **meccanismi di reclamo efficaci** permette di scongiurare gli abusi di potere e al tempo stesso contribuisce ad assicurare e ristabilire la fiducia nell'operato delle autorità di polizia e gestione delle frontiere.
- L'organizzazione di **incontri con i cittadini** (per sentire i loro pareri, discutere il tema della profilazione e raccogliere feedback sulle operazioni) offre la possibilità di trarre insegnamenti importanti e migliorare le attività di profilazione.

6. La profilazione algoritmica deve rispettare specifiche garanzie di protezione dei dati

- Nello sviluppo e nell'utilizzo della profilazione algoritmica, è possibile che siano introdotte **distorsioni** (*bias*) in ogni fase del processo. Per evitare che ciò accada e che di conseguenza si possano verificare violazioni dei diritti fondamentali, **sia gli esperti informatici sia i funzionari che interpretano i dati devono avere una conoscenza precisa dei diritti fondamentali.**
- È indispensabile utilizzare **dati affidabili**. L'utilizzo in un algoritmo di dati che riflettono preconcetti esistenti o provengono da fonti inaffidabili produce risultati non imparziali e inaffidabili.
- La profilazione algoritmica deve essere **legittima**, **necessaria** e **proporzionata.**
- Il trattamento dei dati deve avere **una finalità specifica**.
- I singoli interessati hanno il **diritto di essere informati**, ricevendo informazioni sui dati personali che vengono raccolti e conservati, sul trattamento dei dati e sulla sua finalità, nonché sui propri diritti.
- I dati devono essere **raccolti, trattati e conservati in modo sicuro**. Le autorità dovrebbero tenere registri delle attività di trattamento (comprese le operazioni effettuate sui dati) e dei relativi registri (comprese le informazioni sulla persona o sulle persone che accedono ai dati).
- Il trattamento illecito dei dati deve essere **prevenuto e individuato**: 1) tramite valutazioni d'impatto preliminari e 2) mediante l'utilizzo di strumenti di privacy incorporati «fin dalla progettazione» nell'algoritmo.

Siti web consultabili

Unione europea
Corte di giustizia dell'Unione europea: http://www.curia.eu
Legislazione dell'UE: http://eur-lex.europa.eu/
Agenzia dell'Unione europea per i diritti fondamentali: http://www.fra.europa.eu
Parlamento europeo: http://www.europarl.europa.eu

Consiglio d'Europa
Comitato dei ministri del Consiglio d'Europa: http://www.coe.int/cm
Corte europea dei diritti dell'uomo: http://www.echr.coe.int

Nazioni Unite
Ufficio dell'Alto commissario delle Nazioni Unite per i diritti umani: http://www.ohchr.org

Lotta contro la discriminazione
Commissione europea contro il razzismo e l'intolleranza (ECRI): http://www.coe.int/ecri
Rete europea degli organismi per la parità (Equinet): http://www.equineteurope.org/
Organismi nazionali per la parità: http://www.archive.equineteurope.org/-Equinet-Members-

Protezione dei dati
Garante europeo della protezione dei dati: https://edps.europa.eu/
Comitato europeo per la protezione dei dati: https://edpb.europa.eu
Autorità nazionali per la protezione dei dati: https://edpb.europa.eu/about-edpb/board/members_it

Applicazione della legge e attività di contrasto
Rete delle autorità indipendenti che si occupano dei reclami nei confronti della polizia (IPCAN): https://ipcan.org/
Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL): https://www.cepol.europa.eu/
Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol): https://www.europol.europa.eu/

Gestione delle frontiere
Agenzia europea della guardia di frontiera e costiera: https://frontex.europa.eu/
Ufficio europeo di sostegno per l'asilo (EASO): https://www.easo.europa.eu/

Banche dati su larga scala
Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA): https://www.eulisa.europa.eu/

1 Il quadro generale: che cosa si intende per profilazione?

Il presente capitolo spiega che cosa si intende per profilazione e illustra i principali diritti fondamentali su cui essa può incidere. Introduce la profilazione nel contesto delle attività di contrasto e gestione delle frontiere esaminando tre elementi essenziali:

- il concetto di profilazione e il suo utilizzo da parte delle autorità di contrasto e gestione delle frontiere, con una presentazione di alcuni dei diversi tipi di profilazione esistenti;
- i principi più importanti in materia di diritti fondamentali che devono essere rispettati per effettuare la profilazione in modo lecito, ossia la non discriminazione e il diritto al rispetto della vita privata e alla protezione dei dati;
- le potenziali conseguenze negative della profilazione, comprese le possibili conseguenze sugli individui e sui rapporti con le comunità, nonché sulla fiducia nelle autorità di polizia e di gestione delle frontiere.

1.1. Definizione della profilazione

La profilazione comporta la **classificazione di individui** in base a caratteristiche personali. Tali caratteristiche possono essere «immutabili» (come l'età o l'altezza) o «modificabili» (quali l'abbigliamento, le abitudini, le preferenze e altri elementi del comportamento). La profilazione include l'estrazione di dati (*data mining*), mediante la quale le persone sono classificate «**sulla base di alcune loro caratteristiche**

osservabili per inferirne, con un certo margine di errore, altre che osservabili non sono» ([3]).

Punti salienti

- La profilazione comporta la **classificazione degli individui** sulla base di caratteristiche loro attribuite per inferenza.
- Nel contesto delle attività di contrasto e gestione delle frontiere la profilazione viene utilizzata principalmente per **individuare soggetti noti sulla base di informazioni riguardanti uno specifico individuo** e come **metodo predittivo** per individuare soggetti «non noti» che potrebbero rivestire interesse per le autorità di contrasto e di gestione delle frontiere. Entrambe queste finalità possono incorporare pregiudizi consci o inconsci che possono tradursi in una discriminazione nei confronti di singole persone.
- Le attività di profilazione delle guardie di frontiera e dei funzionari delle autorità di contrasto possono essere influenzate da pregiudizi derivanti da esperienze personali o istituzionali. Tali pregiudizi possono permeare e alterare la valutazione associata alla profilazione, compromettendo sia la liceità che l'efficacia delle attività di polizia.
- Gli stereotipi possono riflettere in certa misura una verità statistica. Anche in questi casi, tuttavia, essi **rimangono problematici** se a causa loro una persona viene trattata come membro di un gruppo e non sulla base della sua situazione individuale.
- Nello sviluppo e nell'utilizzo della profilazione algoritmica, è possibile che **siano introdotte distorsioni in ogni fase del processo**. Per evitare queste e altre potenziali violazioni dei diritti fondamentali, gli esperti informatici che progettano gli algoritmi e chi raccoglie e interpreta i dati dovrebbero avere una conoscenza precisa dei diritti fondamentali e di come applicarli in questo contesto.

La profilazione è utilizzata per:

- generare conoscenze, analizzando dati esistenti per formulare ipotesi su una persona. Utilizza le esperienze passate e l'analisi statistica per stabilire correlazioni tra talune caratteristiche e risultati o comportamenti specifici;
- sostenere i processi decisionali utilizzando tali correlazioni per prendere decisioni sulle azioni da intraprendere.

([3]) Dinant, J.-M., Lazaro, C., Poullet, Y., Lefever, N. e Rouvroy, A. (2008), pag. 3.

Ciò rende la profilazione uno strumento potente per i funzionari delle autorità di contrasto e le guardie di frontiera, ma comporta alcuni rischi significativi:

- la profilazione stabilisce correlazioni generali che potrebbero non essere valide per ogni individuo, dato che ogni individuo può rappresentare l'«eccezione alla regola»;
- i profili possono generare correlazioni errate sia per i singoli individui che per i gruppi;
- i profili possono creare stereotipi deleteri e provocare discriminazioni;
- alcuni stereotipi possono riflettere una verità statistica. Anche in questi casi, tuttavia, gli stereotipi rimangono problematici se fanno sì che una persona sia trattata come membro di un gruppo anziché come individuo.

Esempi

Profilazione potenzialmente imprecisa

La supposizione secondo cui «le donne vivono più a lungo degli uomini» è fondata su ricerche fattuali; tuttavia, un determinato uomo può vivere più a lungo di una determinata donna. Qualsiasi decisione presa nei confronti di una specifica donna sulla base di tale supposizione rischia quindi di essere inesatta e la supposizione rimane valida solo in media.

Il proprietario di un'auto può prestarla a familiari o amici, il che rende inaffidabile qualsiasi profilo di guida rischiosa basato sulla proprietà dell'auto.

1.1.1. La profilazione nel contesto delle attività di contrasto e gestione delle frontiere

La profilazione è comunemente — e legittimamente — utilizzata dalle forze dell'ordine e dalle guardie di frontiera a fini di prevenzione, indagine e perseguimento di reati, nonché di prevenzione e accertamento dell'immigrazione irregolare.

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» ([4]). I risultati di questo trattamento dei dati sono utilizzati per guidare le attività di gestione delle frontiere e di contrasto, come i fermi e le perquisizioni, gli arresti, il diniego dell'accesso a determinate aree, o la decisione di effettuare «verifiche in seconda linea» più approfondite alla frontiera. La profilazione viene utilizzata principalmente per due scopi:

- per identificare le persone sulla base di specifiche informazioni di intelligence, utilizzando un profilo che elenca le caratteristiche di specifiche persone sospette sulla base delle prove raccolte in merito a un determinato evento;

- come metodo predittivo, per identificare persone «non note» che potrebbero rivestire interesse per le autorità di contrasto e di gestione delle frontiere, sulla base dell'analisi dei dati e di supposizioni fondate sull'esperienza. Idealmente, i metodi predittivi sono imperniati sui comportamenti; in pratica, tuttavia, l'attenzione si concentra spesso non tanto (o non solo) sul comportamento, quanto su caratteristiche fisiche visibili, come l'età, il genere o l'origine etnica.

La tabella 1 pone a confronto le caratteristiche principali di questi due tipi di profilazione nel contesto delle attività di polizia.

Tabella 1: Caratteristiche delle attività di polizia basate su informazioni di intelligence specifiche e delle attività di polizia di tipo predittivo

	Attività di polizia basate su informazioni di intelligence specifiche	Attività di polizia di tipo predittivo
Contesto	È stato commesso un reato o è stata emessa una segnalazione su una persona specifica	Non è stato commesso nessun reato o non è stata emessa nessuna segnalazione su una persona specifica
Approccio	Reattivo	Proattivo
Obiettivo	Fermare il sospetto/i sospetti	Prevedere dove e quando potrebbero verificarsi reati o chi potrebbe cercare di entrare nel paese in modo irregolare

([4]) 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 (direttiva di polizia) (GU L 119 del 4.5.2016, pag. 89), articolo 3, paragrafo 4.

Dati utilizzati	Informazioni di intelligence specifiche relative al caso (il «profilo individuale»)	Informazioni di intelligence generiche relative a diversi casi
Tipo di processo	Combinazione di processi basati sui dati e processi con intervento dell'uomo	Basato principalmente su dati («analisi del rischio»)

Fonte: *FRA (2018)*

Entrambi i tipi di profilazione possono essere illeciti se non sono effettuati con garanzie specifiche, tra cui una giustificazione oggettiva e ragionevole per la profilazione. Il capitolo 2 e il capitolo 3 forniscono informazioni pratiche su come far sì che la profilazione sia effettuata in modo lecito e nel rispetto dei diritti umani.

1.1.2. Definizione della profilazione algoritmica

In seguito ai rapidi sviluppi tecnologici, la profilazione si basa sempre più sull'uso di dati conservati in banche dati e sistemi informatici (sistemi IT). La profilazione algoritmica, che utilizza diverse tecniche per definire il profilo delle persone sulla base di correlazioni e modelli o tendenze nei dati, consente ai funzionari delle autorità di contrasto e di gestione delle frontiere di concentrare la propria attenzione su soggetti o gruppi specifici che in base all'analisi dei dati costituiscono un determinato rischio.

La profilazione algoritmica solleva importanti preoccupazioni in materia di diritti fondamentali, ad esempio riguardo alla potenziale discriminazione e alle violazioni del diritto al rispetto della vita privata e del diritto alla protezione dei dati. Questa sezione della guida illustra in che modo i funzionari delle autorità di contrasto e di gestione delle frontiere possono utilizzare e trattare i dati coerentemente con i principi in materia di diritti fondamentali nel loro lavoro quotidiano.

Trattamento dei dati personali: che cosa dice la legge?

Le norme giuridiche per il trattamento dei dati personali ai fini della profilazione sono contenute nel quadro giuridico dell'UE in materia di protezione dei dati. Ai sensi dell'articolo 4, paragrafo 4, del regolamento generale sulla protezione dei dati e dell'articolo 3, paragrafo 4, della direttiva di polizia, si intende per profilazione «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».

L'articolo 22, paragrafo 1, del GDPR indica che la profilazione è ammessa purché la decisione non sia basata unicamente sul trattamento automatizzato e non produca effetti che incidano significativamente sugli individui.

La profilazione che rientra nell'ambito di applicazione della direttiva di polizia (cfr. sezione 3.1 sulla profilazione algoritmica e sulla protezione dei dati) dovrebbe rispettare l'articolo 11, paragrafo 3, della medesima direttiva. Ai sensi di tale articolo, «[l]a profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 (*) è vietata, conformemente al diritto dell'Unione».

(*) Le «categorie particolari di dati personali» sono «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Cfr. articolo 10, paragrafo 1, della direttiva di polizia.

Il metodo utilizzato per generare profili ai fini della profilazione algoritmica è simile a una tecnica nota come «**analisi comportamentale**», in cui sono effettuati collegamenti tra determinate caratteristiche e modalità di comportamento. La figura 1 mostra in che modo si possono utilizzare gli algoritmi per elaborare previsioni.

Figura 1: Il processo di profilazione algoritmica nel contesto dell'attività di contrasto e gestione delle frontiere

Fonte: *FRA (2018) (adattato da/sulla base di Perry, W.L. e al. (2013), pagg. 11-15, e Zarsky, T.Z. (2002-2003), pagg. 6-18)*

Sotto la lente: come vengono utilizzati gli algoritmi a sostegno del processo decisionale

Con il crescere della disponibilità e dell'uso dei dati, i processi decisionali sono sempre più facilitati o sostituiti da metodi di modellazione predittivi, ossia dall'uso di algoritmi. Un algoritmo è una sequenza di comandi impartiti a un computer per trasformare un elemento in ingresso (*input*) in un elemento in uscita (*output*). Molti algoritmi si basano su metodi statistici e utilizzano tecniche che calcolano le relazioni tra diverse variabili. Ad esempio, i dati sulla quantità di alcol che un gruppo di persone beve possono essere incrociati con i dati sulla speranza di vita dello stesso gruppo per calcolare l'incidenza media del consumo di alcol sulla speranza di vita.

L'output degli algoritmi è sempre una probabilità, il che significa che vi è un certo grado di incertezza riguardo alle relazioni stabilite o alle classificazioni effettuate. Ad esempio, i server di posta elettronica utilizzano algoritmi per individuare i messaggi spazzatura e inviarli alla cartella della posta indesiderata. Gli algoritmi funzionano bene, ma non sono perfetti. Talvolta lo spam non viene individuato e finisce nella cartella della posta in arrivo: si ha allora un falso negativo (messaggio erroneamente non identificato come spam). Meno spesso accade che un'e-mail legittima sia intercettata dal filtro antispam e inviata alla cartella della posta indesiderata: si tratta in questo caso di un falso positivo.

Il possesso di una conoscenza di base circa il modo in cui gli algoritmi sono di supporto ai processi decisionali permette di identificare e porre le domande giuste sui potenziali problemi relativi all'uso degli algoritmi, comprese le potenziali discriminazioni e violazioni del diritto al rispetto della vita privata e alla protezione dei dati.

Per ulteriori informazioni, cfr. FRA (2018b).

La creazione di algoritmi predittivi è un processo complesso che comporta numerose decisioni prese da più persone coinvolte nel processo. Non si riferisce quindi soltanto alle regole seguite da un computer, ma anche al processo di raccolta, preparazione e analisi dei dati. Quest'ultimo è un processo con intervento dell'uomo e comprende varie fasi, che comportano l'adozione di decisioni da parte di sviluppatori e dirigenti. Il metodo statistico è solo una parte del processo di definizione delle regole finali utilizzate per prevedere, classificare o prendere decisioni ([5]). In ogni caso, il modo in cui i dati sono raccolti e utilizzati può essere discriminatorio.

Esempio

Per essere efficaci e accurati, i software di riconoscimento facciale devono poter attingere a enormi quantità di immagini e dati: maggiore è la quantità di dati che ricevono, più accurati saranno i risultati. Ciò nonostante, ad oggi per addestrare questi sistemi sono state utilizzate soprattutto immagini di uomini bianchi; il numero di immagini di donne e/o individui di altri gruppi etnici è relativamente modesto. Di conseguenza, per le persone appartenenti

([5]) FRA (2018b), pag. 4.

a tali gruppi i risultati prodotti dai software sono meno precisi e comportano una maggiore probabilità di inesattezza. Quando questi sistemi vengono usati dai funzionari delle autorità di contrasto o dalle guardie di frontiera per la profilazione e decidere, ad esempio, se arrestare o meno una persona, possono verificarsi errori con un impatto potenzialmente grave sui diritti e sulle libertà della persona.

Per ulteriori informazioni, cfr. Center on Privacy and Technology at Georgetown Law (2016) e Buolamwini J., Gebru T. (2018).

In ogni fase della profilazione algoritmica è possibile che siano introdotte distorsioni. Nel raccogliere ed interpretare i dati, sia le persone che progettano gli algoritmi che i funzionari delle autorità di contrasto e gestione delle frontiere dovrebbero avere una conoscenza precisa dei diritti fondamentali e della loro applicazione in questo contesto al fine di evitare distorsioni discriminatorie e violazioni del diritto alla protezione dei dati e alla vita privata.

È indispensabile che i dati utilizzati siano affidabili. Nella profilazione algoritmica, occorre valutare la qualità dei dati utilizzati così da garantirne l'affidabilità: quanto minore è la variabilità dei dati, tanto più elevata è la loro affidabilità. L'utilizzo di dati che riflettono distorsioni esistenti o provengono da fonti inaffidabili per la costruzione di un algoritmo produrrà risultati non imparziali e non affidabili. Errori si possono verificare anche nell'elaborazione mediante inferenza di previsioni a partire dai dati:

- si hanno falsi positivi quando si concentra l'attenzione su specifici soggetti e li si sottopone a ulteriori controlli sulla base della previsione erronea che essi presentino un rischio;

- si hanno falsi negativi quando soggetti che presentano un rischio reale nel contesto delle operazioni di contrasto e gestione delle frontiere non sono stati identificati come tali dal sistema.

1.2. In quali circostanze la profilazione è illecita?

Punti salienti

- Le caratteristiche personali possono essere utilizzate come fattori legittimi per la profilazione, ma per evitare che la profilazione sia discriminatoria e quindi illecita, devono esservi anche ragionevoli motivi di sospetto basati su informazioni diverse dai **motivi protetti**.
  - I motivi protetti comprendono il sesso, la razza, il colore della pelle, l'origine etnica o l'estrazione sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le tendenze politiche o altre idee, l'appartenenza a una minoranza nazionale, le condizioni economiche, la nascita, l'età e l'orientamento sessuale.
  - I motivi protetti possono essere rivelati, desunti o previsti in base ad altri dati personali.
- Per raccogliere e trattare **dati personali**, le autorità di contrasto e di gestione delle frontiere devono garantire che la raccolta e il trattamento dei dati abbiano una base giuridica, perseguano un obiettivo valido e legittimo e siano necessari e proporzionati.
  - I dati personali sono tutte le informazioni che possono essere utilizzate per identificare, direttamente o indirettamente, una persona, quali: un nome, un numero di identificazione, dati relativi all'ubicazione o qualsiasi altra identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale propria di una persona.

Se utilizzata lecitamente, la profilazione è una **tecnica di indagine legittima**. Per essere lecita, deve avere **giustificazioni oggettive e ragionevoli** e rispettare i diritti fondamentali, quali il diritto alla non discriminazione e alla protezione dei dati personali. La profilazione si considera priva di una giustificazione oggettiva e ragionevole «se non persegue un obiettivo legittimo o se non vi è un rapporto ragionevole di proporzionalità tra i mezzi impiegati e lo scopo perseguito» ([6]).

La profilazione può incidere su un gran numero di diritti fondamentali. La presente sezione tratta i diritti fondamentali maggiormente interessati dalla profilazione illecita: il diritto alla non discriminazione, il diritto alla privacy e il diritto alla protezione dei dati. La profilazione è considerata illecita se:

- comporta ingiustificate disparità di trattamento sulla base di motivi protetti (cfr. sezione 1.2.1), oppure

([6]) Commissione europea contro il razzismo e l'intolleranza (2007), punto 28.

- interferisce inutilmente con la vita privata delle persone e/o non rispetta le norme relative al trattamento dei dati personali (cfr. sezione 1.2.2).

1.2.1. Divieto di discriminazione

Divieto di discriminazione: che cosa dice la legge?

«**È vietata qualsiasi forma di discriminazione** fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale» (*).

Articolo 21 della Carta dei diritti fondamentali dell'UE

«**Il godimento di ogni diritto previsto dalla legge deve essere assicurato senza nessuna discriminazione**, in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita o ogni altra condizione.Nessuno potrà essere oggetto di discriminazione da parte di una qualsivoglia autorità pubblica per i motivi menzionati al paragrafo 1».

Articolo 1 del protocollo n. 12 della convenzione europea dei diritti dell'uomo

(*) *Va osservato che molti Stati membri hanno esteso la protezione contro la discriminazione oltre i motivi elencati nella Carta e nella convenzione europea dei diritti dell'uomo (CEDU).*

Sussiste discriminazione «quando [...] una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga» a causa di una caratteristica personale reale o presunta ([7]). Tali caratteristiche sono definite «motivi protetti» o «caratteristiche protette» nella legislazione in materia di non

([7]) Direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica (GU L 180 del 19.7.2000. pag. 22), articolo 2, e direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro (GU L 303 del 2.12.2000, pag. 16), articolo 2.

discriminazione. Ulteriori informazioni sul diritto e sulla giurisprudenza europei in materia di non discriminazione sono disponibili nell'edizione 2018 del manuale di diritto europeo della non discriminazione, pubblicato congiuntamente dalla FRA e dal Consiglio d'Europa ([8]).

Esistono diversi tipi di discriminazione.

Sussiste **discriminazione diretta** quando una persona è trattata meno favorevolmente *esclusivamente o principalmente* a causa di un motivo protetto, come la razza, il genere, l'età, la disabilità o l'origine etnica ([9]).

Esempio

In risposta a una minaccia terroristica, alla polizia viene conferito il potere di fermare e perquisire chiunque a suo parere sia coinvolto in attività terroristiche. Si ritiene che la minaccia provenga da un'organizzazione terroristica che opera in una determinata regione del mondo, ma non esistono ulteriori informazioni di intelligence specifiche. Se un funzionario di polizia ferma un uomo esclusivamente o principalmente perché il suo aspetto indica che può provenire da quella regione del mondo, il suo modo di procedere costituisce una discriminazione diretta ed è illegale.

Sussiste **discriminazione indiretta**, detta anche «discriminazione ad impatto differenziato» (*disparate impact*) nel contesto delle attività di contrasto e di gestione delle frontiere, quando una disposizione, un criterio o una prassi *apparentemente neutri* possono mettere in una posizione di particolare svantaggio le persone con determinate caratteristiche protette rispetto ad altre persone, a meno che tale disposizione, criterio o prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il loro conseguimento siano necessari e proporzionati ([10]). Per accertare la sussistenza di discriminazione indiretta, occorrono in genere dati statistici per valutare se una persona è stata effettivamente trattata in modo meno favorevole rispetto a un'altra per effetto della sua appartenenza a un gruppo con determinate caratteristiche protette.

([8]) FRA e Consiglio d'Europa (2018).

([9]) *Ibid.*, pag. 43.

([10]) Direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro (GU L 303 del 2.12.2000, pag. 16), articolo 2.; cfr. anche FRA e Consiglio d'Europa (2018), pag. 53.

Esempio

Nell'ambito dei controlli di routine, le autorità di contrasto decidono di fermare un'auto ogni dieci nella città X nella fascia oraria 21:00-01:00. Il 60 % della popolazione della città X che guida un'auto in tale fascia oraria è di origine afro-caraibica, mentre la percentuale della popolazione afro-caraibica che vive nella città e nell'area circostante non supera il 30 %. Poiché questo gruppo ha maggiori probabilità rispetto ad altri di essere interessato negativamente dalla misura, sussiste una discriminazione indiretta.

Affrontando la discriminazione sulla base di un unico motivo non si prendono adeguatamente in considerazione le diverse manifestazioni della disparità di trattamento. La **discriminazione multipla** è una forma di discriminazione che avviene sulla base di diversi motivi che operano separatamente. Ad esempio, una persona può subire discriminazione non soltanto a causa dell'origine etnica, ma anche dell'età e del genere ([11]). La **discriminazione intersettoriale** descrive una situazione in cui diversi motivi operano e interagiscono tra loro nello stesso tempo risultando in tal modo inseparabili e producendo tipi specifici di discriminazione (cfr. riquadro dell'esempio).

Esempio

Un agente di polizia ferma e perquisisce un giovane di origine africana senza il ragionevole sospetto che abbia commesso un reato. La discriminazione che subisce questa persona in questo caso è dovuta non soltanto alla sua età (non tutti i giovani vengono fermati) o alla sua origine etnica (non tutte le persone di origine africana sono fermate), bensì al fatto che è sia giovane sia di origine africana.

La discriminazione può derivare anche dal trattamento automatizzato dei dati personali e dall'utilizzo della profilazione algoritmica. Elementi di discriminazione possono essere inclusi durante la progettazione e l'applicazione di algoritmi a causa di distorsioni introdotte — consapevolmente o inconsapevolmente — nell'algoritmo, e possono sussistere quando vengono prese decisioni sulla base delle informazioni ottenute.

L'articolo 9, paragrafo 1, del GDPR stabilisce espressamente che è vietato trattare categorie particolari di dati personali che rivelino caratteristiche personali quali

([11]) FRA e Consiglio d'Europa (2018), pag. 59.

l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche (per l'elenco completo dei motivi protetti, cfr. la figura 7 nella sezione 2.2.4). Tale divieto può non applicarsi in casi specifici, come ad esempio la tutela dell'interesse pubblico, a condizione che l'esenzione abbia una base giuridica, sia proporzionata e necessaria e preveda garanzie adeguate ([12]).

Analogamente, nel contesto delle attività volte a prevenire, indagare, accertare e perseguire reati, l'articolo 11, paragrafo 3, della direttiva di polizia sul processo decisionale automatizzato relativo alle persone fisiche vieta la «profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali», tra cui i dati che rivelino l'origine razziale o etnica e le convinzioni religiose, nonché i dati genetici e biometrici ([13]). Anche in questo caso, eccezioni a tale divieto sono consentite in taluni casi, ma devono essere necessarie, sono assoggettate a garanzie adeguate e dovrebbero essere fondate su una base giuridica o avere l'obiettivo di proteggere gli interessi vitali di una persona ([14]).

Divieto di profilazione discriminatoria: che cosa dice la legge?

«**La profilazione che porti alla discriminazione** di persone fisiche **sulla base di dati personali** che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali **dovrebbe essere vietata** alle condizioni stabilite negli articoli 21 e 52 della Carta [dei diritti fondamentali]».

Considerando 38 della direttiva di polizia

«**La profilazione che porta alla discriminazione** di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 (*) **è vietata**, conformemente al diritto dell'Unione».

Articolo 11, paragrafo 3, della direttiva di polizia

(*) Articolo 10 della direttiva di polizia: «dati [...] che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare

([12]) Regolamento generale sulla protezione dei dati, articolo 9, paragrafo 2, lettera g).

([13]) Per maggiori informazioni, cfr. Gruppo di lavoro articolo 29 per la protezione dei dati (2017b).

([14]) 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 (direttiva di polizia) (GU L 119 del 4.5.2016, pag. 89), articolo 10.

in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale».

«Nell'effettuare le verifiche di frontiera, le guardie di frontiera **non esercitano** verso le persone **discriminazioni** fondate sul sesso, la razza o l'origine etnica, la religione o le convinzioni, la disabilità, l'età o l'orientamento sessuale».

Articolo 7 del codice frontiere Schengen

Il divieto di discriminazione non significa che le caratteristiche personali non possano essere utilizzate come fattori legittimi per la profilazione nell'ambito delle indagini penali o dei controlli di frontiera (cfr. sezione 2.3); per poterle utilizzare, tuttavia, devono esservi ragionevoli motivi di sospetto basati su informazioni diverse dai motivi protetti. Questa condizione sussiste, ad esempio quando un individuo corrisponde a una specifica descrizione di un sospetto o il suo aspetto non corrisponde alle informazioni contenute nel suo documento di viaggio ([15]).

Sotto la lente: discriminazione fondata sulla nazionalità

L'articolo 21 della Carta dei diritti fondamentali dell'UE **limita il divieto di discriminazione fondata sulla nazionalità ai cittadini dell'UE**. La direttiva sull'uguaglianza razziale non include tra i motivi protetti la nazionalità.

Gli Stati membri hanno tuttavia ampliato la portata del divieto di discriminazione così che esso si applichi in vari modi anche alla nazionalità, riconoscendo che la nazionalità è talvolta utilizzata come indicatore indiretto della razza, dell'origine etnica o della religione. In alcuni di questi casi, «le differenze di trattamento fondate sulla nazionalità [... risultano essere] in violazione della legislazione che vieta la discriminazione fondata su questi motivi» [cfr. Rete europea di esperti giuridici in materia di parità di genere e non discriminazione (2016), pag. 99]. Nella pratica, la discriminazione fondata sulla nazionalità e la discriminazione fondata sull'origine etnica sono spesso difficilmente distinguibili.

Il fatto che la nazionalità non sia esplicitamente menzionata come potenziale motivo di discriminazione nell'articolo 21 della Carta rispecchia in primo luogo il

([15]) Regno Unito, Camera dei Lord (2006), Lord Scott, pareri dei Lord con funzioni giurisdizionali di appello per la sentenza nella causa *R (on the application of Gillan e al.) c. Commissioner of Police for the Metropolis e al.*, [2006] UKHL 12, 8 marzo 2006, paragrafo 67.

diverso status di cui godono i cittadini dell'UE (e le altre persone che beneficiano del diritto alla libera circolazione ai sensi del diritto dell'UE) rispetto ai cittadini di paesi terzi a norma del diritto dell'UE. Questo aspetto riveste particolare importanza nelle procedure di frontiera, in cui la cittadinanza è decisiva per stabilire se una persona sarà soggetta a verifiche approfondite o debba essere in possesso di un visto per entrare nello spazio Schengen o transitarvi.

Allo stesso tempo, il fatto di sottoporre sistematicamente a verifiche in seconda linea tutte le persone di una determinata nazionalità rischia di diventare una discriminazione. La nazionalità può legittimamente rientrare nei profili di rischio volti a individuare la migrazione irregolare o presunte vittime della tratta di esseri umani, ma non deve costituire l'unico o principale fattore sulla base del quale effettuare una verifica in seconda linea. Inoltre, come in altri contesti, il trattamento differenziato in base alla nazionalità diventa discriminatorio e, di conseguenza, illecito quando viene utilizzato come indicatore indiretto per operare discriminazioni fondate su motivi protetti che sono strettamente collegati alla nazionalità, quali la razza, l'origine etnica o la religione.

Nei suoi principi e orientamenti raccomandati in materia di diritti umani alle frontiere internazionali, l'Ufficio dell'Alto commissario delle Nazioni Unite per i diritti umani include la nazionalità tra i motivi protetti che non dovrebbero essere utilizzati per la profilazione dei migranti (principio 8).

Giurisprudenza

Nella causa *Rosalind Williams Lecraft c. Spain*, un agente di polizia aveva fermato una donna in una stazione ferroviaria spagnola e le aveva chiesto i documenti di identità. La donna aveva domandato all'agente perché avesse fermato solo lei e aveva ricevuto la seguente risposta: «Perché lei è nera». Nelle sue conclusioni, il Comitato dei diritti umani delle Nazioni Unite ha osservato che in linea di massima è legittimo effettuare controlli d'identità nell'interesse della sicurezza pubblica e a fini di prevenzione della criminalità e controllo dell'immigrazione irregolare, ma ha anche sottolineato che «quando le autorità effettuano tali controlli le caratteristiche fisiche o etniche delle persone individuate non devono essere considerate un indizio della loro presenza illegale nel paese, né tali controlli d'identità devono riguardare esclusivamente persone che hanno specifiche caratteristiche

fisiche od origini etniche. Infatti, non solo si produrrebbero effetti negativi sulla dignità dei soggetti interessati, ma si contribuirebbe a diffondere un atteggiamento xenofobico tra la popolazione generale, mostrando peraltro un atteggiamento incoerente rispetto alla necessità di un'efficace politica volta a combattere la discriminazione razziale».

Una denuncia analoga è stata presentata nel 2017 alla Corte europea dei diritti dell'uomo (Corte EDU) in relazione al trattamento di un cittadino pakistano durante e dopo un fermo di polizia in Spagna. La Corte dovrà decidere se il richiedente abbia subito una discriminazione fondata sull'origine etnica durante il controllo d'identità e se vi sia stata una violazione dell'articolo 8 (diritto al rispetto della vita privata e familiare) in relazione alla mancata adozione, da parte delle autorità spagnole, di tutte le misure ragionevoli per individuare eventuali motivi razzisti alla base del fermo. Al momento della stesura del presente documento, la sentenza non è ancora stata pronunciata.

Per ulteriori informazioni, cfr. UNHRC, Rosalind Williams Lecraft c. Spain, Comm. n. 1493/2006 e Corte EDU, Zeshan Muhammad c. Spain, n. 34085/17, proposto il 6 maggio 2017. Cfr. anche FRA e Consiglio d'Europa (2018).

Nella causa *B.S. c. Spain*, una lavoratrice del sesso di origine nigeriana legalmente residente in Spagna ha lamentato di aver subito dalla polizia spagnola maltrattamenti fisici e verbali fondati sulla razza, sul genere e sulla professione. La ricorrente sosteneva di aver subito ripetuti controlli di polizia e insulti razzisti e sessisti, diversamente da altri lavoratori del sesso di origine europea. Due interventi di terzi presentati dal Centro AIRE e dall'Unità ricerca sociale europea dell'Università di Barcellona hanno chiesto alla Corte EDU di riconoscere la discriminazione intersettoriale. La Corte ha riscontrato una violazione dell'articolo 3 (divieto di trattamenti inumani e degradanti) e ha proceduto inoltre ad esaminare separatamente l'eventuale assenza di indagine in merito alla possibile sussistenza di un nesso di causalità tra i presunti atteggiamenti razzisti e gli atti violenti della polizia. Al riguardo, la Corte EDU ha constatato una violazione dell'articolo 14 (divieto di discriminazione), stante il fatto che i tribunali nazionali non avevano tenuto conto della particolare vulnerabilità della ricorrente, in quanto donna africana che lavorava come prostituta. Pur adottando un approccio intersettoriale, la sentenza non ha utilizzato il termine «intersettorialità».

Per ulteriori informazioni, cfr. Corte EDU, B.S. c. Spain, n. 47159/08, 24 luglio 2012.

Sotto la lente: l'onere della prova

Nel 2016 la Corte di cassazione francese si è pronunciata per la prima volta sulla questione dei controlli d'identità discriminatori. Nelle sue *sentenze del 9 novembre 2016*, la Corte ha stabilito che la polizia aveva sottoposto a controlli d'identità discriminatori tre dei 13 ricorrenti, uomini di origine africana o araba, constatando la responsabilità dello Stato nei casi in questione e condannandolo a versare un risarcimento ai tre ricorrenti. In altri otto casi, la Corte ha invece stabilito che i controlli d'identità contestati erano leciti, in quanto si basavano su elementi oggettivi e quindi non discriminatori. I giudici non si sono pronunciati sugli altri due casi, rinviandoli ai tribunali di grado inferiore per un nuovo processo.

La Corte ha inoltre fornito chiarimenti sull'onere della prova in casi di questo genere. I controlli d'identità non vengono registrati quando non conducono a procedimenti giudiziari o amministrativi. La Corte ha spiegato che i ricorrenti dovrebbero fornire prove dell'esistenza di una discriminazione, mentre la polizia deve dimostrare l'assenza di disparità di trattamento nell'esecuzione dei controlli d'identità o una differenza di trattamento giustificata da elementi oggettivi.

Inoltre, la Corte ha ritenuto che i giudici possano prendere in considerazione, come prova, studi e informazioni statistiche da cui risulti la frequenza dei controlli d'identità effettuati, per motivi discriminatori, sullo stesso gruppo di popolazione del ricorrente (ossia le minoranze visibili, determinate da caratteristiche fisiche derivanti da un'origine etnica reale o presunta). Tuttavia, questa prova non basta da sola a far presumere l'esistenza di una discriminazione.

Il giudice ha quindi ritenuto che un controllo d'identità basato su caratteristiche fisiche associate a un'origine etnica effettiva o presunta, senza una preventiva giustificazione oggettiva, sia discriminatorio e rappresenti una colpa grave che, in questi tre casi, ha comportato la responsabilità dello Stato.

Per ulteriori informazioni, cfr. Francia, Cour de Cassation, Décision 1245, 9 novembre 2016.

1.2.2. Diritto al rispetto della vita privata e alla protezione dei dati personali

A norma della legislazione dell'UE, il diritto al rispetto della vita privata (articolo 7 della Carta) e il diritto alla protezione dei dati personali (articolo 8 della Carta) sono distinti, seppur strettamente connessi. Il diritto alla vita privata (o diritto alla privacy) è un diritto più ampio, che vieta *qualsiasi ingerenza* nella vita privata di un individuo. Per vita privata non si intende semplicemente ciò che un individuo desidera mantenere riservato, ma anche il modo in cui un individuo esprime la propria personalità, ad esempio la scelta delle persone con cui interagire o del modo di vestire. La protezione dei dati personali è limitata alla valutazione della liceità in relazione al *trattamento dei dati personali* ([16]). Nel caso in cui non si faccia riferimento in modo specifico al diritto dell'UE, i due termini sono utilizzati in modo intercambiabile ai fini della presente guida. Tali diritti non sono assoluti e possono essere limitati in determinate circostanze (cfr. articolo 8 della CEDU e articolo 52 della Carta).

Diritto alla privacy e diritto alla protezione dei dati personali: che cosa dice la legge?

«1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

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

Articolo 8 della convenzione europea dei diritti dell'uomo

«Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

Articolo 7 della Carta dei diritti fondamentali dell'Unione europea

«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro

([16]) FRA, GEPD e Consiglio d'Europa (2018).

fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica [...]».

Articolo 8 della Carta dei diritti fondamentali dell'Unione europea

«1. L'interessato ha il diritto di non essere sottoposto a una decisione **basata unicamente sul trattamento automatizzato**, compresa la profilazione, **che produca effetti giuridici** che lo riguardano **o** che **incida in modo analogo significativamente sulla sua persona**.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto [...];

b) sia autorizzata dal diritto [...] che precisa [...] misure adeguate a tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato; o

c) si basi sul consenso esplicito dell'interessato».

Articolo 22, paragrafi 1 e 2, del regolamento generale sulla protezione dei dati

«Gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento».

Articolo 11, paragrafo 1, della direttiva di polizia

Il diritto derivato dell'UE tratta in modo approfondito il diritto alla privacy e alla protezione dei dati personali. Due atti legislativi specificano le modalità con cui si possono effettuare la raccolta e il trattamento dei dati personali: il regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati, GDPR), che stabilisce i principi generali e le garanzie che si applicano al trattamento dei dati personali, e la direttiva (UE) 2016/680 (direttiva di polizia), che stabilisce più in particolare le norme per il trattamento dei dati personali nell'ambito delle operazioni di contrasto a fini di prevenzione, indagine, accertamento e perseguimento di reati. I principi più importanti e alcune differenze fondamentali tra i due atti sono illustrati nella tabella 2. Le leggi che istituiscono le grandi banche dati dell'UE utilizzate per la gestione delle frontiere, quali il sistema di informazione visti (VIS), il sistema di ingressi/uscite (EES) o il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), contengono anch'esse disposizioni specifiche dedicate alla protezione dei dati (cfr. la sezione 3.2 sulle banche dati su larga scala).

Tabella 2: Prescrizioni in materia di protezione dei dati — Differenze tra la direttiva di polizia e il GDPR

Principio di protezione dei dati	GDPR	Direttiva di polizia
Liceità, correttezza, trasparenza	I dati personali devono essere trattati in modo lecito, corretto **e trasparente**.	I dati personali devono essere trattati in modo lecito e corretto.
Limitazione della finalità	I dati personali raccolti per una determinata finalità non dovrebbero essere sottoposti a ulteriore trattamento per una finalità incompatibile; **un ulteriore trattamento a fini scientifici, storici o statistici non è incompatibile con le finalità iniziali**.	I dati personali raccolti per una determinata finalità non dovrebbero essere sottoposti a ulteriore trattamento per una finalità incompatibile; altre finalità non sono incompatibili con la finalità iniziale purché tale trattamento sia autorizzato dalla legge e sia necessario e proporzionato.
Minimizzazione dei dati	I dati personali raccolti devono essere adeguati, pertinenti **e limitati a quanto necessario** rispetto alle finalità per le quali sono stati raccolti.	I dati personali raccolti devono essere adeguati, pertinenti e **non eccedenti** rispetto alle finalità per le quali sono stati raccolti.
Limitazione della conservazione	I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per il periodo di tempo necessario al conseguimento della finalità per la quale sono stati raccolti; i **dati personali possono essere conservati per periodi più lunghi a fini scientifici, storici o statistici**.	I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per il periodo di tempo necessario al conseguimento della finalità per la quale sono stati raccolti.
Esattezza	I dati personali raccolti devono essere esatti e aggiornati. I dati personali non corretti o inesatti devono essere cancellati o rettificati.	
Integrità e riservatezza	I dati personali devono essere protetti da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.	

Fonte: *FRA (2018)*

Esempi

Una guardia di frontiera invia l'elenco dei passeggeri di un aereo a persone non autorizzate. Una volta condivisi, tali dati personali possono essere utilizzati per altre finalità e/o per finalità private. Si tratta di una chiara violazione dei principi di protezione dei dati.

Una funzionaria di polizia esce dal suo ufficio lasciando visualizzato sullo schermo del computer un elenco di dati personali relativi a sospetti. Questo comportamento lede il principio della sicurezza dei dati personali e costituisce quindi una violazione dei principi di protezione dei dati.

Giurisprudenza

Le sentenze degli organi giurisdizionali forniscono orientamenti sul modo in cui tali principi sono applicati nella pratica.

Limitazione della finalità

Nella causa *Heinz Huber c. Bundesrepublik Deutschland*, la Corte di giustizia dell'Unione europea ha valutato la legittimità del registro centrale tedesco degli stranieri (*Auslanderzentralregister, AZR*) che contiene determinati dati personali relativi a cittadini stranieri — di Stati membri dell'UE e di paesi terzi — che soggiornano in Germania per oltre tre mesi. La Corte ha concluso che i dati raccolti per una finalità specifica non possono essere utilizzati per finalità diverse. La Corte ha stabilito che l'AZR è uno strumento legittimo per applicare le norme sulla residenza e che la differenza di trattamento tra cittadini stranieri e cittadini tedeschi, su cui vengono conservati meno dati, è giustificata alla luce della finalità perseguita; ha tuttavia rilevato che i dati conservati nell'AZR non possono essere utilizzati per il contrasto alla criminalità in generale, poiché si tratta di una finalità diversa da quella per cui i dati sono stati originariamente raccolti.

Per ulteriori informazioni, cfr. CGUE, causa C-524/06, Heinz Huber c. Bundesrepublik Deutschland, 16 dicembre 2008.

Limitazione della conservazione

Nel caso *S. e Marper c. Regno Unito* i ricorrenti avevano chiesto la cancellazione dei rispettivi dati (impronte digitali, campioni di cellule e profili del DNA) dalla banca dati del DNA utilizzata per l'identificazione dei criminali nel Regno Unito. I processi a loro carico si erano conclusi con un'assoluzione e i ricorrenti erano preoccupati dei possibili utilizzi attuali e futuri dei loro dati. La polizia aveva rifiutato di procedere alla cancellazione. La Corte EDU ha concluso che la conservazione per una durata illimitata dei campioni di DNA di persone arrestate ma successivamente assolte o che hanno beneficiato di un'archiviazione costituisce una violazione del diritto al rispetto della vita privata. La Corte ha evidenziato il rischio di stigmatizzazione, in quanto i dati di persone non riconosciute colpevoli di nessun reato erano trattati alla stregua dei dati di condannati; ha inoltre riconosciuto che il pregiudizio potenziale causato dalla conservazione di tali dati è particolarmente forte nel caso di minori, vista l'importanza del loro sviluppo e integrazione nella società.

Per ulteriori informazioni, cfr. Corte EDU, S. e Marper c. Regno Unito, n. 30562/04 e n. 30566/04, 4 dicembre 2008.

Per la raccolta e il trattamento di dati personali a fini di profilazione, le autorità di contrasto e di gestione delle frontiere devono rispettare quattro criteri giuridici essenziali. La raccolta e il trattamento dei dati devono:

- **essere definiti e regolamentati per legge (*base giuridica*):** qualsiasi limitazione del diritto al rispetto della vita privata e del diritto alla protezione dei dati deve essere sancita dalla legge e rispettare il contenuto essenziale di tali diritti. Le norme di diritto devono rispettare i principi di chiarezza e qualità, quindi i cittadini devono potervi accedere e le norme devono essere sufficientemente chiare e precise affinché i cittadini ne comprendano l'applicazione e le conseguenze;

- **avere una finalità valida, lecita e appropriata (*finalità legittima*):** le finalità legittime sono definite dalla legge e non possono essere ampliate. Possono riguardare la sicurezza nazionale, la salute, l'ordine pubblico o la prevenzione della criminalità;

- **essere indispensabili al raggiungimento di tale finalità (*necessità*):** il trattamento dei dati personali dovrebbe essere limitato a quanto necessario rispetto alla finalità per la quale sono stati raccolti;

- **non essere eccessivi (*proporzionalità*):** le autorità che effettuano il trattamento di dati personali devono ottenere un giusto equilibrio tra la finalità e i mezzi utilizzati per conseguirla: il valore aggiunto del trattamento non dovrebbe quindi superare il suo potenziale impatto negativo.

Il capitolo 3 spiega in che modo questi principi possono essere applicati nella pratica.

La figura 2 indica come usare questi principi per valutare se un'azione possa violare il diritto al rispetto della vita privata e familiare e il diritto alla protezione dei dati (cfr. anche sezione 2.3.3 sui meccanismi di reclamo). Il caso *Gillan and Quinton c. the United Kingdom*, riguardante l'esercizio dei poteri di fermo e perquisizione, illustra in che modo la Corte EDU abbia applicato tali principi per stabilire se vi fosse stata una violazione del diritto alla protezione dei dati personali e alla privacy (cfr. riquadro sulla giurisprudenza).

Figura 2: Violazione della privacy e della protezione dei dati — Il processo di valutazione

Fonte: *FRA (2018) sulla base di Consiglio d'Europa (2003), The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human rights*

Giurisprudenza

Nel caso *Gillan and Quinton c. the United Kingdom*, i ricorrenti, due cittadini britannici, avevano depositato un ricorso giurisdizionale per contestare la legittimità dei poteri di fermo e perquisizione esercitati nei loro confronti.

La misura adottata è prevista dalla legge? La misura era conforme agli articoli 44-47 della legge sul terrorismo (*Terrorism Act*) del 2000, a norma dei quali: 1) per la prevenzione di atti di terrorismo, i funzionari di polizia di grado elevato potevano autorizzare qualsiasi operatore di polizia in divisa presente in una determinata zona ad effettuare operazioni di fermo e perquisizione; 2) le autorizzazioni erano soggette a conferma da parte del segretariodi Stato ed erano soggette a scadenza, ma potevano essere rinnovate all'infinito; 3) sebbene lo scopo di tali operazioni di perquisizione fosse trovare elementi che potessero essere utilizzati per atti di terrorismo, le operazioni di fermo e perquisizione non dovevano necessariamente essere basate sul sospetto che la persona o le persone fermate avessero con sé elementi di tale genere; e 4) le persone che rifiutavano di farsi perquisire erano punibili con la reclusione e/o un'ammenda (*Gillan and Quinton*, punti 76-80).

La misura adottata interferisce con la protezione della privacy e/o dei dati? L'uso di poteri coercitivi da parte delle autorità di contrasto per fermare una persona ed effettuare perquisizioni sui suoi indumenti e sui suoi effetti personali rappresenta un'evidente interferenza con il diritto al rispetto della vita privata, la cui gravità è amplificata dalla pubblica esposizione di informazioni personali, che comporta umiliazione e imbarazzo (*Gillan and Quinton*, punto 63).

Valutazione della proporzionalità e della necessità: la Corte ha espresso una serie di preoccupazioni in merito alla proporzionalità e alla necessità della legge (*Gillan and Quinton*, punti 80-86):

- la disposizione legislativa applicabile all'autorizzazione dei fermi non imponeva adempimenti gravosi;
- l'ampiezza dei poteri legali è tale per cui la persona che cerchi di dimostrare che un'autorizzazione o conferma travalica i poteri delle autorità competenti (*ultra vires*) o configura un abuso di potere incontra enormi ostacoli;

- le zone geografiche coperte dall'autorizzazione erano molto ampie e la durata è stata più volte prorogata, riducendo il carattere mirato dell'autorizzazione;
- le restrizioni alla discrezionalità dei singoli funzionari erano più formali che sostanziali;
- vi erano scarse possibilità di ricorso giurisdizionale in quanto il funzionario che effettuava il fermo non era tenuto a dimostrare la ragionevolezza del proprio sospetto; dimostrare che vi era stato un esercizio improprio del potere era perciò quasi impossibile.

Queste considerazioni hanno indotto la Corte EDU a concludere che gli articoli in questione della legge sul terrorismo non erano «né sufficientemente circoscritti né accompagnati da garanzie legali adeguate contro gli abusi» e quindi violavano l'articolo 8 della CEDU.

Per ulteriori informazioni, cfr. Corte EDU, Gillan and Quinton c. the United Kingdom, n. 4158/05, 12 gennaio 2010.

I requisiti giuridici in materia di profilazione stabiliti nel quadro giuridico riformato dell'UE in materia di protezione dei dati sono descritti dettagliatamente nel capitolo 3.

1.3. Quali sono i potenziali effetti negativi della profilazione illecita sulle attività di contrasto e gestione delle frontiere?

La profilazione basata unicamente su categorie generali quali la razza, l'origine etnica o la religione non solo è illecita, ma può anche nuocere all'efficacia delle attività di polizia e gestione delle frontiere. La presente sezione esamina due potenziali conseguenze negative:

- la difficoltà maggiore riguarda le tensioni che può creare nei rapporti con le comunità. La profilazione può generare risentimento tra le comunità particolarmente interessate da tale pratica e ridurre la fiducia nelle autorità di polizia e di gestione delle frontiere, il che a sua volta può compromettere l'efficacia dei metodi basati sulla cooperazione pubblica;

- vi sono inoltre dubbi circa l'efficacia dell'uso di categorie generali di profili nella gestione delle frontiere o nell'attività di contrasto, ad esempio se per effetto di tale uso una persona viene sospettata ingiustamente ([17]).

Inoltre, quando la profilazione è effettuata in modo illecito, le autorità sono passibili di denuncia o azione legale, che può assumere la forma di una supervisione attuata dalle autorità competenti per i reclami, sia interne alla polizia che specializzate, o di un intervento delle autorità di vigilanza o del sistema dei tribunali civili e penali (cfr. sezione 2.3). Singoli funzionari e dirigenti di medio livello possono essere soggetti a sanzioni amministrative e/o penali in conseguenza della loro partecipazione alla profilazione illecita o accettazione passiva di tale pratica; ciò può logorare le risorse e il morale delle autorità e nuocere alla loro reputazione.

Punti salienti

- **La profilazione illecita mina la fiducia** nelle autorità di contrasto e di gestione delle frontiere e può comportare un deterioramento dei rapporti con le comunità locali.
- Vi sono **dubbi circa la reale efficacia dell'utilizzo di profili generali** per l'accertamento di reati o nella gestione delle frontiere. Gli elementi esistenti non permettono di stabilire con certezza se la profilazione effettuata utilizzando profili generali migliori il tasso di successo delle attività di contrasto o di gestione delle frontiere.

1.3.1. Impatto sulla fiducia nella polizia e nelle autorità di gestione delle frontiere e sui buoni rapporti con le comunità

Le ricerche effettuate evidenziano l'impatto negativo che l'uso di profili generali può avere sugli individui interessati e sulle comunità a cui appartengono ([18]). Il riquadro seguente contiene le reazioni di alcune persone a un fermo e perquisizione o a una verifica di frontiera.

([17]) FRA (2017d), pag. 51.

([18]) FRA (2017d).

Esempi

Impatto delle operazioni di fermo e perquisizione e delle verifiche di frontiera sugli individui

1. Fermi di polizia — Keskinen, S. e al. (2018)

Tra il 2015 e il 2017, la Scuola svedese di scienze sociali presso l'università di Helsinki ha intervistato 185 persone circa le loro esperienze in materia di profilazione etnica. Dalla ricerca è emerso che per la maggior parte degli intervistati i fermi sono stati esperienze sgradevoli, fastidiose o umilianti. Di seguito sono riportati alcuni stralci delle testimonianze degli intervistati.

«Dopo un po', un altro poliziotto mi ha fermata di nuovo [...] mentre camminavo per strada con due amiche bianche, una finlandese e l'altra olandese. È andata esattamente nello stesso modo[...] mi ha fatto la stessa domanda. Mi sono girate le scatole: non capivo perché prendessero di mira proprio me. Gliel'ho chiesto e loro mi hanno risposto semplicemente che stavano facendo il loro lavoro» (donna di età compresa tra 30 e 39 anni, paese africano).

«Una volta mia mamma e mio fratello erano in giro in città e i poliziotti li hanno fermati, chiedendo loro i passaporti. Per me questa è profilazione etnica. Allora mio fratello [ha detto in finlandese] "Non abbiamo il passaporto, non lo portiamo sempre con noi". A quel punto, quando hanno visto che parlava bene il finlandese, hanno detto qualcosa tipo "Oh, non fa niente". Mi sono arrabbiata perché io lo so che la profilazione etnica è illegale, ma mia mamma e mio fratello no. Secondo me avevano subito un abuso, perciò mi sono molto arrabbiata. Una volta gli ho detto che quello che gli era successo era illegale, perché per loro era ovvio che erano stati fermati perché [...] dall'aspetto non erano finlandesi, erano stranieri» (donna di età compresa tra 20 e 29 anni, Somalia-Finlandia).

«Hanno sempre più o meno la stessa descrizione. Allora mi viene da pensare che se da 11 anni cercano la stessa persona che è riuscita a non farsi prendere, significa che non stanno facendo un buon lavoro, perché la descrizione che hanno [al controllo di frontiera] è sempre più o meno la stessa, e io

corrispondo sempre a quella descrizione [risate]» (uomo, poco più di 30 anni, paese africano-Finlandia).

Per ulteriori informazioni, cfr. Keskinen, S. e al. (2018), The Stopped – Ethnic Profiling in Finland.

2. Verifiche di frontiera – FRA (2014a e 2014b)
«Capisco perché [la guardia di frontiera] mi ha fermato, ma non per questo doveva mandarmi qui [verifica in seconda linea/posto di polizia] o trattarmi come un delinquente. Lo fanno con tutti quelli che vengono dall'Europa orientale» (passeggero serbo intervistato all'aeroporto di Francoforte).

Domanda: «Com'è stato il trattamento che ha ricevuto alla verifica in prima linea?».

Risposta: «Non penso che sia stato buono. È stato umiliante. Mi ha trattato male. Mi ha preso il passaporto, gli ha dato un'occhiata e ha subito chiamato l'immigrazione. Mi ha fatto delle domande e ha alzato la voce, ma non capivo niente. Mi hanno fatto uscire dalla fila ma non mi hanno rispettato e mi hanno spaventato».

D: «Perché si è sentito spaventato o umiliato?».

R: «Perché non sapevo che cosa sarebbe successo e non mi spiegavano niente. Intorno c'erano molte persone e la guardia parlava con altre guardie ma con me non parlava. Poi ho dovuto aspettare e continuavo a non sapere perché mi trovassi lì» (passeggero angolano intervistato a Schiphol).

«Sul serio, le capisco [...] le guardie di frontiera. Anche per loro dev'essere difficile lavorare per ore e ore nella cabina! Per questo, qualche volta mostrano atteggiamenti negativi nei confronti di persone come noi, ad esempio si mettono a urlare» (cittadino turco, autotrasportatore che attraversa spesso la frontiera, Kipi).

La somma di queste esperienze individuali può tradursi in effetti di gruppo negativi ([19]), che possono contribuire a un marcato peggioramento dei rapporti tra i funzionari di polizia e gestione delle frontiere e i membri di comunità di minoranza sottoposte a un numero elevato di fermi e perquisizioni o verifiche di frontiera approfondite.

Caso di studio

Il ruolo dei fermi e perquisizioni nei disordini pubblici (Regno Unito 2011 e Francia 2005)

A seguito dei disordini verificatisi in diverse grandi città del Regno Unito nell'agosto del 2011, la London School of Economics e il quotidiano Guardian hanno intervistato 270 persone chiedendo loro perché avessero partecipato ai tumulti. Lo studio ha individuato nella sfiducia e nell'avversione nei confronti delle forze di polizia un fattore significativo e ha riscontrato che «le rimostranze più comuni riguardavano l'esperienza quotidiana delle persone rispetto alle attività di polizia: molti esprimevano una profonda frustrazione per il modo in cui le persone della loro comunità erano sottoposte a fermi e perquisizioni».

Per ulteriori informazioni, cfr. London School of Economics (2011).

Dinamiche analoghe sono state individuate in altri Stati membri dell'UE. In Francia, l'evento scatenante dei disordini del novembre 2005 è stato la morte accidentale di due giovani appartenenti a una minoranza durante un inseguimento della polizia [cfr. Jobard (2008) e Body-Gendrot (2016)].

Per ulteriori informazioni, cfr. Hörnqvist (2016).

Un aspetto collegato da tenere presente è che la profilazione può determinare una maggiore ostilità nelle altre interazioni con la polizia o altre autorità di contrasto, aumentando la probabilità che le interazioni di routine degenerino rapidamente in manifestazioni aggressive e conflittuali, pericolose sia per i funzionari che per i membri della comunità.

([19]) Nazioni Unite (2007), punto 57.

Più in generale, ricerche recenti indicano che chi viene fermato, arrestato, condannato o incarcerato tende ad evitare di rivolgersi a servizi pubblici al di fuori del sistema di giustizia penale, quali l'assistenza sanitaria, i servizi per l'occupazione e l'istruzione ([20]). Senza voler minare i motivi legittimi che portano all'arresto di persone condannate, occorre tenere presente che l'esclusione di segmenti già emarginati della popolazione da tali servizi può pregiudicare l'inclusione sociale e l'integrazione delle minoranze.

Sotto la lente: risultati dell'indagine UE-MIDIS II della FRA

Nel 2015 e 2016, la FRA ha raccolto informazioni da oltre 25 500 soggetti appartenenti a diverse minoranze etniche o immigrati nei 28 Stati membri dell'UE.

Quali informazioni sono state raccolte?

In relazione alla profilazione, è stato chiesto agli intervistati se ritenevano di essere stati fermati dalla polizia a causa della loro origine migratoria o dell'appartenenza a minoranze etniche; inoltre, è stato chiesto loro come erano stati trattati dalla polizia e se avevano avuto esperienze di aggressione fisica da parte della polizia. Non sono state chieste informazioni circa le esperienze nell'ambito della gestione delle frontiere.

Che cosa indicano i risultati?

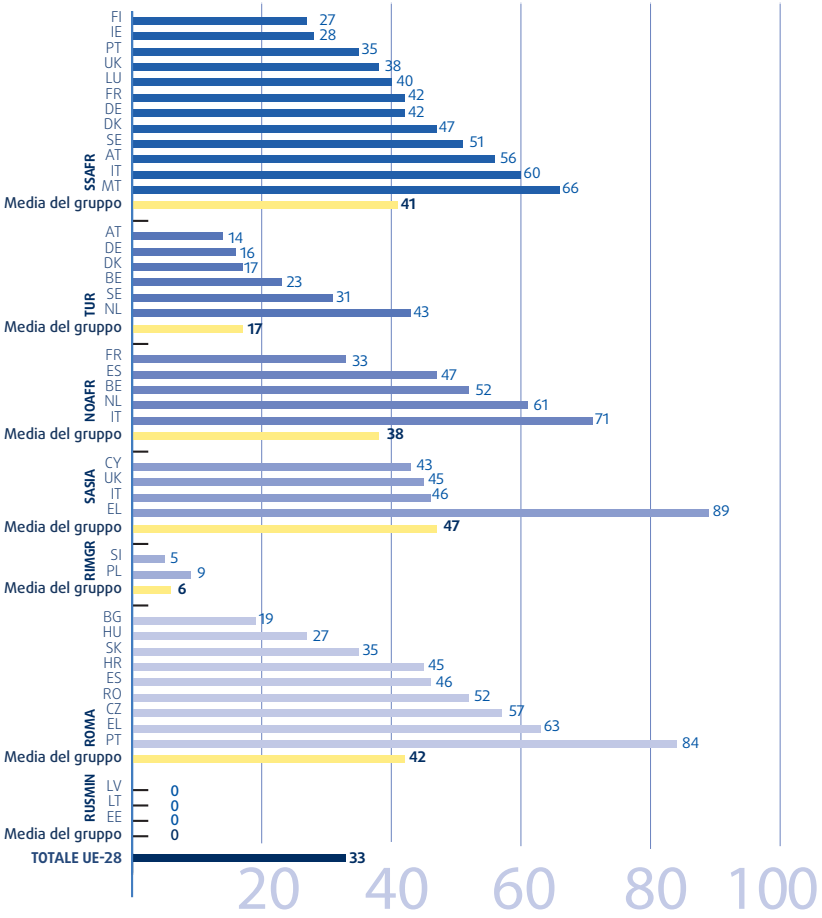
Fermi e origine etnica: i risultati indicano che il 26 % delle persone intervistate per UE-MIDIS II è stato fermato dalla polizia nei cinque anni precedenti l'indagine. Delle persone fermate nei cinque anni precedenti l'indagine, il 33 % ha affermato che il fermo era stato motivato dall'origine etnica e migratoria.

Percezione della discriminazione: in media, quasi la metà degli intervistati originari dell'Asia (47 %), dell'Africa sub-sahariana (41 %) e del Nordafrica (38 %) fermati durante il periodo considerato ha dichiarato che il fermo era stato motivato dall'origine migratoria o dall'appartenenza a una minoranza etnica. Anche tra i rom intervistati che erano stati fermati, quasi la metà (42 %) riteneva che il fermo fosse stato motivato dall'origine etnica.

([20]) Brayne, S. (2014), pagg. 367–391.

Questa percentuale è risultata invece molto più bassa tra gli intervistati fermati di origine turca (17 %) (cfr. figura 3).

Figura 3: Ultimo fermo di polizia percepito come motivato dalla profilazione etnica tra coloro che sono stati fermati nei cinque anni precedenti l'indagine, per Stato membro dell'UE e gruppo interessato (%) [a, b, c, d]



Note: [a] *tra gli intervistati che sono stati fermati dalla polizia nei cinque anni precedenti l'indagine (n = 6 787); risultati ponderati.*

[b] *I risultati basati su un basso numero di risposte sono statisticamente meno affidabili. Pertanto, i risultati basati su un numero di osservazioni non ponderate compreso tra 20 e 49 in un totale di gruppo o su cellule con meno di 20 osservazioni non ponderate sono annotati fra parentesi. I risultati basati su meno di 20 osservazioni non ponderate in un totale di gruppo non sono stati pubblicati.*

[c] *Domande: «Negli ultimi cinque anni in [PAESE] (o dal momento in cui è arrivato in [PAESE]), è mai stato fermato, perquisito o interrogato dalle forze dell'ordine?»; «Crede che L'ULTIMA VOLTA che l'hanno fermata sia stato a causa della Sua origine etnica o di immigrazione?».*

[d] *Gli acronimi dei gruppi si riferiscono agli immigrati provenienti da [paese/regione] e ai loro discendenti: TUR = Turchia, SSAFR = Africa subsahariana, NOAFR = Nordafrica, SASIA = Asia meridionale, ASIA = Asia, ROMA = minoranza rom.*

Fonte: *FRA (2017b)*

Rispetto: i risultati mostrano che tra gli intervistati che erano stati fermati dalla polizia nei cinque anni precedenti all'indagine, la maggioranza (59 %) riteneva di avere ricevuto un trattamento rispettoso (25 % «molto rispettoso», 34 % «abbastanza rispettoso»). Un intervistato su quattro (24 %) ha dichiarato che il trattamento ricevuto dalle forze dell'ordine era stato «né rispettoso, né irrispettoso». Il 17 % ha dichiarato invece che il trattamento ricevuto dalle forze dell'ordine era stato irrispettoso (8 % «abbastanza irrispettoso» e 9 % «molto irrispettoso»). Gli intervistati rom e gli intervistati di origine nordafricana che erano stati fermati hanno indicato di aver ricevuto un trattamento irrispettoso dalla polizia durante l'ultimo fermo (rispettivamente 25 % e 21 %) in misura maggiore rispetto agli altri gruppi interessati.

Per ulteriori informazioni, cfr. FRA (2017b).

Sotto la lente: importanza e utilità della raccolta di dati sui fermi di polizia

Dei 28 Stati membri dell'UE, il Regno Unito è attualmente l'unico in cui la raccolta di dati sui fermi di polizia include sistematicamente informazioni sull'origine etnica delle persone fermate (cfr. anche sezione 2.2.5 e sezione 2.3.1).

I dati raccolti misurano il «tasso di fermi e perquisizioni» per i diversi gruppi etnici in Inghilterra e nel Galles. Le categorie etniche utilizzate sono quelle elencate nel censimento del Regno Unito a partire dal 2001. Il censimento ha individuato 16 categorie, ordinate in cinque gruppi più ampi:

- bianchi: inglesi/gallesi/scozzesi/nordirlandesi/britannici; irlandesi; bianchi di qualsiasi altra origine;
- gruppi etnici misti/multipli: caraibici bianchi e neri; africani bianchi e neri; bianchi e asiatici; e qualsiasi altra origine etnica mista/multipla:

- asiatici/britannici asiatici: indiani; pakistani; bengalesi; e qualsiasi altra origine asiatica;
- neri/africani/caraibici/britannici neri: africani; caraibici; e qualsiasi altra origine nera/africana/caraibica;
- altri gruppi etnici: cinesi; e altri gruppi etnici.

I dati raccolti sui fermi e sulle perquisizioni mettono a confronto il numero di persone di un particolare gruppo etnico fermate e perquisite con il numero totale di persone di quel gruppo etnico che vivono in una determinata zona e calcolano quindi un tasso per 1 000 persone.

Per il 2016-2017 l'analisi dei dati raccolti indica che vi sono stati quattro fermi ogni 1 000 persone tra i bianchi, mentre tra i neri i fermi sono stati 29 ogni 1 000 persone. I dati indicano inoltre che i tassi più elevati sono stati registrati nei tre gruppi etnici neri: altri neri (70 fermi ogni 1 000 persone), caraibici neri (28 ogni 1 000 persone) e africani neri (19 ogni 1 000 persone).

In mancanza di prove ricavate da dati disaggregati, è difficile dimostrare se vi siano differenze nell'attività di polizia nei confronti di particolari gruppi etnici e, in caso affermativo, se tali differenze possano essere il risultato di prassi di profilazione discriminatorie. In Inghilterra e nel Galles i dati disaggregati, suddivisi per forza di polizia, sono di dominio pubblico e permettono quindi di individuare differenze tra le varie forze che possono essere giustificate in quanto legittime o essere utilizzate per identificare eventuali discriminazioni nelle prassi di polizia. I dati sono utilizzati anche a livello dei singoli agenti di polizia per identificare eventuali prassi discriminatorie nel loro operato.

Per ulteriori informazioni, cfr. la pagina del governo britannico dedicata a fermi e perquisizioni, il sito dell'Independent Office for Police Conduct e il sito sugli open data in materia di criminalità e attività di polizia dell'Home Office. Cfr. anche Regno Unito (2018). Per indicazioni sulle metodologie di registrazione, cfr. Open Society Justice Initiative (2018b).

Caso di studio

Indagine sui rapporti tra la polizia e la popolazione in Francia

Nel 2016 il difensore civico francese (*Défenseur des droits*), che funge anche da commissione nazionale per le denunce presentate nei confronti della polizia, ha condotto un'indagine riguardante l'accesso ai diritti su un campione rappresentativo di oltre 5 000 persone.

La prima parte della relazione presenta i risultati relativi al comportamento delle autorità di contrasto. Nel complesso, l'indagine rivela buoni rapporti tra la popolazione e la polizia; la grande maggioranza degli intervistati ha dichiarato di avere fiducia nella polizia (82 %).

Per quanto riguarda in particolare i controlli d'identità, l'indagine mostra che la maggior parte delle persone non vi è sottoposta: l'84 % degli intervistati ha dichiarato di non essere stato sottoposto ad alcun controllo negli ultimi cinque anni (90 % delle donne e 77 % degli uomini). Le persone che hanno dichiarato di essere state controllate hanno segnalato in pochi casi comportamenti in contraddizione con la deontologia delle forze di sicurezza durante l'ultimo controllo d'identità, quali l'uso del «tu» (16 %), la brutalità (8 %) o gli insulti (7 %). Il 29 % ha segnalato una mancanza di cortesia e oltre la metà degli intervistati (59 %) che erano stati controllati ha indicato che i motivi del controllo non erano stati spiegati. In generale, i controlli d'identità sono percepiti come più legittimi quando le forze di sicurezza prendono il tempo per spiegare i motivi del controllo.

Dai dati emerge inoltre che gruppi specifici di persone segnalano esperienze più negative. I giovani uomini di età compresa tra 18 e 24 anni hanno una probabilità quasi sette volte maggiore di essere sottoposti a controlli d'identità frequenti (più di cinque volte negli ultimi cinque anni) rispetto alla popolazione nel suo complesso e i giovani uomini percepiti come neri o arabi sono 6-11 volte più interessati da controlli d'identità frequenti rispetto al resto della popolazione maschile. Combinando questi due criteri, risulta che l'80 % degli uomini di età inferiore ai 25 anni e percepiti come arabi o neri è stato controllato almeno una volta negli ultimi cinque anni (rispetto al 16 % degli altri intervistati). Rispetto alla popolazione nel suo complesso, in questo gruppo la probabilità di essere sottoposti a controlli d'identità è 20 volte superiore.

Inoltre, i giovani uomini percepiti come neri o arabi hanno segnalato livelli più elevati di comportamenti problematici durante l'ultimo controllo d'identità, quali l'uso del «tu» (40 % contro il 16 % del campione totale), gli insulti (21 % contro il 7 % del campione totale) o la brutalità (20 % rispetto all'8 % del campione totale). Queste esperienze negative e la frequenza dei controlli sono associate a una scarsa fiducia nella polizia. In effetti, questo gruppo ha segnalato il deterioramento dei rapporti con la polizia.

Infine, dai risultati emerge che tra gli intervistati che segnalano violazioni della deontologia durante i controlli d'identità, pochi (5 %) agiscono per denunciare tali violazioni. I risultati indicano essenzialmente che le persone non rendono pubbliche le loro esperienze perché le denunce sono considerate inutili.

Per ulteriori informazioni, cfr. Défenseur des droits (2017).

Se a un gruppo di minoranza vengono applicati profili generali e se a ciò si aggiungono altre azioni politiche stigmatizzanti, è possibile non soltanto che tale gruppo sviluppi una percezione negativa di se stesso, ma che anche la comunità più in generale sviluppi una percezione negativa di tale gruppo. Il gruppo di minoranza può diventare una «comunità sospetta» che la popolazione associa alla criminalità ([21]) e i pregiudizi possono di conseguenza aumentare.

Al gruppo di minoranza può essere dedicata una quantità sproporzionata di risorse di polizia, il che, a sua volta, può determinare un maggior numero di arresti o controlli alle frontiere. Si instaura quindi una spirale che si auto-alimenta, fatta di rigidi controlli di polizia e tassi di arresti più alti (cfr. riquadro) ([22]).

Sotto la lente: il rischio di una «profezia che si autoavvera»

Quando i funzionari di polizia basano la profilazione non su motivi ragionevoli ma su pregiudizi, è probabile che interpretino le informazioni in un modo che conferma i loro preconcetti. Si tratta del cosiddetto «*bias* di conferma». Ciò accade quando a causa dei propri pregiudizi i funzionari si aspettano che una persona agisca in modo illecito sulla base di caratteristiche effettive o presunte

([21]) Osservatorio europeo dei fenomeni di razzismo e xenofobia (2006), pag. 54.

([22]) Harcourt, B. (2004), pagg. 1329-1330; House of Commons Home Affairs Committee (2009), paragrafo 16; e Nazioni Unite (2007).

di tale persona quali la razza, l'origine etnica, il genere, l'orientamento sessuale, la religione o qualsiasi altro motivo protetto. A causa di questo tipo di *bias*, è probabile che i funzionari che nutrono tali pregiudizi concentrino la propria attenzione sugli individui che corrispondono a tale descrizione.

Poiché è più probabile che vengano trovate prove di comportamenti criminali tra le persone che vengono fermate che tra quelle non fermate, questa profilazione basata sul pregiudizio rinforza gli stereotipi esistenti degli operatori. Questa «prova» fallace del fatto che la decisione di fermare tali individui era corretta è nota come «profezia che si autoavvera». Una profilazione di questo tipo è discriminatoria, illecita, inefficace e perpetua gli stereotipi.

La figura 4 descrive in che modo la «profezia che si autoavvera» perpetua la criminalizzazione degli individui.

Figura 4: Il ciclo della profezia che si autoavvera

Fonte: *FRA (2018)*

1.3.2. L'efficacia della profilazione

Vi sono dubbi anche sull'efficacia della profilazione basata su categorie generali ai fini dell'accertamento di reati. Non è chiaro infatti se la profilazione aumenti effettivamente il tasso di successo (o «tasso di riscontro positivo») delle operazioni di contrasto.

Alcuni elementi indicano che i tassi di fermo degli individui non corrispondono necessariamente ai tassi di illeciti dei diversi gruppi etnici o razziali (cfr. riquadro). Va osservato che i dati della giustizia penale nella maggior parte degli Stati membri dell'UE non consentono di conoscere l'esito dei singoli casi nel sistema di giustizia penale. Pertanto, non è possibile stabilire se un arresto sfoci nell'azione penale e in una condanna.

Caso di studio

La modifica dei modelli di perquisizione porta a un «tasso di riscontro positivo» più elevato (1998-2000, USA)

Nel 1998, il 43 % delle perquisizioni effettuate dalle autorità doganali statunitensi riguardava neri e latino-americani, una cifra assai più alta rispetto alla proporzione in cui questo gruppo era rappresentato tra i viaggiatori in generale. Fu effettuato un numero particolarmente elevato di perquisizioni, utilizzando anche tecniche invasive come i raggi X e perquisizioni personali approfondite, su donne latino-americane e nere sospettate di essere corrieri della droga sulla base di un profilo basato in misura preponderante sulla nazionalità e sull'origine etnica. Il tasso di successo per queste perquisizioni fu basso per tutti i gruppi: 5,8 % per i bianchi, 5,9 % per i neri e 1,4 % per i latino-americani, e fu particolarmente basso per le donne latino-americane, che costituivano in effetti il gruppo in cui era meno probabile trovare persone che portassero droga con sé o all'interno del corpo. Nel 1999 il servizio doganale modificò le proprie procedure ed eliminò il fattore razziale dagli elementi da considerare per compiere fermi, introducendo invece tecniche di osservazione incentrate su comportamenti quali nervosismo e incoerenze nelle spiegazioni dei passeggeri, un uso maggiore delle informazioni di intelligence e una stretta vigilanza sulle decisioni di fermo e perquisizione. Nel 2000 le disparità razziali nelle perquisizioni doganali erano quasi scomparse. Il numero di perquisizioni effettuate è crollato del 75 % mentre il tasso di riscontro positivo è migliorato, passando da meno del 5 % a più del 13 %, ed è diventato quasi uguale per tutti i gruppi etnici.

Per ulteriori informazioni, cfr. Harris (2002), USA (2000).

Inefficacia della profilazione illecita (2007-2008, Ungheria)

Ricerche condotte in Ungheria hanno evidenziato che i rom sono sottoposti in misura sproporzionata a controlli d'identità. Circa il 22 % di tutte le persone controllate dalla polizia apparteneva alla comunità rom, mentre la percentuale di rom nella popolazione era intorno al 6 %. Al numero sproporzionato di controlli d'identità sui rom non ha fatto riscontro una percentuale altrettanto elevata di illeciti accertati: il 78 % dei controlli d'identità riguardanti i rom non ha dato adito a nessuna azione da parte della polizia e il 19 % % % è risultato legato a un reato minore (*) (rispetto al 18 % dei controlli sulla popolazione generale). Inoltre, i tassi di arresto per la comunità rom e la popolazione generale sono risultati simili.

Per ulteriori informazioni, cfr. Tóth, B.M. e Kádár, A. (2011).

(*) «I reati minori sono illeciti quasi penali, la cui gravità non raggiunge il livello penale (il che significa che tali illeciti non sono disciplinati dal codice penale). I reati minori vanno da illeciti punibili con una pena detentiva di 60 giorni, quali la prostituzione o le minacce fisiche, a illeciti punibili con misure meno severe (ad esempio un'ammenda, la confisca dei beni o il divieto di accedere a determinati eventi). Tra gli esempi si citano i piccoli furti o le infrazioni del codice della strada». *Cfr. Kádár, A., Körner, J., Moldova, Z. e Tóth, B. (2008), pag. 23.*

Interrogativi riguardano anche i motivi per cui alcune persone sono fermate. Secondo uno studio del Regno Unito «un allarmante 27 % (2 338) dei verbali di fermo e perquisizione esaminati [...] non conteneva motivi ragionevoli per una perquisizione personale, anche se molti di questi verbali erano stati approvati dai superiori» ([23]). Secondo la ricerca questo indica «la possibilità che le forze di polizia non rispettino pienamente l'obbligo di uguaglianza del settore pubblico, che impone loro di tenere debitamente conto della necessità di eliminare la discriminazione illecita e di promuovere le pari opportunità, favorire buone relazioni e, a tal fine, raccogliere, analizzare e pubblicare dati atti a dimostrare che hanno sufficienti informazioni per comprendere l'effetto del proprio lavoro».

([23]) Regno Unito, Her Majesty's Inspectorate of Constabulary (2013), pag. 6.

2 Profilazione lecita: principi e prassi

Questo capitolo è incentrato sulla profilazione effettuata dal personale di polizia con funzioni operative, in particolare le operazioni di fermo e perquisizione, e dagli addetti alla gestione delle frontiere, in particolare l'invio a ulteriori verifiche «in seconda linea». Illustra i principi e le prassi principali che possono contribuire a ridurre il rischio di profilazione illecita e che possono essere adottati sia a livello di direzione sia a livello operativo e tiene conto dei diversi contesti giuridici e pratici delle operazioni di fermo e perquisizione e delle verifiche di frontiera.

Nel contesto della gestione delle frontiere, il codice frontiere Schengen [regolamento (UE) 2016/399] ([24]) stabilisce norme unificate che disciplinano i controlli alle frontiere esterne dell'UE. Ciò significa che alcuni dei principi delineati nel presente capitolo, ad esempio per quanto riguarda le informazioni da fornire ai cittadini di paesi terzi oggetto di una verifica in seconda linea, sono stabiliti dalla legge e vincolanti per gli Stati membri. Frontex svolge inoltre un ruolo importante nel promuovere uno standard costantemente elevato nei controlli di frontiera. In particolare, il regolamento del 2016 sulla guardia di frontiera e costiera europea stabilisce che nella formazione delle guardie di frontiera gli Stati membri debbano seguire il programma comune di base elaborato da Frontex. Tale programma, pubblicato nel 2012, contiene una componente relativa ai diritti fondamentali che comprende anche la profilazione (cfr. sezione 2.2.3 sulla formazione mirata).

([24]) 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) (GU L 77 del 23 marzo 2016, pag. 1).

Sotto la lente: i motivi per una verifica in seconda linea alla frontiera

I controlli di frontiera sono sistematici e quindi ogni viaggiatore è sottoposto a una verifica di base in prima linea che consiste nel controllo dei documenti di viaggio e degli altri requisiti per l'ingresso. Inoltre, alcuni viaggiatori possono essere inviati a un'ulteriore verifica in seconda linea. Ciò può avvenire per diversi motivi: un riscontro positivo in una banca dati, un documento di viaggio sospetto, la corrispondenza a un profilo di rischio o un comportamento sospetto.

Durante la verifica in prima linea, la guardia di frontiera può avvalersi delle informazioni ottenute confrontando i dati contenuti nel documento di viaggio a lettura ottica (che comprende identificatori biometrici) con i dati conservati nelle banche dati nazionali, dell'UE e internazionali, quali il sistema d'informazione Schengen, il sistema d'informazione visti e le banche dati di Europol e Interpol. In pratica, l'invio a una verifica in seconda linea è spesso dovuto a un riscontro positivo in una delle banche dati.

Una persona può tuttavia essere inviata a una verifica in seconda linea anche per altri motivi, ad esempio quando corrisponde a un profilo di rischio o il funzionario ha altri sospetti sul suo conto. Il catalogo Schengen dell'UE indica che oltre all'effettuazione di verifiche di frontiera conformemente al codice frontiere Schengen, l'obiettivo delle verifiche in prima linea dovrebbe essere il *profiling* dei passeggeri e l'individuazione delle persone sospette da sottoporre a verifiche approfondite in seconda linea (*). Le guardie di frontiera devono pertanto valutare un insieme di altri indicatori e criteri per stabilire se è possibile che una persona stia cercando di entrare in modo irregolare, se possa rappresentare un rischio per la sicurezza o se, ad esempio, possa essere vittima della tratta di esseri umani. Indipendentemente dal fatto che applichino uno specifico profilo di rischio esistente, in queste situazioni le guardie di frontiera utilizzano la profilazione.

Dovendo garantire un'agevole circolazione dei viaggiatori, le guardie di frontiera hanno poco tempo per valutare in modo oggettivo se inviare una persona a una verifica in seconda linea. Le informazioni fornite da Frontex indicano che i funzionari degli Stati membri dell'UE dispongono in media di 12 secondi per decidere se effettuare ulteriori verifiche su una persona (**). Ciò significa che sono sottoposti a una forte pressione affinché prendano una decisione corretta in tempi brevi.

(*) Consiglio dell'Unione europea (2009), raccomandazione 43.
(**) Agenzia europea della guardia di frontiera e costiera (2015).

I principi e gli strumenti pratici del presente capitolo contengono informazioni volte a stimolare la discussione e l'azione affinché gli operatori e le loro organizzazioni possano mantenere le loro attività di profilazione entro i confini stabiliti dalla legge. I tre principi chiave discussi sono:

- rispettare la dignità delle persone;
- garantire che la profilazione si basi su motivi ragionevoli e oggettivi;
- garantire la rendicontabilità.

In relazione a ciascuno di tali principi è importante garantire che i funzionari di polizia e le guardie di frontiera operino entro i confini della legge quando ricorrono alla profilazione.

2.1. Rispetto della dignità della persona

Punti salienti

- Garantire un'**interazione di buona qualità** in sé non elimina la profilazione discriminatoria; è probabile tuttavia che assicuri migliori risultati e riduca le potenziali incidenze negative delle operazioni di fermo e perquisizione. Nella gestione delle frontiere, un comportamento professionale e rispettoso costituisce un obbligo giuridico.
- Un **comportamento professionale e rispettoso** in genere aumenta la soddisfazione relativa all'interazione.
- **Spiegando i motivi per cui una persona viene fermata** si contribuisce a rafforzare la fiducia nelle operazioni di polizia e gestione delle frontiere e a ridurre la sensazione che la profilazione sia discriminatoria.
- Il rispetto e la cortesia **non rendono in nessun caso giustificabili verifiche di frontiera o fermi e perquisizioni illeciti da parte della polizia**.

Oltre a essere un diritto fondamentale in sé, il rispetto della dignità delle persone è anche un principio fondamentale delle operazioni di polizia e di gestione delle frontiere. Nelle operazioni in prima linea, il modo in cui gli operatori di polizia e gestione delle frontiere parlano e interagiscono con le persone che fermano è cruciale, così come lo sono le informazioni che forniscono.

Va sempre ricordato che, indipendentemente dal livello di cortesia e di professionalità dei funzionari, essere chiamati da parte per verifiche più approfondite rappresenta comunque un'esperienza intrusiva che deve sempre avere motivazioni legittime. La percezione del carattere discriminatorio della profilazione è legata anche alla frequenza e al numero di interazioni con le autorità di polizia e gestione delle frontiere, il che sottolinea l'importanza di garantire che vi siano sempre motivi oggettivi e ragionevoli per fermare una persona.

Che cosa dicono le norme?

«Le verifiche di frontiera dovrebbero essere effettuate nel pieno rispetto della dignità umana. Il controllo di frontiera dovrebbe essere eseguito in modo professionale e rispettoso ed essere proporzionato agli obiettivi perseguiti».

Considerando 7 del codice frontiere Schengen

«Tutti i viaggiatori hanno il diritto ad essere informati sulla natura dei controlli e ad essere trattati in modo professionale, cordiale e cortese conformemente al diritto internazionale, dell'Unione e nazionale applicabile».

Sezione 1.2 del Manuale pratico per le guardie di frontiera (Manuale Schengen)

«Il personale di polizia deve agire con integrità e rispetto nei confronti dei cittadini e con particolare considerazione per la situazione degli individui appartenenti a gruppi particolarmente vulnerabili».

Raccomandazione 44 del codice europeo di etica per la polizia

Non è sempre facile garantire che i funzionari di polizia e le guardie di frontiera siano cortesi e forniscano informazioni in situazioni tese e difficili; tuttavia, è dimostrato che l'uso di un tono rispettoso aumenta notevolmente il livello di soddisfazione in merito all'interazione ([25]). La figura 5 illustra alcuni elementi di un'interazione improntata al rispetto.

Alcuni elementi delle verifiche di frontiera sono disciplinati dal codice frontiere Schengen, come l'obbligo di effettuare le verifiche in modo professionale e rispettoso o di fornire informazioni circa l'obiettivo perseguito e la procedura seguita per

([25]) FRA (2014b).

Figura 5: I tre elementi di un'interazione rispettosa

Fonte: *FRA (2018)*

la verifica (codice frontiere Schengen, considerando 7, articolo 7 e articolo 8, paragrafo 5). L'uso di una lingua comune non è invece un requisito assoluto nel contesto della gestione delle frontiere a causa della natura intrinsecamente varia del traffico frontaliero. Il codice frontiere Schengen prevede tuttavia che gli Stati membri incoraggino le guardie di frontiera ad apprendere le lingue necessarie per l'esercizio delle loro funzioni (articolo 16, paragrafo 1). Il catalogo Schengen, che contiene una serie di raccomandazioni e migliori prassi per il controllo delle frontiere esterne, raccomanda inoltre che le guardie di frontiera siano in grado di comunicare in lingue straniere legate ai loro compiti quotidiani. Come migliore pratica, il catalogo indica una conoscenza soddisfacente delle lingue dei paesi limitrofi, nonché di altre lingue in funzione della natura del traffico frontaliero. Se possibile, in ogni turno si dovrebbe prevedere la presenza di agenti con conoscenze linguistiche appropriate ([26]).

La mancanza di considerazione e di rispetto durante i fermi di polizia può avere effetti diretti sull'efficacia delle attività di polizia (cfr. sezione 1.3.2). Secondo il codice di condotta relativo alla legge sulla polizia e sulle prove penali del Regno Unito «tutti i fermi e le perquisizioni devono essere effettuati con cortesia, considerazione e rispetto per la persona interessata. Ciò ha un impatto significativo sulla fiducia della popolazione nella polizia. Deve essere compiuto ogni ragionevole sforzo per ridurre al minimo l'imbarazzo che una persona può provare durante una perquisizione» ([27]).

([26]) Consiglio dell'Unione europea (2009), raccomandazioni 27 e 41.

([27]) Regno Unito, Home Office (2014a), sezione 3.1.

Alcuni elementi importanti che concorrono al rispetto della dignità, come fornire informazioni sul fermo e garantire ai fermati la possibilità di esprimere il proprio punto di vista, sono componenti essenziali delle procedure di polizia e di gestione delle frontiere. I moduli per i verbali di fermo e perquisizione possono essere utili per fornire queste informazioni in modo strutturato (cfr. sezione 2.3.1).

Nel contesto della gestione delle frontiere, i moduli standard sono uno strumento utile per comunicare ai viaggiatori lo scopo e la procedura della verifica in seconda linea e possono agevolare la comunicazione con i viaggiatori, a condizione che siano accompagnati e integrati da ulteriori spiegazioni fornite a voce, se necessario. Il codice frontiere Schengen prevede che le persone sottoposte a una verifica in seconda linea siano informate per iscritto, in una lingua loro comprensibile o che si possa ragionevolmente supporre sia loro comprensibile, sull'obiettivo e sulla procedura seguita per effettuare tale verifica. Le informazioni dovrebbero:

- essere disponibili in tutte le lingue ufficiali dell'UE e nelle lingue dei paesi limitrofi al paese interessato;

- indicare che il viaggiatore può chiedere il nome o il numero di matricola del funzionario che effettua la verifica in seconda linea nonché il nome del valico di frontiera e la data dell'attraversamento della frontiera.

Gli elementi di un'interazione rispettosa associati alle capacità comunicative e interpersonali sono più difficili da definire nelle procedure operative e possono richiedere ulteriori investimenti nella formazione. Le difficoltà a dare un'impronta positiva alle interazioni possono derivare da:

- capacità di comunicazione limitate;

- incapacità di definire il motivo dell'azione;

- mancato superamento di preconcetti personali e istituzionali e stereotipi negativi, nonché ostilità che si sono radicate in parti della comunità.

2.2. Motivi ragionevoli e oggettivi

Punti salienti

- Quando le attività di contrasto e gestione delle frontiere sono basate su informazioni di intelligence specifiche e aggiornate, è più probabile che siano oggettive.
- Per essere leciti, i fermi e l'invio a verifiche in seconda linea devono essere fondati su **motivi ragionevoli e oggettivi che inducano a nutrire sospetti**. Le «sensazioni» e l'«istinto» non sono un motivo ragionevole od oggettivo per fermare e perquisire una persona o per inviarla a una verifica di frontiera in seconda linea.
- Caratteristiche protette quali la razza, l'origine etnica, il genere o la religione possono rientrare tra i fattori presi in considerazione dalle autorità di contrasto e dalle guardie di frontiera nell'esercizio delle loro competenze, ma **non possono essere l'unica o principale ragione per concentrare l'attenzione su un soggetto**.
- La profilazione basata esclusivamente o principalmente su uno o più motivi protetti costituisce una discriminazione diretta ed è illegale.

L'oggettività è un principio importante dell'attività di polizia e di gestione delle frontiere. Nel contesto della profilazione, il fermo e la perquisizione o l'invio a verifiche in seconda linea dovrebbero essere effettuati unicamente se sussistono motivi ragionevoli e oggettivi che inducono a sospettare di una persona. Sono considerate giustificazioni oggettive ad esempio il comportamento del soggetto, informazioni di intelligence specifiche o circostanze che mettono in relazione uno o più soggetti con una sospetta attività illecita.

Per garantire l'oggettività nella profilazione occorre:

- evitare distorsioni e preconcetti, anche mediante orientamenti chiari e una formazione mirata; e
- usare in modo efficace le informazioni di intelligence e di altro tipo.

2.2.1. Evitare distorsioni e preconcetti

Il codice europeo di etica per la polizia fornisce orientamenti sulla condotta di polizia in settori quali le azioni, gli interventi, la responsabilità e il controllo della polizia ([28]). Esso sottolinea il principio generale secondo cui: «La polizia deve compiere le proprie

([28]) Consiglio d'Europa, Comitato dei ministri (2001), Raccomandazione Rec(2001)10 del Comitato dei ministri agli Stati Membri sul tema del Codice europeo di etica per la polizia, 19 settembre 2001.

funzioni in modo equo, guidata, in particolare, dai principi di imparzialità e non discriminazione». ([29])

Concentrare l'attenzione su singole persone usando *come fattore unico o determinante* la razza, l'origine etnica, il genere, l'orientamento sessuale, la religione, la disabilità o altre caratteristiche, effettive o presunte, che costituiscono motivi vietati rappresenta una violazione dei diritti fondamentali e può anche avere conseguenze negative significative per le autorità pubbliche e le comunità (cfr. sezione 1.3).

La profilazione discriminatoria può riflettere distorsioni e preconcetti a livello sia personale che delle istituzioni. Oltre alle distorsioni e ai preconcetti personali, possono anche esistere stereotipi e comportamenti discriminatori derivanti da prassi specifiche delle autorità di contrasto e gestione delle frontiere. Rendendo più trasparenti le procedure e le prassi istituzionali si può contribuire a contrastare la discriminazione e la perpetuazione degli stereotipi.

Può essere difficile riconoscere distorsioni e preconcetti radicati. I funzionari di polizia e di gestione delle frontiere possono essere convinti che i motivi per i quali concentrano l'attenzione su determinate persone siano ragionevoli e oggettivi (ad esempio, il comportamento), quando invece le loro decisioni sono espressione dei loro preconcetti.

Quando fermano un soggetto, gli operatori spesso sostengono di aver agito sulla base di una «sensazione» (istinto) o del proprio «intuito», che probabilmente trovano il loro fondamento nelle competenze e nelle esperienze passate, ma che possono anche riflettere preconcetti consci o inconsci del funzionario. Al fine di evitare la profilazione illecita, i funzionari devono riflettere al fine di stabilire se la loro decisione è giustificata da informazioni oggettive. Le «sensazioni» o l'«istinto» non sono un motivo ragionevole od oggettivo per fermare o perquisire una persona o per sottoporla a verifiche più approfondite alla frontiera.

2.2.2. Orientamenti chiari per i funzionari

La disponibilità di orientamenti di taglio pratico, comprensibili e pronti per l'uso è particolarmente importante per aiutare i funzionari delle autorità di contrasto e di gestione delle frontiere a evitare la profilazione illecita. Gli orientamenti possono assumere diverse forme: possono essere acclusi alle norme legislative, emanati dalle stesse autorità di contrasto e di gestione delle frontiere o forniti quotidianamente dai

([29]) *Ibid.*, punto 40.

superiori. L'uso di esempi concreti per dimostrare cosa fare in particolari situazioni è probabilmente più efficace di una spiegazione delle norme e delle procedure.

I dirigenti devono informare il personale che caratteristiche effettive o presunte quali la razza, l'origine etnica, il genere, l'orientamento sessuale, la religione o altri motivi di discriminazione vietati non possono essere il fattore determinante per agire nei confronti di un soggetto. Chiarendo quando e come si possono usare le caratteristiche personali si può contribuire a ridurre il rischio di interpretazioni divergenti e l'affidamento su stereotipi e pregiudizi. Gli orientamenti dovrebbero riguardare anche le questioni relative alla tutela della vita privata e alla protezione dei dati.

La tabella 3 mostra alcuni tipi di orientamenti utilizzabili e caratteristiche importanti da prendere in considerazione.

Tabella 3: Tipi di orientamenti, caratteristiche e coinvolgimento delle parti interessate

Tipi di orientamenti	Caratteristiche degli orientamenti	Coinvolgimento delle parti interessate

• procedure operative standard
• codici di condotta
• indicazioni fornite regolarmente dai superiori
	• dettagliati e specifici
	• riguardanti tutte le attività in cui è possibile che la profilazione sia fondata su preconcetti:
	  • fermi e perquisizioni
	  • arresti
	  • verifiche di frontiera
	  • uso della forza ecc.
		• formulare orientamenti con altre parti interessate
		• mettere gli orientamenti a disposizione delle comunità
		• incoraggiare il feedback delle comunità sugli orientamenti

Fonte: FRA (2018)

Caso di studio

Codice deontologico e approccio degli ambasciatori (polizia olandese)

La polizia olandese ha elaborato un codice deontologico, redatto insieme ad organizzazioni della società civile come Amnesty International, che descrive i quattro principi alla base di un fermo improntato alla professionalità:

☑ selezione legittima e giustificabile delle persone fermate;

☑ spiegazione del motivo alla base del fermo e perquisizione;

- ☑ comunicazione professionale;
- ☑ riflessione da parte degli agenti sulle prassi utilizzate e feedback reciproco tra agenti.

È difficile modificare prassi che non sono considerate problematiche, ad esempio l'attività di polizia proattiva che può portare alla profilazione etnica. Ad Amsterdam la polizia ha elaborato un approccio dal basso che interessa gli operatori sul campo (ambasciatori) delle squadre, assistiti dai loro dirigenti e formatori. Il primo passo consiste nel sensibilizzare i funzionari mostrando e discutendo l'impatto dei fermi proattivi sulle persone che li subiscono e introducendo un quadro alternativo equo ed efficace. Il secondo passo consiste nel far sì che i funzionari adottino questa nuova prassi.

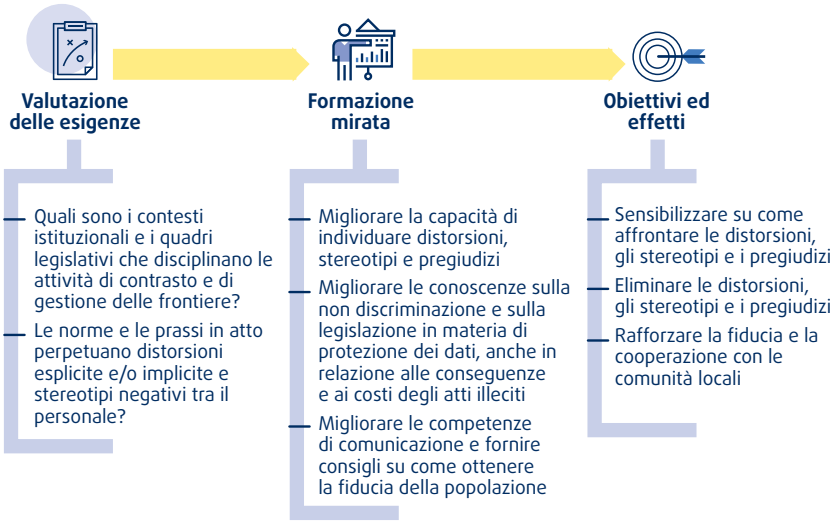
Ulteriori informazioni sono disponibili in neerlandese nel sito della polizia.

2.2.3. Formazione mirata

La formazione dei funzionari di polizia e delle guardie di frontiera è un altro strumento importante per ridurre al minimo il rischio di profilazione illecita. Esistono molti tipi diversi di formazione che possono essere erogati in fasi diverse del percorso professionale di un funzionario, ad esempio la formazione iniziale al reclutamento, la formazione in servizio e l'aggiornamento professionale continuo. Indipendentemente dal tipo, i moduli di formazione dovrebbero tenere conto della cultura organizzativa e offrire corsi che includano strategie intese a combattere e scalzare gli stereotipi. Infine, la valutazione dell'impatto della formazione è fondamentale per monitorare il modo in cui la formazione ha contribuito a modificare la percezione dei funzionari e a migliorarne le prassi, nonché per identificare carenze per le quali potrebbero essere necessarie ulteriori attività di formazione. La figura 6 pone in evidenza alcuni aspetti da considerare nello sviluppo di una formazione mirata.

Alcuni tipi di formazione per i funzionari delle autorità di contrasto o le guardie di frontiera, ad esempio la «formazione alla diversità» e la «formazione alla sensibilità», sono già ben sviluppati in alcuni paesi. La formazione alla diversità mira ad affrontare i sentimenti personali sull'origine etnica, le differenze e gli stereotipi e il modo in cui influenzano la nostra vita quotidiana. Non tutti i corsi sulla diversità, tuttavia, trattano il tema della discriminazione. In alcuni studi si afferma che in realtà la formazione culturale e alla diversità può dare maggior forza e rilievo alle differenze, irrobustendo gli

Figura 6: Il processo e gli obiettivi dello sviluppo di una formazione mirata



Fonte: *FRA (2018)*

stereotipi anziché ridurli ([30]).formazione alla sensibilità culturale» (rispetto alla «formazione alla diversità generale») mira a preparare i funzionari della polizia e delle autorità di contrasto in merito alla cultura degli specifici gruppi etnici con i quali spesso vengono a contatto ma con cui non hanno dimestichezza. Questo tipo di formazione fornisce indicazioni su cosa si debba o non si debba fare e sul modo in cui i vari gruppi etnici, religiosi o nazionali percepiscono la cortesia. La formazione alla sensibilità culturale si dimostra efficace soprattutto quando viene sviluppata ed erogata con l'aiuto e la partecipazione dei membri delle comunità interessate.

Caso di studio

Formazione sulla profilazione lecita

Formazione sulla profilazione per i funzionari di polizia (Italia)

Dal 2014, in Italia l'Osservatorio per la sicurezza contro gli atti discriminatori offre un modulo di formazione sulla profilazione etnica rivolto agli agenti e agli allievi delle forze di polizia. Tale modulo riguarda in particolare le

([30]) Wrench, J. (2007).

presunte distorsioni che possono influenzare la profilazione, le conseguenze in termini di efficienza delle attività di polizia e l'impatto negativo sui rapporti con le comunità. Finora circa 5 000 persone hanno partecipato alla formazione. Dal 2017 è previsto anche un modulo di formazione online nel quadro dei corsi di aggiornamento per la polizia.

Per ulteriori informazioni, consultare il sito della Polizia di Stato italiana.

Strumento per i diritti fondamentali nella formazione delle guardie di frontiera (UE)

Il programma comune di base (CCC) per la formazione delle guardie di frontiera europee definisce i livelli minimi di competenze e conoscenze che ogni guardia di frontiera europea deve possedere. Contiene capitoli dedicati alla sociologia e ai diritti fondamentali e sezioni specifiche sulla non discriminazione (1.5.4) e sulla profilazione etnica (1.7.10), che i formatori possono utilizzare. Il CCC evidenzia i rischi potenziali connessi a pregiudizi, razzismo, discriminazione razziale, xenofobia, islamofobia, omofobia e altre forme di intolleranza correlate che possono emergere quando si effettuano attività di profilazione. L'aggiornamento 2017 del CCC comprende sezioni dedicate alle nuove competenze, in particolare nel campo dei diritti fondamentali.

Frontex inoltre, in consultazione con università e organizzazioni internazionali, ha sviluppato un manuale per i formatori (cfr. Frontex, 2013), che fornisce metodologie per migliorare le conoscenze e le competenze delle guardie di frontiera nel campo dei diritti fondamentali e della protezione internazionale. Il manuale menziona esplicitamente la profilazione e stabilisce norme fondamentali intese ad evitare la discriminazione. La formazione è impartita con regolarità. Tuttavia non è previsto un meccanismo permanente per valutare il conseguimento degli obiettivi della formazione.

Per ulteriori informazioni, cfr. Frontex (2012).

Giornate di studio della profilazione per il personale di grado elevato (Belgio)

Nel 2015 il Centro per le attività di polizia e la sicurezza (CPS), che ha sede a Gand (Belgio), ha organizzato con l'organismo belga per la parità (UNIA) una giornata di studio sulla profilazione etnica (*Profilage ethnique: l'égalité sous pression?*). Nel corso della giornata sono stati trattati diversi aspetti, ad esempio:

gli operatori di polizia di origine migratoria possono migliorare i rapporti con le minoranze etniche, e in caso affermativo, come? Con che frequenza viene usata la profilazione etnica dai funzionari di polizia? Come è stata valutata?

Nel 2016, l'UNIA ha organizzato due giornate di studio per il personale di polizia di grado elevato dei quartieri settentrionali di Bruxelles al fine di sensibilizzarlo sul tema della profilazione etnica e promuovere la riflessione sull'identificazione delle prassi di profilazione da parte degli agenti in prima linea. Funzionari di polizia spagnoli e britannici hanno presentato esempi di buone prassi a una platea composta da funzionari delle autorità di contrasto, ricercatori e organizzazioni non governative. In particolare, hanno dimostrato che riducendo la profilazione basata sull'origine etnica si è ottenuto un aumento del tasso di successo degli arresti di persone ricercate. Hanno sottolineato che questo risultato è stato reso possibile verbalizzando correttamente tutti i fermi e garantendo trasparenza sui relativi motivi. La formazione mirava a creare una comprensione comune delle prassi di profilazione etnica nell'intento di sostenere lo sviluppo futuro della ricerca sulle prassi attualmente in uso nelle forze di polizia in questo ambito.

Per ulteriori informazioni, cfr. Belgio (2015 e 2017).

La formazione dovrebbe trattare i preconcetti e gli stereotipi che possono albergare nelle stesse istituzioni che si occupano di attività di contrasto e gestione delle frontiere. Prima di impartire la formazione sulla prevenzione della profilazione illecita, è bene esaminare il contesto istituzionale più ampio e le politiche interne esistenti, ad esempio i meccanismi di reclamo posti in essere, l'eventuale presenza di un «codice del silenzio» tra i colleghi ecc. I programmi dovrebbero trattare i preconcetti e gli stereotipi presenti nelle attività di polizia, ad esempio in fermi e perquisizioni, arresti, trattenimenti e uso della forza.

Gli alti e medi funzionari hanno un ruolo fondamentale ai fini della riuscita della formazione, sia in qualità di partecipanti sia per l'importanza che attribuiscono alla formazione ([31]). In quanto destinatari della formazione, i funzionari di alto livello possono apprendere nuove prassi e competenze trasferibili agli agenti in prima linea. La cultura organizzativa, definita in larga misura dall'alta dirigenza, ha un impatto sostanziale sul comportamento quotidiano dei funzionari di polizia e delle guardie di frontiera, incluso il modo in cui interagiscono con la popolazione.

([31]) Cfr. Commissione europea (2017b).

Gli alti funzionari possono anche fare in modo che la formazione sia vista in modo positivo. Il comportamento del personale con funzioni dirigenziali, ad esempio il modo in cui comunica ai funzionari le finalità della formazione, o il fatto che i funzionari pensino di essere stati scelti a caso oppure perché sono «problematici» possono influire sul livello di interesse e di impegno nella formazione. Incoraggiando i funzionari a partecipare attivamente ai programmi di formazione e ad essere aperti alla possibilità di cambiare i propri comportamenti per migliorare il lavoro quotidiano con buona probabilità si migliora l'incidenza della formazione ([32]).

Una volta completata, la formazione dovrebbe essere riesaminata e valutata per verificarne l'incidenza sulla sensibilizzazione e sulla modifica dei comportamenti.

Sotto la lente: i principi guida della formazione

La formazione specializzata è essenziale per garantire un uso lecito della profilazione. La Commissione europea ha elaborato una serie di principi guida per garantire una formazione efficace e di qualità per quanto riguarda i crimini d'odio. Gli stessi principi si applicano alla formazione sulla profilazione lecita.

Formazione sui crimini d'odio per le autorità di contrasto e di giustizia penale: dieci principi guida

Garantire l'incidenza e la sostenibilità:

- ☑ inserire la formazione in un approccio più ampio alla lotta contro la discriminazione;
- ☑ elaborare una metodologia per rispondere alle esigenze di formazione.

Individuare gli obiettivi e creare sinergie:

- ☑ personalizzare i programmi sulla base del personale dell'organizzazione;
- ☑ cooperare con la società civile in modo strutturato.

([32]) Miller, J. e Alexandrou, B. (2016).

Scegliere la metodologia corretta:

☑ combinare diverse metodologie;

☑ formare i formatori.

Trasmettere contenuti di qualità:

☑ elaborare un programma di formazione di qualità;

☑ elaborare moduli di formazione in materia di discriminazione.

Monitorare e valutare i risultati:

☑ collegare la formazione alle procedure di riesame delle prestazioni;

☑ garantire il monitoraggio e la valutazione periodici dei metodi di formazione.

Per ulteriori informazioni, cfr. Commissione europea (2017a).

La formazione da sola non è tuttavia efficace per contrastare i preconcetti impliciti dei funzionari: per farlo, serve un cambiamento della mentalità istituzionale. Le autorità devono quindi prendere in considerazione interventi che si sviluppano su varie dimensioni per contrastare i preconcetti personali e istituzionali (cfr. caso di studio).

Caso di studio

Contrastare il «razzismo istituzionale» nella polizia

In risposta alle preoccupazioni sul ruolo della razza nella gestione inadeguata delle indagini di polizia sull'omicidio razzista di Stephen Lawrence nel Regno Unito, il governo britannico avviò un'indagine di ampia portata per individuare gli «insegnamenti da trarre per le indagini e l'azione penale nei confronti dei reati a sfondo razziale».

Secondo la relazione dell'indagine, pubblicata nel 1999, il «razzismo istituzionale» nella polizia metropolitana, che si manifesta tra l'altro con differenze nel numero di fermi e perquisizioni effettuati, costituisce motivo di grande preoccupazione per le comunità interessate. Le raccomandazioni dell'indagine, che spaziano dalla formazione di sensibilizzazione al razzismo

alla verbalizzazione e registrazione degli incidenti, sono state accompagnate da un invito generale a rafforzare l'apertura, la rendicontabilità e il recupero della fiducia da parte del servizio di polizia.

I riesami pubblicati nel 2009, dieci anni dopo l'indagine, hanno evidenziato miglioramenti nel modo in cui la polizia interagisce con le comunità delle minoranze etniche e indaga sui reati a sfondo razziale. Emerge tuttavia che la popolazione di colore continua ad avere molte più probabilità di essere fermata e perquisita rispetto ai bianchi.

Per ulteriori informazioni, cfr. Regno Unito, Home Office (1999), Regno Unito, Equality and Human Rights Commission (2009), Regno Unito, House of Commons Home Affairs Committee (2009).

2.2.4. Motivi ragionevoli di sospetto: far uso di informazioni di intelligence e di altro tipo

Quando i funzionari di polizia e di gestione delle frontiere concentrano la propria attenzione su un soggetto, in genere basano la propria decisione su una combinazione di elementi, tra cui informazioni tendenzialmente «oggettive», quali specifiche informazioni di intelligence, comportamenti, indumenti o effetti che il soggetto porta con sé, nonché conoscenze «soggettive» basate sull'esperienza.

Tutti questi elementi possono rappresentare un «segnale» di attività illecita. Le informazioni devono tuttavia essere combinate e utilizzate con cautela. I dati dimostrano che per i funzionari può essere difficile distinguere, nella pratica, elementi oggettivi e soggettivi, come nell'esempio citato nel riquadro.

Esempio

«È molto soggettivo. Ci sono le sensazioni personali su una persona e un caso, ma ci sono anche elementi che indicano incongruenze in ciò che dichiara il soggetto, discrepanze tra ciò che dichiara il soggetto e ciò che dichiara il garante, contraddizioni tra ciò che dichiara il soggetto e i documenti, tra ciò che dichiara il soggetto e quello che ha nel bagaglio. Quindi, ci sono elementi di prova ma [nessuna di

queste cose da sola] depone completamente a sfavore del soggetto. È il quadro completo che il funzionario deve costruire su una persona». (Funzionario del servizio immigrazione presso uno dei principali aeroporti del Regno Unito)

Per ulteriori informazioni, cfr. FRA (2014a), pag. 46.

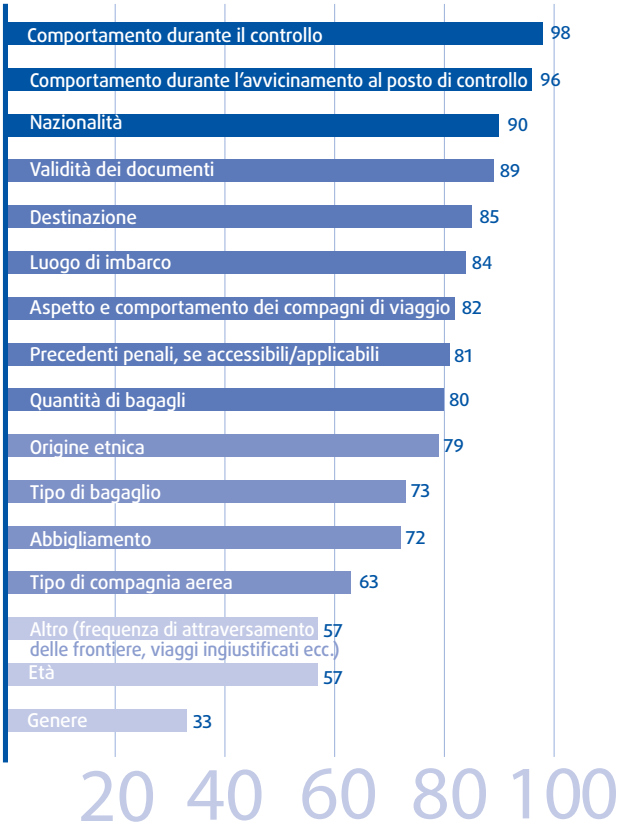
Sotto la lente: identificazione delle persone che cercano di entrare in modo irregolare in un paese

Le ricerche condotte dalla FRA nel 2012 presso i principali aeroporti indicano che le guardie di frontiera prendono in considerazione una serie di fattori al momento di decidere se un soggetto stia cercando di entrare nel paese in modo irregolare. Tali fattori spesso comprendono un insieme di criteri «oggettivi», quali il comportamento del soggetto durante l'avvicinamento al posto di controllo e in fase di controllo, il tipo e la quantità di bagagli e la validità dei documenti di viaggio, nonché l'esperienza personale in controlli di frontiera precedenti, come illustra la figura 7.

Le guardie di frontiera hanno indicato nel comportamento durante il controllo o l'avvicinamento al posto di controllo il fattore più utile per riconoscere chi sta cercando di entrare nel paese in modo irregolare. Sono stati tuttavia considerati significativi anche fattori quali la nazionalità e l'origine etnica, che possono essere indizi di profilazione discriminatoria.

Anche l'abbigliamento, che è stato considerato un indicatore utile, è un esempio di come informazioni apparentemente «oggettive» possano essere utilizzate in modo non imparziale. Alcuni tipi di abbigliamento possono essere ricollegabili a profili di rischio specifici. Ad esempio, le vittime della tratta di esseri umani di una determinata nazionalità possono indossare di norma determinati indumenti; l'abbigliamento può tuttavia indicare anche l'appartenenza a uno specifico gruppo etnico o religioso. Anche se esistono altri motivi sufficienti per giustificare l'invio a una verifica in seconda linea, le persone che si identificano fortemente con la propria origine etnica o la propria religione, che hanno avuto in precedenza esperienze negative o che non ricevono spiegazioni adeguate dal funzionario possono percepire il trattamento cui sono sottoposte come discriminatorio.

Figura 7: Indicatori ritenuti utili o molto utili per riconoscere efficacemente le persone che stanno cercando di entrare in modo irregolare nel paese prima che i funzionari rivolgano loro la parola (%)



Nota: *le risposte valide sono state tra 206 e 216 su 223. Gli intervistati che non hanno risposto a una determinata domanda sono stati esclusi dal calcolo dei risultati. Le non risposte variano da 7 a 17 a seconda della domanda.*

Fonte: *FRA, indagine sulle guardie di frontiera, 2012 (domanda 17)*

Per ulteriori informazioni, cfr. FRA (2014a). In relazione ai profili delle vittime di tratta, cfr. Frontex (2017).

Buone informazioni di intelligence sui modelli di comportamento o sugli avvenimenti possono accrescere l'oggettività della profilazione in relazione ad attività criminali o, nel caso della gestione delle frontiere, alla migrazione irregolare o alla criminalità transfrontaliera. Quando le attività di contrasto e di gestione delle frontiere si basano

su informazioni di intelligence specifiche e tempestive, ad esempio informazioni su una determinata persona e/o sul contesto, è più probabile che siano oggettive e meno probabile che siano basate su stereotipi.

Oltre alle informazioni di intelligence e agli elementi oggettivi, anche le informazioni su caratteristiche protette effettive o presunte quali la razza, l'origine etnica, la nazionalità, il genere o la religione possono essere utilizzate legittimamente come componente aggiuntiva nelle valutazioni di profilazione in determinate circostanze. Per essere legittimo, l'uso di tali informazioni deve essere disciplinato dalla legge, rispettare l'essenza dei diritti e delle libertà interessati, essere proporzionato (ossia rispettare un equilibrio di interessi) e necessario (vale a dire che non dovrebbero essere disponibili altri mezzi meno restrittivi). Vi deve essere un motivo giustificabile, diverso dai motivi protetti, che giustifichi il diverso trattamento di una persona rispetto ad altre da parte dei funzionari. Tale motivo inoltre deve riguardare in modo specifico la persona in questione, come nell'esempio riportato nel riquadro.

Esempio

Testimoni riferiscono che il sospetto rapinatore indossava scarpe da corsa rosse e un cappellino da baseball nero, è alto tra 1,60 e 1,70 metri e dall'aspetto sembra di origine cinese. In questa situazione, le autorità di contrasto possono legittimamente considerare l'origine etnica come pertinente per determinare se una persona diventi un potenziale sospetto, in quanto l'origine etnica è accompagnata da informazioni specifiche.

Sotto la lente: descrizioni dettagliate del sospetto

Descrizioni accurate del sospetto possono ridurre il rischio di profilazione illecita. Una descrizione del sospetto consiste in informazioni sulla persona, ad esempio il colore della pelle, dei capelli e degli occhi, la statura e il peso e gli indumenti. Tali informazioni sono fornite dalla vittima o da testimoni, o ricavate sulla base di altre informazioni di intelligence specifiche. Una descrizione accurata del sospetto può essere utilizzata dagli operatori come base per le operazioni di fermo e perquisizione effettuate per trattenere i sospetti o inviarli a verifiche di frontiera in seconda linea.

Tuttavia, quando i funzionari delle autorità di contrasto ricevono una descrizione eccessivamente generale in cui figurano la razza, l'appartenenza etnica o caratteristiche simili, non dovrebbero utilizzarla come base per le

operazioni. In casi di questo genere, infatti, è probabile che le operazioni portino al fermo di molte persone innocenti che presentano le stesse caratteristiche. Dovrebbero invece cercare ulteriori informazioni operative specifiche per orientare le indagini.

Per ulteriori informazioni, cfr. Commissione europea (2017b).

Informazioni che sembrano oggettive possono in realtà essere viziate da distorsioni. Fattori apparentemente oggettivi quali l'ora, il giorno, il luogo ecc. possono essere utilizzati per surrogare motivi discriminazione vietati, ad esempio caratteristiche effettive o presunte quali la razza, il paese di origine, il genere, l'orientamento sessuale o la religione, come dimostra l'esempio che segue.

Esempio

Un'operazione di fermo e perquisizione viene condotta di venerdì intorno a mezzogiorno nell'area X. Tale orario coincide con il momento di preghiera più importante per i musulmani. Poiché l'area X si trova in prossimità di una moschea, i fattori apparentemente oggettivi rappresentati dal giorno della settimana, dall'ora e dal luogo possono essere utilizzati in realtà come surrogati per effettuare fermi e perquisizioni sulla base della religione, che è un motivo di discriminazione vietato.

Allo stesso modo, l'attenzione prestata a determinati comportamenti sospetti può sembrare un modo oggettivo per identificare eventuali illeciti. I funzionari possono tuttavia interpretare il comportamento di una persona in modi diversi sulla base di altre caratteristiche della persona stessa. È dimostrato che la conoscenza operativa e la comprensione delle informazioni di intelligence possono variare notevolmente da funzionario a funzionario e spesso non corrispondono a modelli di criminalità effettivi ([33]).

Fornendo ai funzionari informazioni di intelligence tempestive e dettagliate, ad esempio in una riunione informativa prima dell'inizio del turno di lavoro, si dovrebbe riuscire a ridurre la discrezionalità e fornire loro indicazioni su come esercitare i propri poteri in modo mirato per affrontare in modo più specifico le tendenze criminali in

([33]) National Policing Improvement Agency (NPIA) del Regno Unito (2012).

atto e i problemi di sicurezza identificati. Ciò riduce il peso dei preconcetti. Il miglioramento della qualità e dell'uso delle informazioni di intelligence per concentrarsi su fattori comportamentali o informazioni specifiche ha la massima efficacia quando è accompagnato da un'intensificazione della supervisione e dei controlli sui modi in cui i funzionari esercitano i propri poteri.

Caso di studio

Garantire l'oggettività nella profilazione

Briefing pre-turno (UE)

Il catalogo Schengen raccomanda che prima dell'inizio di ciascun turno l'agente in servizio fornisca informazioni su qualsiasi indicatore di rischio e profili di rischio. Prevedendo sovrapposizioni tra i turni si può garantire che ci sia sufficiente tempo per il passaggio di consegne e lo scambio di informazioni tra il personale del turno entrante e quello del turno uscente.

Per ulteriori informazioni, cfr. Consiglio dell'Unione europea (2009).

Programma di formazione SDR (Paesi Bassi)

Il programma di formazione sulla perquisizione, accertamento e reazione (Search, Detect and React, SDR) mira a prevenire reati o atti terroristici prima che vengano commessi migliorando la capacità di profilazione comportamentale del personale delle forze di sicurezza. A tal fine, il programma induce a distogliere l'attenzione da caratteristiche inalterabili come il colore della pelle per concentrarla invece sui comportamenti individuali quando si effettuano scelte relative all'azione di polizia. Poiché gli indicatori di comportamento sospetto sono specificamente legati al contesto, la formazione è modulata in funzione dell'ambiente e respinge l'idea che esista un'unica soluzione utilizzabile in ogni situazione. I funzionari che hanno individuato modelli di comportamento aventi rilevanza sono invitati ad agire in modo «sensibile», il che significa, nella maggior parte dei casi, avere una conversazione informale con il sospetto piuttosto che avvalersi dei poteri formali di polizia. Il programma prevede l'insegnamento in classe oltre alla formazione applicata e sul posto di lavoro.

Per ulteriori informazioni, cfr. il sito della SDR Academy.

Lo strumento per la prassi professionale autorizzata (APP) in materia di fermi e perquisizioni (Regno Unito)

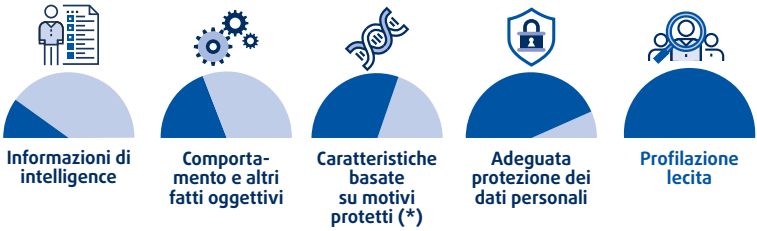
Il College of Policing del Regno Unito ha elaborato una guida alla prassi professionale autorizzata (Authorised Professional Practice, APP) che tratta vari aspetti dell'attività di polizia. L'APP in materia di fermi e perquisizioni spiega che cosa sono i fermi e le perquisizioni, perché è importante utilizzarli correttamente e quali sono le caratteristiche che devono avere le operazioni di fermo e perquisizione per essere lecite. Spiega che la liceità e l'efficacia delle operazioni di fermo e perquisizione presuppongono:

- **equità:** la decisione del funzionario di fermare e perquisire una persona deve basarsi esclusivamente su fattori appropriati e oggettivi. Una persona non deve mai essere fermata esclusivamente o principalmente sulla base di caratteristiche protette o di fattori quali condanne precedenti;
- **legalità:** i fermi e le perquisizioni devono avere una base giuridica applicata nel rispetto della legge;
- **professionalità:** durante l'operazione di fermo e/o perquisizione i funzionari devono rispettare norme di condotta professionali, in particolare il codice deontologico, comunicare con le persone in modo efficace e trattarle con dignità e rispetto;
- **trasparenza:** ogni singola operazione deve essere verbalizzata in modo accurato. Devono essere garantiti un monitoraggio e una supervisione efficaci dei fermi e delle perquisizioni, nonché il controllo pubblico.

Per ulteriori informazioni, cfr. Regno Unito, College of Policing (2016).

La figura 8 illustra i diversi elementi che possono essere utilizzati nella profilazione lecita; la specifica combinazione di elementi da impiegare dipende dalle caratteristiche del caso specifico.

Figura 8: Combinazione di elementi

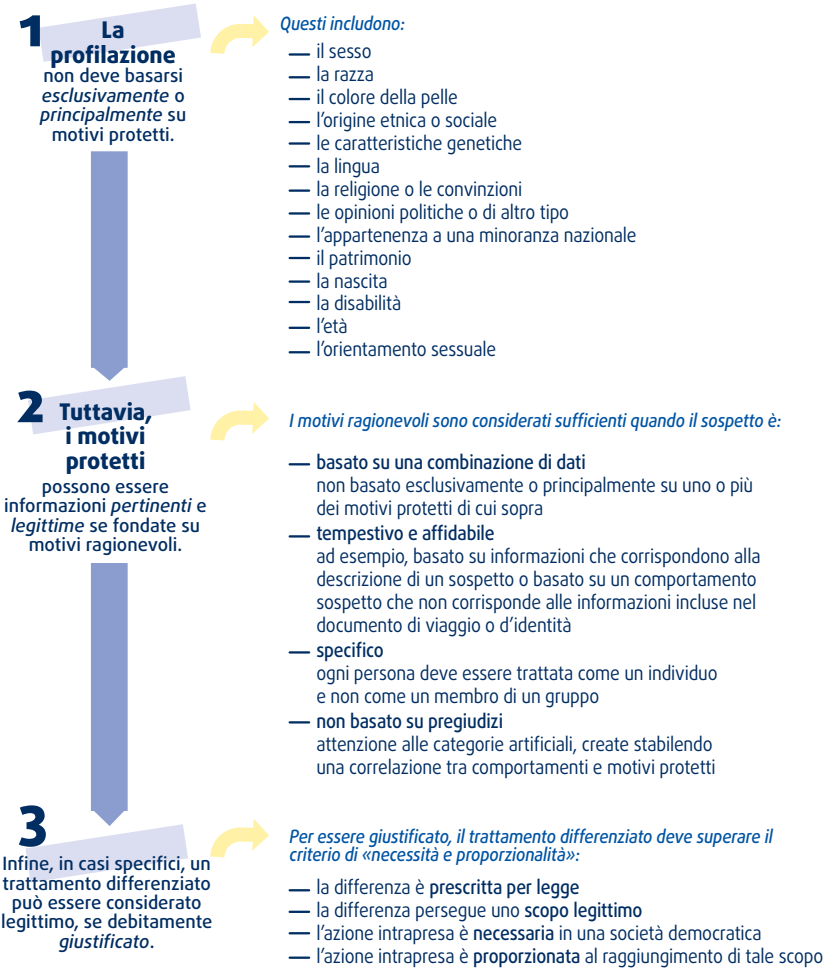


(*) *Per l'elenco dei motivi protetti ai sensi del diritto dell'UE, cfr. figura 9. La profilazione non dovrebbe mai essere basata unicamente o principalmente su caratteristiche protette.*

Fonte: *FRA (2018)*

La figura 9 mostra come si possono combinare questi elementi per garantire che la profilazione non sia discriminatoria.

Figura 9: Elementi della profilazione non discriminatoria



Nota: *l'elenco dei motivi protetti varia da uno Stato membro all'altro. Per una panoramica dei motivi di discriminazione previsti nei codici penali dei singoli Stati membri, cfr. FRA (2018d). Cfr. anche il sito di Equinet, la rete europea degli organismi per la parità, che elenca i motivi di discriminazione contemplati dagli organismi nazionali per la parità*

Fonte: *FRA (2018)*

2.2.5. Moduli per i verbali di fermo e perquisizione per la profilazione nelle attività di contrasto

I moduli per i verbali di fermo e perquisizione possono aiutare i funzionari a riflettere per stabilire se i fermi che effettuano sono fondati su motivi ragionevoli; inoltre, permettono ai superiori di monitorare potenziali prassi discriminatorie nel ricorso a fermi e perquisizioni da parte di singoli funzionari. Pur essendo talvolta considerati un adempimento gravoso, forniscono anche registrazioni dei fermi che, opportunamente aggregate, permettono di ricavare indicazioni utili per stabilire se i fermi sono effettuati in modo lecito ([34]), contribuendo così a promuovere l'apertura e la rendicontabilità. Per registrare le informazioni è possibile usare, oltre ai moduli cartacei da compilare, anche nuove tecnologie come le app mobili.

Alcuni elementi importanti da inserire nella struttura dei moduli per i verbali di fermo e perquisizione sono descritti nel riquadro che segue.

Sotto la lente: gli elementi di un verbale di fermo e perquisizione ben strutturato

I moduli per i verbali di fermo e perquisizione devono essere ben strutturati per risultare utili. In primo luogo, la compilazione del modulo comporta un carico di lavoro supplementare per i funzionari: se non è strutturato in modo chiaro e non è ragionevolmente conciso, c'è il rischio che i funzionari non lo compilino per intero o lo compilino in modo sommario. In secondo luogo, un modulo ben strutturato consente di estrarre e aggregare facilmente i dati per monitorare e valutare le operazioni di fermo e perquisizione.

Per quanto possibile, il modulo per i verbali di fermo e perquisizione dovrebbe:

- utilizzare campi a scelta multipla, che sono più veloci da compilare e più facili da trattare in termini statistici;
- presentare un elenco esaustivo di opzioni per ciascuna voce;
- evitare voci ambigue;
- essere facilmente comprensibile sia per il funzionario che per la persona fermata;

([34]) Regno Unito, Stop Watch (2011).

- comprendere:
  - le basi giuridiche per la perquisizione. Semplici spiegazioni sono preferibili a un elenco di norme;
  - la data, l'ora e il luogo in cui è avvenuta la perquisizione della persona o del veicolo;
  - l'obiettivo della perquisizione, ad esempio l'oggetto o gli oggetti che i funzionari stanno cercando;
  - l'esito del fermo;
  - il nome e la stazione di polizia dell'agente o degli agenti che effettuano la perquisizione;
  - i dati personali della persona o delle persone perquisite, quali il nome, l'indirizzo, la nazionalità, possono essere verbalizzati; tuttavia, i soggetti possono rifiutarsi di fornire tali informazioni.

Per essere efficaci, i moduli per i verbali dovrebbero essere compilati al momento del fermo.

Una loro copia dovrebbe essere consegnata alla persona fermata o alla persona cui è affidato il veicolo perquisito. Nel Regno Unito, le persone fermate hanno il diritto di chiedere una copia del verbale entro tre mesi dal fermo. In questo modo, il verbale documenta il fermo non soltanto per la polizia, ma anche per le persone fermate.

Per ulteriori informazioni, cfr. Regno Unito, West Midlands Police (2012), pag. 7, e Regno Unito, Home Office (2014a).

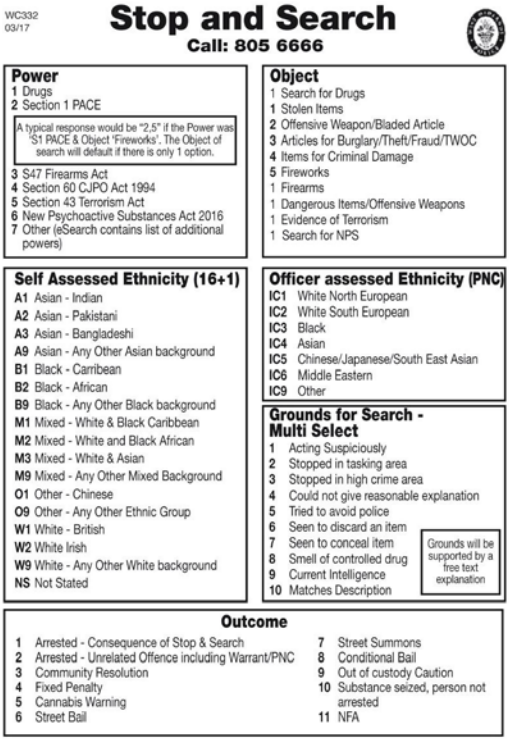
Caso di studio

Modulo per i verbali di fermo e perquisizione (Regno Unito)

Il modulo per i verbali di fermo e perquisizione utilizzato dalla West Midlands Police nel Regno Unito è riprodotto di seguito.

Alla persona fermata viene chiesto di auto-identificarsi come appartenente a una delle origini etniche dell'elenco, in cui figurano le opzioni «altra» e «non dichiarata». L'agente che effettua il fermo può aggiungere le proprie impressioni se non concorda con l'auto-identificazione.

Il codice deontologico per l'esercizio dei poteri di fermo e perquisizione nel Regno Unito indica che gli agenti dovrebbero spiegare alle persone fermate che le informazioni sull'origine etnica «sono necessarie per ottenere un quadro esatto delle attività di fermo e perquisizione e per contribuire a migliorare il monitoraggio etnico, a contrastare le prassi discriminatorie e a promuovere un uso efficace dei poteri».



WC332
03/17

Stop and Search
Call: 805 6666

Power
1 Drugs
2 Section 1 PACE

A typical response would be "2,5" if the Power was 'S1 PACE & Object 'Fireworks'. The Object of search will default if there is only 1 option.

3 S47 Firearms Act
4 Section 60 CJPO Act 1994
5 Section 43 Terrorism Act
6 New Psychoactive Substances Act 2016
7 Other (eSearch contains list of additional powers)

Object
1 Search for Drugs
1 Stolen Items
2 Offensive Weapon/Bladed Article
3 Articles for Burglary/Theft/Fraud/TWOC
4 Items for Criminal Damage
5 Fireworks
1 Firearms
1 Dangerous Items/Offensive Weapons
1 Evidence of Terrorism
1 Search for NPS

Self Assessed Ethnicity (16+1)
A1 Asian - Indian
A2 Asian - Pakistani
A3 Asian - Bangladeshi
A9 Asian - Any Other Asian background
B1 Black - Carribean
B2 Black - African
B9 Black - Any Other Black background
M1 Mixed - White & Black Caribbean
M2 Mixed - White and Black African
M3 Mixed - White & Asian
M9 Mixed - Any Other Mixed Background
O1 Other - Chinese
O9 Other - Any Other Ethnic Group
W1 White - British
W2 White Irish
W9 White - Any Other White background
NS Not Stated

Officer assessed Ethnicity (PNC)
IC1 White North European
IC2 White South European
IC3 Black
IC4 Asian
IC5 Chinese/Japanese/South East Asian
IC6 Middle Eastern
IC9 Other

Grounds for Search - Multi Select
1 Acting Suspiciously
2 Stopped in tasking area
3 Stopped in high crime area
4 Could not give reasonable explanation
5 Tried to avoid police
6 Seen to discard an item
7 Seen to conceal item
8 Smell of controlled drug
9 Current Intelligence
10 Matches Description

Grounds will be supported by a free text explanation

Outcome
1 Arrested - Consequence of Stop & Search
2 Arrested - Unrelated Offence including Warrant/PNC
3 Community Resolution
4 Fixed Penalty
5 Cannabis Warning
6 Street Bail
7 Street Summons
8 Conditional Bail
9 Out of custody Caution
10 Substance seized, person not arrested
11 NFA

Per ulteriori informazioni, cfr. Regno Unito, West Midlands Police (2017a), e Regno Unito, Home Office (2014a), pag. 19.

Molte forze dell'ordine stanno abbandonando l'uso di moduli per i verbali per la raccolta dei dati su fermi e perquisizione e stanno orientandosi verso tecnologie quali applicazioni per cellulari, sistemi via radio, terminali data mobili o computer portatili. Queste tecnologie possono rendere più rapido il processo di verbalizzazione e ridurre

la burocrazia, ma creano anche nuovi rischi, in particolare in relazione all'utilizzo algoritmico dei dati personali (cfr. capitolo 3).

Caso di studio

Verbalizzazione in diretta delle operazioni di fermo e perquisizione

«eSearch» (West Midlands Police, Regno Unito)

Questo sistema, adottato nell'aprile 2014, è basato su una chiamata tra il funzionario sul posto e un operatore del centro di contatto (sala di controllo). I dettagli dell'operazione di fermo e perquisizione sono immediatamente registrati nel centro di contatto e inseriti in una banca dati. Queste informazioni possono quindi essere consultate e utilizzate per controllare l'efficacia delle operazioni di fermo e perquisizione, sia internamente che esternamente. Il sistema eSearch ha trasformato la verbalizzazione delle operazioni di fermo e perquisizione. I registri possono essere visualizzati molto più rapidamente nei sistemi di polizia, con benefici per l'intelligence e l'integrazione nelle attività operative di polizia.

Per ulteriori informazioni, cfr. Regno Unito, West Midlands Police (2014 e 2016).

App mobile per gli agenti in prima linea (West Midlands Police, Regno Unito)

Una nuova app mobile, lanciata a ottobre 2017, mira a rendere più rapide ed efficienti le operazioni di fermo e perquisizione. L'app eSearch permette agli agenti di verbalizzare le informazioni sulle operazioni inserendole direttamente nell'app tramite smartphone, senza dover chiamare il centro di contatto. Ad ogni fermo viene attribuito un numero di riferimento univoco e il GPS ne registra automaticamente la posizione. L'app dovrebbe ridurre le chiamate al centro di contatto di quasi 1 000 chiamate al mese.

Per ulteriori informazioni, cfr. Regno Unito, West Midlands Police (2017b).

Il personale di grado gerarchico elevato svolge un ruolo importante nel garantire che le operazioni di fermo e perquisizione siano effettuate entro i limiti stabiliti dalla legge. L'esempio che segue illustra in che modo può mantenere la vigilanza garantendo anche che le operazioni di fermo e perquisizione non siano usate come misura delle prestazioni basata sul numero di fermi effettuati.

Caso di studio

Nullaosta ai verbali di fermo e perquisizione (Regno Unito)

Da agosto 2014, ogni verbale di fermo e perquisizione nel Regno Unito deve ricevere il nullaosta dal superiore del funzionario che ha effettuato la perquisizione e deve essere classificato come conforme o non conforme alle norme pertinenti. In quest'ultimo caso, il funzionario verbalizzante deve registrare i motivi nel verbale di fermo e perquisizione.

Per ulteriori informazioni, cfr. Regno Unito, Home Office (2014a).

2.3. Rendicontabilità

Punti salienti

- I funzionari delle autorità di contrasto e di gestione delle frontiere hanno la responsabilità di mantenere la profilazione nell'ambito della legalità e sono tenuti a **renderne conto**.
- La **raccolta di dati affidabili, esatti e tempestivi** sulle attività di profilazione è fondamentale per garantire la rendicontabilità.
- L'istituzione di **meccanismi di reclamo efficaci** permette di scongiurare gli abusi di potere e al tempo stesso di assicurare e ristabilire la fiducia nell'operato delle autorità di polizia e gestione delle frontiere.
- L'organizzazione di **incontri con i cittadini** per sentire i loro pareri, discutere il tema della profilazione e raccogliere feedback sulle operazioni offre la possibilità di trarre insegnamenti importanti e migliorare le attività di profilazione.

La rendicontabilità è un principio fondamentale della governance democratica. In termini molto generali, comporta che si debba rispondere ai soggetti che hanno diritto di chiedere conto di qualcosa ([35]). La rendicontabilità si applica non soltanto alle decisioni individuali, ma anche a quelle delle istituzioni («rendicontabilità istituzionale»). In quanto pubblici ufficiali e organismi pubblici, i funzionari delle autorità di contrasto e di gestione delle frontiere e le rispettive organizzazioni devono rendere

([35]) Bovens, M., Schillermans, T. e Goodlin, R.E. (2014), pagg. 1-11.

conto alla collettività delle proprie decisioni e delle proprie azioni e quindi devono garantire che la profilazione sia effettuata conformemente alla legge.

La raccolta di dati affidabili, esatti e tempestivi è fondamentale per garantire la rendicontabilità. Poiché molti dati contengono informazioni personali sensibili, il loro trattamento deve essere effettuato in conformità alle norme e alle procedure in materia di protezione dei dati (cfr. capitolo 3).

Checklist per la rendicontabilità

La checklist che segue fornisce una panoramica di base delle misure che le autorità di contrasto e di gestione delle frontiere possono adottare per garantire la rendicontabilità relativamente alle decisioni e alle attività di profilazione. La checklist può orientare i funzionari verso il miglioramento della rendicontabilità, ma non dovrebbe essere intesa come un elenco di adempimenti obbligatori per i funzionari delle autorità di contrasto e di gestione delle frontiere. A seconda del contesto, alcune raccomandazioni potrebbero non essere applicabili alla gestione delle frontiere, viste le sue peculiarità.

1. Identificare

- ☑ Prendere atto del problema della profilazione illecita e **riconoscerlo**. I preconcetti e gli stereotipi esistono e presentano rischi per i soggetti coinvolti, compresi i funzionari e le comunità locali.
- ☑ **Raccogliere e utilizzare dati disaggregati:** sono uno strumento importante per valutare l'efficacia e la prestazione.
- ☑ Partecipare a gruppi di discussione esterni organizzati dalla comunità o dalla società civile per ottenere un **feedback** sulle prassi utilizzate e per accrescere la fiducia nel proprio operato.

2. Raccogliere informazioni

- ☑ Garantire la rendicontabilità **conservando registrazioni** delle attività di profilazione.
- ☑ Fatte salve le garanzie necessarie, la **videosorveglianza** e/o le **videocamere indossabili** possono migliorare la rendicontabilità

e fornire prove a sostegno delle azioni volte a modificare modelli di comportamento non imparziali.

☑ Creare **moduli per i verbali di fermo e perquisizione** che i funzionari di polizia devono compilare dopo ogni fermo.

3. Agire e prevenire

☑ Effettuare **valutazioni** per individuare eventuali norme e prassi che perpetuano i preconcetti espliciti o impliciti e stereotipi negativi.

☑ Introdurre corsi specifici e/o **sessioni di formazione** su come affrontare i preconcetti personali e istituzionali e gli stereotipi.

☑ **Fornire informazioni** alle persone che vengono fermate per aumentare la percezione che la finalità del fermo sia equa e fornire alle persone informazioni sufficienti affinché possano decidere se chiedere riparazione. Per i casi di invio a verifiche in seconda linea ai valichi di frontiera, la comunicazione di informazioni costituisce un obbligo giuridico.

☑ Mostrare **tolleranza zero** nell'organizzazione per gli episodi fondati su preconcetti.

☑ Istituire **meccanismi interni** di supervisione e di controllo, ad esempio gruppi di discussione interni per discutere se i fermi siano effettuati sulla base di motivi ragionevoli.

☑ Assicurarsi che gli **indicatori di prestazione** siano legati al fatto di evitare l'imparzialità e gli stereotipi.

☑ Istituire **meccanismi di reclamo** per scoraggiare gli abusi di potere e garantire la rendicontabilità.

Fonte: FRA (2018)

2.3.1. Sorveglianza interna

La direzione e la gestione delle autorità di polizia e di gestione delle frontiere svolgono un ruolo importante nella definizione di una deontologia che tuteli i diritti individuali e il principio di non discriminazione, sia all'interno dell'organizzazione che nei suoi rapporti con la popolazione; inoltre, contribuiscono a creare un clima di rendicontabilità e trasparenza. La comunicazione aperta tra il personale (sia orizzontale

che verticale) e la definizione di norme di comportamento chiare, come i codici deontologici, sono due degli elementi interni che dovrebbero essere posti in atto per accrescere la rendicontabilità. Anche le assunzioni e la formazione hanno un ruolo importante (cfr. sezione 2.2.3).

Ai sensi del diritto dell'UE, qualsiasi autorità o organismo pubblico deve designare un **responsabile della protezione dei dati** incaricato di consigliare le forze di polizia e di gestione delle frontiere riguardo ai loro obblighi in materia di protezione dei dati, tra cui la tenuta di registri delle attività di trattamento dei dati o lo svolgimento di valutazioni d'impatto sulla protezione dei dati. Nel contesto della profilazione, il responsabile della protezione dei dati, ad esempio, fornisce pareri e vigila affinché i dati personali raccolti per, o durante, la profilazione siano trattati e conservati in modo lecito.

Sotto la lente: il ruolo dei responsabili della protezione dei dati

La **direttiva di polizia** prevede che gli Stati membri debbano nominare un responsabile della protezione dei dati con il compito di:

- sorvegliare l'osservanza della normativa applicabile in materia di protezione dei dati personali, compresi:
  - l'attribuzione delle responsabilità;
  - la sensibilizzazione e la formazione del personale;
  - le attività di controllo;
- fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- fungere da punto di contatto per l'autorità di controllo.

Il responsabile della protezione dei dati dovrebbe essere coinvolto pienamente e tempestivamente in tutte le questioni riguardanti la protezione dei dati personali.

Cfr. articoli 32-34 della direttiva di polizia.

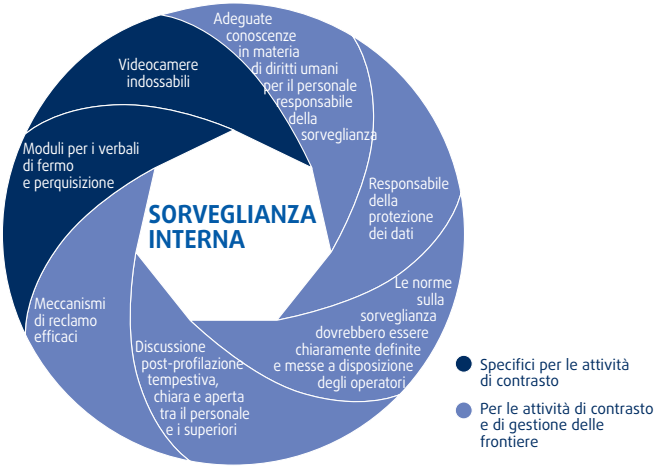
Nelle forze di polizia, la sorveglianza interna della profilazione può essere effettuata nell'ambito di un'ampia gamma di altre misure volte a tenere registri delle interazioni tra le autorità e la popolazione generale (cfr. figura 10), anche mediante l'uso di:

- **moduli per i verbali di fermo e perquisizione:** tali moduli sono un utile strumento pratico per incoraggiare i funzionari a effettuare fermi fondati su solidi motivi e per promuovere l'apertura e la rendicontabilità nei confronti della popolazione (cfr. sezione 2.2.5);

- **videocamere indossabili:** fatte salve le garanzie necessarie, possono rafforzare la fiducia tra le comunità e la polizia e fungere da deterrente per l'uso improprio della forza e la discriminazione (cfr. sezione 2.3.2).

Anche le attività di sorveglianza interna nelle organizzazioni di gestione delle frontiere possono avvalersi di tali misure; ad esempio, il catalogo Schengen raccomanda di registrare il numero e i motivi dell'invio alla verifica in seconda linea. Inoltre, i diversi contesti dei controlli di frontiera, le infrastrutture ai valichi di frontiera e la presenza in loco dei superiori creano altre opportunità di sorveglianza interna; ad esempio, possono essere disponibili attrezzature tecnologiche supplementari come gli impianti di videosorveglianza.

Figura 10: Elementi della sorveglianza interna



Fonte: *FRA (2018)*

Fatte salve le garanzie necessarie, i video possono fornire elementi per valutare il modo in cui viene svolta la profilazione e fornire prove in caso di reclami specifici; ad esempio, potrebbero confermare se il comportamento di una persona in attesa della verifica in prima linea abbia fornito un motivo sufficiente per inviarla a una verifica in seconda linea.

A differenza delle operazioni di fermo e perquisizione, la presenza della videosorveglianza è considerata probabile dai passeggeri ai valichi di frontiera, dato che questi sono luoghi pubblici in cui si applicano considerazioni legate alla sicurezza. L'uso di tali strumenti, tuttavia, deve rispettare il diritto alla privacy e le norme applicabili in materia di protezione dei dati.

La tenuta di registri può offrire vantaggi sia a breve che a lungo termine. L'esempio dei moduli per i verbali di fermo e perquisizione indica che:

- nell'**immediato**, i moduli dei verbali di fermo e perquisizione possono assicurare la rendicontabilità sul posto. Nel Regno Unito, ogni persona fermata riceve una registrazione del modulo del verbale di fermo o una ricevuta indicante dove è possibile accedere a una copia. Il verbale riporta il motivo del fermo e informazioni sulle modalità di reclamo e precisa inoltre dove può essere presentato reclamo: in questo modo, la persona può vedere il motivo e, se lo ritiene iniquo, contestarlo;

- a **lungo termine**, l'analisi dei registri permette alla polizia di capire se i poteri di fermo e perquisizione sono esercitati in maniera sproporzionata nei confronti di membri di determinati gruppi minoritari e adattare di conseguenza gli orientamenti forniti ai funzionari. I registri possono essere resi pubblici per aumentare la trasparenza e promuovere la fiducia della popolazione nell'uso dei poteri di fermo e perquisizione.

Tenuta di registri: che cosa dice la legge?

Per garantire la liceità del trattamento dati, la direttiva di polizia prevede che le autorità preposte all'applicazione della legge debbano tenere un registro di tutte le categorie di attività di trattamento effettuate sotto la propria responsabilità. Inoltre, nei sistemi di trattamento automatizzato, tali autorità sono tenute ad effettuare registrazioni che consentano di sapere chi ha consultato o comunicato dati personali, data e ora in cui ciò è avvenuto, chi ha ricevuto i dati e la motivazione del trattamento dei dati (cfr. sezione 3.1.3).

Articoli 24 e 25 della direttiva di polizia

Caso di studio

Utilizzo di registri per rilevare la sproporzionalità nelle operazioni di fermo e perquisizione (Regno Unito)

Il codice di buona pratica relativo alla legge sulle prove penali e la polizia elaborato in Inghilterra e Galles (Regno Unito) stabilisce che le forze di polizia abbiano per legge l'obbligo di sorvegliare l'uso dei poteri di fermo e perquisizione per accertare se siano «esercitati sulla base di immagini stereotipate o di generalizzazioni inappropriate». Qualsiasi uso apparentemente sproporzionato dei poteri da parte di particolari operatori o gruppi di operatori o in relazione a specifici gruppi della comunità dovrebbe essere identificato e indagato e dovrebbero essere adottate misure adeguate per porvi rimedio. Inoltre, la polizia deve prendere disposizioni affinché i registri siano esaminati dai rappresentanti della comunità e spiegare l'uso dei poteri di fermo e perquisizione a livello locale.

Per ulteriori informazioni, cfr. Regno Unito, Home Office (2014a).

La polizia del Regno Unito ha messo a punto vari strumenti per aumentare la trasparenza rendendo facilmente accessibili i dati relativi a fermi e perquisizioni. Il sito www.police.uk permette agli utenti di inserire il proprio codice postale per avere informazioni dettagliate sul numero e sulla natura dei fermi nella propria zona. Le informazioni pubblicate sono ricavate dai moduli dei verbali di fermo e perquisizione compilati. Inoltre, il quadro di controllo su fermi e perquisizioni della polizia metropolitana fornisce dati su tutte le operazioni di fermo e perquisizione a Londra, compresa la percentuale di persone appartenenti a minoranze etniche fermate rispetto alla popolazione complessiva. Gli utenti possono accedere online a dati dettagliati in vari modi, ad esempio mediante:

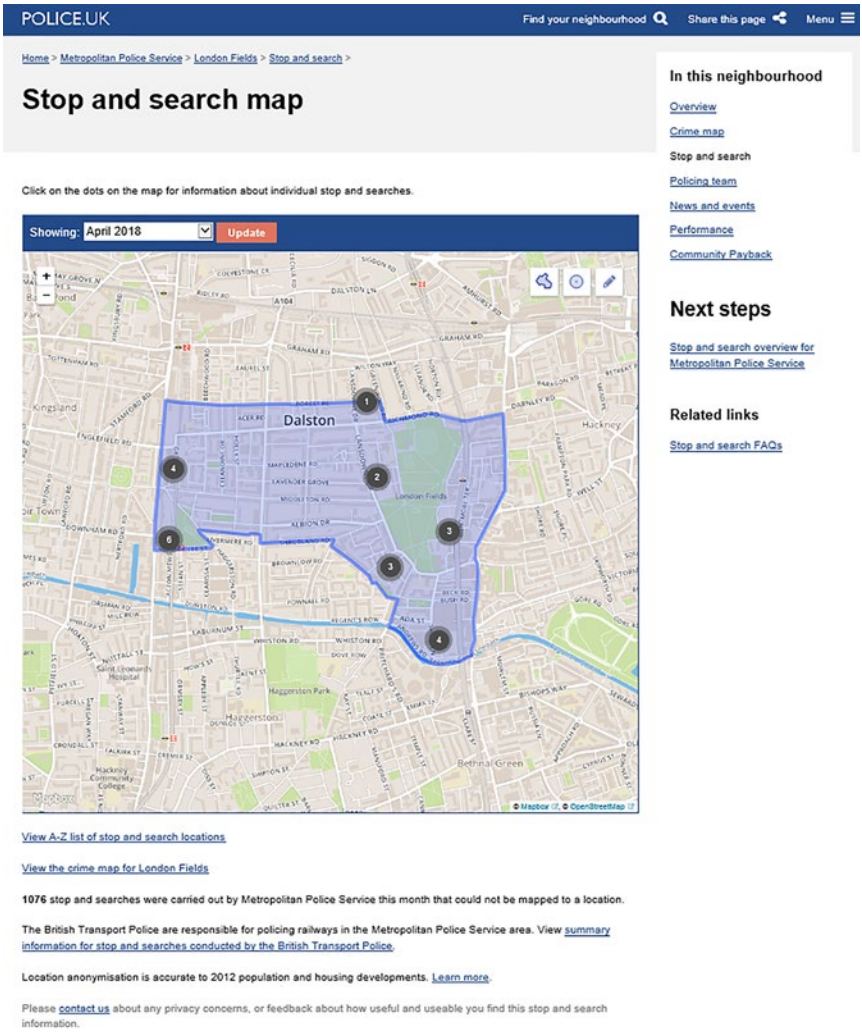
- una mappa in cui è indicata, su base mensile, la posizione esatta delle operazioni di fermo e perquisizione effettuate in una determinata zona, con informazioni dettagliate su ciascuna operazione (oggetto, tipo, esito, se è stata effettuata nel quadro di un'operazione di mantenimento dell'ordine), sulla persona fermata (genere, fascia di età, origine etnica dichiarata, origine etnica indicata dall'operatore) e sulle norme che hanno giustificato il fermo (cfr. figura 11);

- un quadro d'insieme delle statistiche e dei grafici sulle operazioni di fermo e perquisizione della polizia, che consente di aggregare e scaricare i dati.

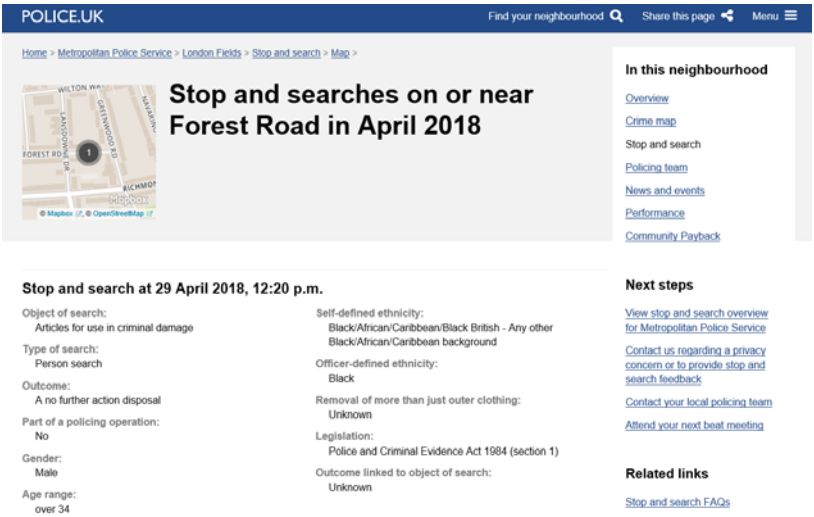
Tale prassi promuove la trasparenza e la fiducia ma potrebbe incidere sul diritto alla privacy e sulla protezione dei dati degli interessati: è possibile, infatti, che l'identità di

una persona possa essere dedotta dalla combinazione di dati disponibili in questo o in altri strumenti online. Tali rischi devono essere valutati e, ove necessario, affrontati.

Figura 11: Strumento online che mostra i dettagli delle operazioni di fermo e perquisizione effettuate a Londra



Fonte: *Regno Unito, Home Office, pagina web sulla mappa dei fermi e delle perquisizioni*



Fonte: *Regno Unito, Home Office, pagina web sulle perquisizioni specifiche*

2.3.2. Videocamere indossabili

Le forze di polizia utilizzano sempre più le videocamere indossabili, che svolgono un ruolo importante nel garantire la rendicontabilità, migliorare la qualità delle singole interazioni e modificare i modelli di comportamento non imparziali e possono anche contribuire a smorzare situazioni pericolose. Oltre al personale di polizia, anche i cittadini sempre più spesso riprendono i fermi e le altre interazioni con la polizia; anche questi video possono essere utilizzati per esaminare l'operato della polizia.

Caso di studio

L'efficacia delle videocamere indossabili

Nel Regno Unito, uno studio condotto nel 2015 sull'uso di 500 videocamere da parte di 814 agenti della polizia metropolitana ha evidenziato che non vi era «nessuna incidenza complessiva sul numero o sul tipo di fermi e perquisizioni effettuati; nessun effetto sulla proporzione di arresti per crimini violenti; e nessuna prova che le videocamere abbiano modificato le modalità di

interazione con le vittime o i sospetti». Relazioni che valutano l'impatto di sperimentazioni simili presentate da altre forze di polizia evidenziano che vi sono scarse prove, o addirittura nessuna, che le videocamere abbiano avuto un effetto positivo sulla riduzione della criminalità, sulle denunce presentate nei confronti degli operatori o sull'uso della forza.

Per ulteriori informazioni, cfr. Big Brother Watch (2017).

In Francia, le videocamere indossabili sono state utilizzate in 300 località per un periodo pilota di due anni. Nel giugno 2018 un riesame effettuato dal ministero dell'Interno ha evidenziato gli effetti positivi e i risultati della sperimentazione. In particolare, è emerso che le videocamere indossabili hanno avuto un effetto deterrente sui soggetti fermati, scoraggiando le aggressioni o gli oltraggi nei confronti della polizia. Le relazioni dei comuni hanno indicato che l'uso di videocamere individuali ha ridotto l'aggressività e gli oltraggi nei confronti dei funzionari di polizia. Alcuni comuni hanno sottolineato che l'uso di videocamere indossabili sembra avere smorzato situazioni che altrimenti avrebbero potuto sfociare in reati contro i funzionari di polizia. Sebbene le relazioni indichino che l'utilità delle videocamere indossabili risiede in particolare nella capacità di dissuasione, in qualche caso le riprese sono state utilizzate come prova nei procedimenti giudiziari per identificare gli autori di reati. Infine, diversi comuni hanno sottolineato l'utilità educativa delle videocamere, in quanto alcuni funzionari di polizia hanno ricevuto una formazione sulle procedure e le tecniche di intervento guardando le registrazioni effettuate durante gli interventi. A seguito del progetto pilota, è stato presentato al parlamento francese un progetto di legge che mira ad armonizzare l'uso delle videocamere indossabili in tutte le forze di polizia e ad estenderne l'impiego ai vigili del fuoco e alle guardie penitenziarie.

Per ulteriori informazioni, cfr. Francia, Ministero dell'interno (2018).

Nel 2012-2013 a Rialto, negli Stati Uniti, è stata condotta per 12 mesi un'ampia sperimentazione sull'uso delle videocamere indossabili volta a stabilire se l'uso di tali apparecchi induca gli operatori ad adottare comportamenti socialmente auspicabili. I risultati mostrano che, rispetto al 2011, durante i 12 mesi della sperimentazione i casi di uso della forza sono scesi da 60 a 25 e le denunce nei confronti della polizia sono scese da 28 a 3.

Per ulteriori informazioni, cfr. Farrar, T. (2018).

Tuttavia, l'utilizzo di videocamere indossabili da parte della polizia desta preoccupazioni sia per quanto riguarda i diritti fondamentali che sul piano operativo. Per affrontare tali preoccupazioni sono necessarie garanzie e politiche chiare relative al loro uso:

- il **ruolo delle videocamere indossabili ai fini dell'accertamento e dissuasione della profilazione illecita** non è chiaro. Le videocamere catturano singoli episodi e non consentono la raccolta di dati statistici utilizzabili per stabilire se le operazioni di fermo e perquisizione siano discriminatorie. Possono tuttavia essere utilizzate per esaminare e discutere singoli fermi, contribuendo a migliorarne la qualità;

- l'uso di videocamere indossabili potrebbe avere **ripercussioni negative sui rapporti con le comunità di minoranza**, se ritengono di essere prese di mira in modo specifico. La messa a punto di garanzie e politiche in consultazione con le comunità locali può contribuire a promuovere le videocamere indossabili come strumento per migliorare la rendicontabilità piuttosto che come mezzo per stigmatizzare i gruppi di minoranza;

- l'uso di videocamere indossabili ha **conseguenze sul diritto alla privacy e alla protezione dei dati**, nonché su altri diritti umani fondamentali: ad esempio, le videocamere indossabili possono ledere la libertà di riunione pacifica se vengono utilizzate per controllare manifestazioni pubbliche. Spesso non è chiaro quando si debbano accendere o spegnere e cosa accade se un operatore dimentica di accendere la videocamera o decide di non farlo; sono quindi necessarie indicazioni precise a questo riguardo. Le imprese private che forniscono questo servizio devono avere ben chiaro che non possono trattare i video per le proprie finalità. L'uso di videocamere indossabili deve essere disciplinato per legge al fine di garantire il rispetto dei diritti fondamentali.

Sotto la lente: uso efficace delle videocamere indossabili

Il rispetto di tre importanti principi può contribuire a garantire un uso efficace delle videocamere indossabili:

- **autenticità:** le immagini devono essere palesemente riconducibili all'episodio. Dovrebbero essere registrate la data e l'ora (ad esempio mediante marcatura temporale) e l'ubicazione esatta (ad esempio mediante GPS) del fermo;

- **affidabilità:** le immagini dovrebbero essere caricate nel sistema centrale in modo rigoroso, sicuro e riservato. Le immagini dovrebbero inoltre rispettare il principio della protezione dei dati e del rispetto per la vita privata, e quindi non dovrebbero essere conservate più a lungo di quanto consentito dalla legge;
- **ammissibilità:** per essere utili nei procedimenti penali, i filmati devono essere ammissibili nei procedimenti giudiziari. Ciò può comportare la necessità di:
  - evitare registrazioni video continue, che interferiscono in modo inaccettabile con il diritto alla privacy sia dei funzionari di polizia che delle persone riprese;
  - informare le persone che possono essere riprese e ottenere il loro consenso (se necessario);
  - conservare immagini con un livello di sicurezza adeguato e tenere traccia dell'accesso alle immagini da parte sia dei funzionari di polizia che dei cittadini.

Per ulteriori informazioni, cfr. Coudert e al. (2015), pag. 8.

Ulteriori sviluppi tecnologici richiederanno l'elaborazione di nuove misure di salvaguardia per garantire che le videocamere indossabili siano utilizzate in modo lecito. Ad esempio, gli apparecchi da ripresa che possono riconoscere automaticamente il volto di una persona confrontandolo con i dati inseriti in una banca dati esistente pongono nuovi problemi riguardo al diritto alla privacy e alla protezione dei dati.

Caso di studio

Videocamere indossabili per la polizia: scheda comparativa delle politiche (Stati Uniti)

Per aumentare la trasparenza e la rendicontabilità in relazione alle videocamere indossabili, la Leadership Conference on Civil and Human Rights & Upturn degli Stati Uniti ha messo a punto uno strumento per valutare e strutturare le informazioni che si possono estrarre dai video ripresi dalle videocamere indossabili.

Lo strumento propone otto criteri, che permettono di valutare:

1) se le riprese siano rese pubbliche e messe prontamente a disposizione dalla polizia;

2) se il margine di discrezionalità degli operatori riguardo a quando effettuare le riprese sia chiaramente indicato;

3) se le preoccupazioni relative alla tutela della vita privata siano prese in considerazione;

4) se i funzionari debbano rivedere le riprese prima di redigere il verbale iniziale;

5) se le riprese non classificate come riprese da conservare debbano essere cancellate entro un termine predefinito;

6) se le riprese siano protette contro la manomissione e l'uso improprio;

7) se le riprese siano messe a disposizione delle persone che presentano reclami o denunce;

8) se l'uso di tecnologie biometriche per identificare gli individui che compaiono nelle riprese sia limitato o meno.

Tali iniziative possono contribuire a rafforzare la rendicontabilità definendo norme e incoraggiando l'attuazione di meccanismi per valutare se le riprese vengano acquisite e utilizzate in modo corretto.

Per ulteriori informazioni, cfr. Leadership Conference on Civil and Human Rights & Upturn, scheda comparativa delle politiche.

2.3.3. Meccanismi di reclamo

L'istituzione di meccanismi di reclamo efficaci permette di scongiurare abusi di potere e al tempo stesso contribuisce ad assicurare e ristabilire la fiducia nell'operato delle autorità di polizia e gestione delle frontiere. Tali meccanismi di solito affiancano i canali legali che consentono di impugnare l'azione o la decisione di un'autorità pubblica dinanzi a un tribunale indipendente e imparziale.

Affinché siano efficaci, è essenziale che:

- **i meccanismi di reclamo siano facilmente accessibili**: i dati indicano sistematicamente che vi è riluttanza a presentare reclami, ad esempio perché il procedimento è lungo o costoso, oppure perché si temono ripercussioni negative. Rendendo i meccanismi di reclamo facilmente accessibili tramite l'uso di piattaforme online quali siti web o app se ne può incoraggiare l'utilizzo. È possibile inoltre prevedere che un'organizzazione possa aiutare le persone a presentare un reclamo, proponendolo essa stessa per l'interessato o tramite meccanismi di ricorso collettivo, come stabilito dall'articolo 80, paragrafo 2, del GDPR;

- **i reclami siano trattati in modo trasparente**, così da accrescere la fiducia nei meccanismi di reclamo;

- gli **organismi di reclamo siano indipendenti** dall'organizzazione o dalla parte dell'organizzazione nei confronti della quale è presentato il reclamo.

Esistono molti meccanismi diversi che trattano diversi tipi di reclami. La figura 12 fornisce una panoramica di alcuni dei meccanismi di reclamo disponibili negli Stati membri e a livello dell'UE.

I meccanismi in cui i funzionari di polizia si confrontano con i cittadini per ascoltare i loro reclami, discutere la profilazione e ottenere un feedback sul proprio operato offrono l'opportunità di trarre insegnamenti importanti per migliorare i processi che regolano la profilazione; inoltre, creano uno strumento per coinvolgere i cittadini nelle attività di contrasto (cfr. caso di studio).

Figura 12: Panoramica dei meccanismi di reclamo negli Stati membri dell'UE

Fonte: *FRA (2018)*

Caso di studio

Meccanismi di reclamo pubblici nel settore dell'attività di contrasto

Gruppi di controllo pubblici (West Midlands Police, Regno Unito)

In ognuna delle otto divisioni territoriali della West Midlands Police (WMP) si svolge una riunione bimensile del gruppo di controllo delle attività di fermo e perquisizione, presieduto da cittadini. Il gruppo valuta i registri dei fermi e delle perquisizioni, si assicura che la WMP rispetti la legge e mette a disposizione delle comunità un canale per presentare i reclami e richiamare l'attenzione su questioni problematiche. Gli ordini del giorno e i verbali delle riunioni sono pubblicati online. La WMP ha adottato una serie di ulteriori prassi di coinvolgimento delle comunità nell'intento di rendere i fermi più equi e più mirati e di accrescere la rendicontabilità degli operatori di polizia.

Per ulteriori informazioni, cfr. West Midlands Police, pagina dedicata ai fermi e perquisizioni, e Her Majesty's Inspectorate of Constabulary (2016).

Gruppo di discussione sui ragionevoli motivi (Northamptonshire Police, Regno Unito)

La Northamptonshire Police ha istituito un gruppo di discussione sui ragionevoli motivi per coinvolgere la popolazione nel miglioramento delle operazioni di fermo e perquisizione. Il gruppo è un canale di discussione sull'uso dei poteri di fermo e perquisizione e sul loro impatto sulle comunità. È presieduto da un ispettore capo ed è composto da un membro della polizia con funzioni operative e da due membri della comunità, che possono anche essere persone che hanno commesso un reato. Oltre a migliorare la comunicazione tra la polizia e la popolazione, il gruppo può privare i funzionari dei loro poteri e inviarli a un'ulteriore formazione volta a migliorare le loro attività di fermo e perquisizione.

Per ulteriori informazioni, cfr. Northamptonshire Police, pagina dedicata al gruppo sui ragionevoli motivi, e Open Society Justice Initiative (2018a).

Rete informale di meccanismi di reclamo nei confronti della polizia

La rete delle autorità indipendenti che si occupano dei reclami nei confronti della polizia (Independent Police Complaints Authorities' Network, IPCAN) è una rete informale per lo scambio e la cooperazione tra strutture indipendenti che si occupano del controllo esterno delle forze di sicurezza. È stata creata nel 2013 e riunisce le autorità per la gestione dei reclami di una ventina di paesi, in maggioranza Stati membri dell'UE. Tali organismi ricevono e danno corso ai reclami nei confronti delle forze di sicurezza pubbliche e, in qualche caso, private.

Per ulteriori informazioni, cfr. sito dell'IPCAN.

Nella gestione delle frontiere, i meccanismi di reclamo pubblici possono prevedere la presentazione del reclamo sul posto o a posteriori. La possibilità di accedere a tali meccanismi aumenta la trasparenza e la rendicontabilità e promuove il rispetto reciproco e le buone relazioni tra le guardie di frontiera e la popolazione. La possibilità di presentare un reclamo a posteriori a un organismo superiore anziché (solo) direttamente al valico di frontiera assicura un certo grado di supervisione e può influenzare positivamente la propensione dei viaggiatori a denunciare eventuali episodi ([36]).

Caso di studio

Meccanismi di reclamo pubblici nella gestione delle frontiere

Meccanismo di reclamo interno all'aeroporto di Manchester (Regno Unito)

All'aeroporto di Manchester, il Central Allocation Hub offre un punto di contatto unico a disposizione di tutti i passeggeri che intendono presentare un reclamo. I reclami possono essere presentati mediante posta elettronica, per lettera, telefonicamente, via fax o di persona, in inglese o in gallese. Gli orientamenti dell'autorità di frontiera (Border Force) del Regno Unito illustrano le possibili modalità di risoluzione dei reclami. I reclami legati a condotte scorrette di lieve entità, quali il comportamento sgarbato, brusco o comunque inappropriato, possono in genere essere risolti a livello locale, ad esempio chiarendo la questione, spiegando le procedure operative,

([36]) FRA (2014b).

concordando ulteriori azioni e porgendo delle scuse, se del caso. I reclami relativi a colpe gravi sono in genere assegnati all'unità Professional Standards che si occupa di norme deontologiche. Gli orientamenti della Border Force includono criteri per la determinazione di segnali di possibile discriminazione, che costituirebbero una colpa grave. Se gli elementi disponibili fanno subito ritenere che il trattamento di un passeggero possa essere motivato da fattori diversi dalla razza, di solito il caso è risolto a livello locale.

Per ulteriori informazioni, cfr. FRA (2014a), pag. 74.

Meccanismo di denuncia individuale di Frontex (UE)

A seguito dell'adozione del nuovo regolamento relativo all'Agenzia europea della guardia di frontiera e costiera nel 2016, Frontex ha istituito un meccanismo di denuncia individuale per monitorare il rispetto dei diritti fondamentali nelle attività dell'Agenzia. Tali attività comprendono progetti pilota, operazioni di rimpatrio, operazioni congiunte, interventi rapidi alle frontiere, dispiegamento di squadre di sostegno per la gestione della migrazione e interventi di rimpatrio. Qualsiasi persona i cui diritti siano stati direttamente lesi dalle azioni del personale (compreso il personale delle autorità pubbliche nazionali) che partecipa a tali attività di Frontex può presentare una denuncia al responsabile dei diritti fondamentali di Frontex. Il responsabile dei diritti fondamentali decide in merito all'ammissibilità del reclamo e lo invia al direttore esecutivo di Frontex, nonché alle autorità dello Stato membro interessato, se nella presunta violazione è coinvolto personale nazionale. La denuncia può essere presentata in qualsiasi lingua, per posta elettronica, lettera o tramite un modulo di reclamo online disponibile sul sito di Frontex: http://frontex.europa.eu/complaints/.

Sotto la lente: i diritti dei funzionari delle autorità di contrasto

I funzionari di polizia godono degli stessi diritti e delle stesse libertà degli altri cittadini e sono tutelati dalle norme in materia di diritti umani nello svolgimento delle loro funzioni. Possono quindi fare riferimento ai diritti sanciti da vari documenti internazionali sui diritti umani, come la convenzione europea dei diritti dell'uomo o il Patto internazionale relativo ai diritti civili e politici (ICCPR). Il codice europeo di etica per la polizia chiarisce che «[i]l personale di polizia gode di norma degli stessi diritti civili e politici degli altri cittadini. Questi diritti possono subire limitazioni solo quando questo si rende

necessario all'esercizio delle funzioni della polizia in una società democratica, in applicazione della legge, e in conformità con la convenzione Europea dei Diritti dell'Uomo». Un'eccezione a questa nozione generale è contenuta nell'articolo 11 CEDU, che riguarda la libertà di riunione e di associazione.

Durante lo svolgimento delle funzioni di polizia, soprattutto quando applica i poteri di polizia, un funzionario di polizia non agisce in veste di privato cittadino ma in qualità di pubblico ufficiale. L'obbligo dello Stato di rispettare e tutelare i diritti umani, pertanto, ha un effetto diretto sulle possibili risposte di un funzionario di polizia alle aggressioni. I diritti dei funzionari di polizia, che potrebbero rischiare di rimanere feriti o perdere la vita nell'esercizio delle proprie funzioni, devono anch'essi essere rispettati e protetti, per esempio fornendo dispositivi di protezione, pianificando attentamente le operazioni di polizia o mettendo a punto misure preventive. Le restrizioni dei diritti di un funzionario di polizia potrebbero essere necessarie per l'esercizio delle funzioni di polizia, ma ogni eventuale limitazione deve sempre riflettere il principio di proporzionalità. In considerazione del loro particolare ruolo di pubblici ufficiali, gli operatori di polizia possono essere soggetti a una maggiore restrizione dei propri diritti rispetto ai «normali cittadini». Nel caso ad esempio di una manifestazione che degenera in violenza, un «normale cittadino» potrebbe scappare o cercare aiuto, mentre un agente di polizia è obbligato a proteggere i diritti umani altrui e a ripristinare l'ordine pubblico.

Per ulteriori informazioni, cfr. FRA (2013).

3 Profilazione algoritmica

La profilazione algoritmica comprende tecniche informatiche costituite da una serie di passaggi successivi che analizzano i dati per individuare tendenze, modelli o correlazioni ([37]). Con la profilazione, la persona viene selezionata «sulla base di connessioni con altre persone identificate dall'algoritmo e non di un comportamento effettivo» e «le scelte degli individui sono strutturate in base alle informazioni sul gruppo» e non alle loro scelte personali ([38]).

Per le autorità di contrasto e di gestione delle frontiere, la profilazione algoritmica può essere un modo efficiente di utilizzare i dati a fini di prevenzione, accertamento e indagine sui reati. La raccolta e l'elaborazione di grandi set di dati destano tuttavia una serie di preoccupazioni in merito ai diritti fondamentali. A questo proposito, occorre tenere conto non soltanto dell'importanza di evitare discriminazioni, ma anche del fatto che la profilazione algoritmica introduce nuovi rischi, in particolare in relazione al diritto alla privacy e alla protezione dei dati. Questa sezione analizza innanzitutto questi nuovi rischi, per poi illustrare i problemi legati all'uso della profilazione algoritmica in banche dati su larga scala ai fini della gestione delle frontiere e della sicurezza; infine propone alcuni sistemi per ridurre al minimo tali rischi.

([37]) Per ulteriori informazioni sugli algoritmi, cfr. FRA (2018b), pag. 4.

([38]) Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. e Floridi, L. (2016).

Sotto la lente: attività di polizia di tipo predittivo

Le autorità di contrasto utilizzano diversi software per prevedere quando e dove sarà commesso un reato, ad esempio PredPol nel Regno Unito e negli Stati Uniti, il Criminality Awareness System (CAS) nei Paesi Bassi e Precobs in Germania e in Svizzera. Tuttavia, l'efficacia di tali metodi predittivi per la prevenzione dei reati non è stata ancora adeguatamente valutata. Gli elementi fin qui raccolti mostrano risultati contraddittori, come indicano gli esempi che seguono.

Sperimentazione sul campo dell'attività di polizia predittiva nel Kent (Regno Unito) e a Los Angeles (Stati Uniti)

Nel Regno Unito e negli Stati Uniti la polizia ha condotto un esperimento per confrontare, rispetto a un approccio più tradizionale, un algoritmo totalmente automatizzato per l'identificazione dei punti nevralgici della criminalità e la conseguente pianificazione delle pattuglie di polizia.

I risultati dell'esperimento hanno evidenziato che l'algoritmo automatizzato era in grado di prevedere meglio i reati futuri: il numero di azioni criminali previsto da tale algoritmo è infatti risultato 1,4-2,2 volte superiore rispetto a quello previsto da un analista del crimine utilizzando informazioni di intelligence sulla criminalità e mappe della criminalità. Anche i pattugliamenti basati sullo strumento predittivo sono risultati più efficaci e hanno permesso di ridurre in media del 7,4 % il numero di reati.

Per ulteriori informazioni, cfr. Mohler, G.O., e al. (2016).

Programma PILOT di focalizzazione operativa predittiva basata sulle informazioni di intelligence a Shreveport (Stati Uniti)

Il programma PILOT utilizza un modello predittivo per identificare piccole zone in cui vi è un rischio accresciuto di reati contro il patrimonio e per applicare in tali zone un modello di intervento volto a prevenire tali reati. I risultati ottenuti in tre distretti in cui si è utilizzato PILOT sono stati messi a confronto con quelli ottenuti in tre distretti in cui venivano svolte attività di polizia tradizionali. Nei tre distretti in cui si è utilizzato PILOT non è emersa alcuna prova statistica di una maggiore riduzione dei reati contro il patrimonio.

Per ulteriori informazioni, cfr. Hunt, P. e al. (2014).

Software Beware (Stati Uniti)

Il software Beware presenta agli operatori incaricati di rispondere alle chiamate di emergenza un codice colore (rosso, giallo e verde) che indica il livello di pericolosità della persona o del luogo a cui si riferisce la chiamata. Il codice viene ricavato dal software mediante una ricerca effettuata ad esempio nella banca dati dei verbali di arresto, nei registri dei beni, in banche dati commerciali, su Internet, sui social media e in altre banche dati pubbliche.

I punti di forza e di debolezza di questo sistema non sono stati valutati; tuttavia, la mancanza di supervisione sul processo decisionale e l'impossibilità di ottenere informazioni dettagliate sull'algoritmo, che è protetto da segreti industriali, hanno destato preoccupazioni in merito alla rendicontabilità. Inoltre, la potenziale inesattezza dei dati raccolti e/o delle informazioni ricavate dall'analisi può ridurre l'efficacia complessiva dello strumento.

Per ulteriori informazioni, cfr. American Civil Liberties Union (2016).

Caso di studio

Valutazione degli impatti e del rischio delle attività di polizia predittive: lo strumento di valutazione ALGO-CARE

Per garantire una visione d'insieme equilibrata e trasparente dell'impatto sulla società dell'attività di polizia di tipo predittivo occorre tenere conto dei potenziali effetti negativi. L'analisi effettuata da un gruppo composto da docenti universitari e personale di polizia ha concluso che l'attività di polizia di tipo predittivo richiede una valutazione dettagliata dell'impatto sulla società e sui singoli, essendo tale attività ancora in fase sperimentale nel Regno Unito. Secondo la ricerca, alcune decisioni potrebbero avere sulla società e sui singoli un impatto tanto grande da non poter lasciare che siano influenzate da una tecnologia emergente; tali casi dovrebbero essere sottratti al processo decisionale algoritmico.

Il gruppo ha messo a punto un quadro decisionale, denominato ALGO-CARE, per l'introduzione di strumenti di valutazione algoritmica nel contesto delle attività di polizia. Il quadro mira a orientare i funzionari di polizia nella valutazione dei rischi potenziali connessi all'uso delle attività di polizia di

tipo predittivo. Si prefigge inoltre di tradurre i principi fondamentali del diritto pubblico e dei diritti umani in considerazioni e orientamenti pratici che possono essere recepiti dagli enti pubblici.

Lo strumento di valutazione invita gli operatori di polizia a valutare il ricorso alle attività di polizia di tipo predittivo in base a otto aspetti complementari:

- **carattere orientativo:** valutare la portata dell'intervento umano;
- **liceità:** valutare la giustificazione giuridica per l'utilizzo dell'algoritmo;
- **granularità:** valutare se l'algoritmo possa raggiungere un livello di dettaglio sufficiente nel caso specifico;
- **titolarità:** fare in modo che la forza di polizia abbia la titolarità giuridica del codice sorgente e la capacità tecnica per accedervi, effettuarne la manutenzione, aggiornarlo e correggerlo regolarmente;
- **contestabilità:** provvedere affinché siano in atto meccanismi di vigilanza e controllo;
- **accuratezza:** valutare se l'algoritmo corrisponda al fine dell'attività di polizia e possa essere convalidato periodicamente e verificare che la probabilità e l'impatto della non accuratezza rappresentino un rischio accettabile;
- **responsabilità:** valutare l'equità, la rendicontabilità e la trasparenza dell'algoritmo;
- **spiegabilità:** valutare l'accessibilità delle informazioni relative alle regole decisionali e all'impatto che ciascun fattore ha sul risultato finale.

Per ulteriori informazioni, cfr. Oswald, M., e al. (2017).

3.1. Il quadro giuridico di protezione dei dati che disciplina la profilazione algoritmica

Lo sviluppo e l'uso crescente di nuove tecnologie — compreso l'uso crescente di grandi set di dati a sostegno del processo decisionale — hanno indotto l'Unione europea a rivedere in modo approfondito le norme che disciplinano il trattamento dei dati personali nel 2016. I due nuovi strumenti, il regolamento generale sulla protezione dei dati e la direttiva di polizia, stabiliscono principi e norme importanti che si applicano a qualsiasi decisione basata su processi decisionali informatizzati, compresa la profilazione algoritmica.

Il GDPR e la direttiva di polizia sono entrati in vigore nel maggio 2018; ciò significa che gli esempi pratici di attuazione di tali strumenti giuridici scarseggiavano al momento della stesura del presente documento. La sezione 1.2.2 descrive le norme giuridiche che disciplinano il diritto alla privacy e il diritto alla protezione dei dati e spiega alcune delle principali differenze tra il GDPR e la direttiva di polizia (cfr. tabella 2). Il presente capitolo riprende e amplia tali informazioni per descrivere e spiegare le disposizioni giuridiche in materia di profilazione algoritmica introdotte dal GDPR e dalla direttiva di polizia. Sono inclusi:

- il trattamento dei dati deve avere una finalità specifica fondata su una base giuridica specifica;
- le persone devono essere informate quando i loro dati personali sono sottoposti a trattamento;
- i dati devono essere conservati in modo sicuro;
- il trattamento illecito dei dati deve essere individuato e prevenuto.

I funzionari di polizia e le guardie di frontiera che necessitano di informazioni supplementari in merito alle disposizioni di legge descritte nel presente capitolo dovrebbero rivolgersi al responsabile della protezione dei dati della propria organizzazione. Inoltre, il manuale sulla normativa europea in materia di protezione dei dati, elaborato dalla FRA, dal GEPD e dal Consiglio d'Europa, offre ulteriori orientamenti sull'applicazione della direttiva di polizia e del GDPR ([39]).

([39]) FRA, GEPD e Consiglio d'Europa (2018).

Punti salienti

- La profilazione algoritmica deve essere **legittima**, **necessaria** e **proporzionata**.
- I dati non devono essere trattati senza una **finalità specifica fondata su una base giuridica specifica**.
- Ogni persona dispone di diritti specifici, descritti in dettaglio nelle disposizioni del GDPR e della direttiva di polizia, tra cui:
  - **il diritto di essere informata**, compreso il diritto di ricevere informazioni significative sulla logica utilizzata nell'algoritmo;
  - il diritto di **accedere ai propri dati personali**;
  - il diritto di **presentare reclamo un'autorità di controllo**;
  - il diritto a un **ricorso giurisdizionale effettivo**.
- I dati devono essere raccolti, trattati e conservati **in modo sicuro**.
- Il trattamento illecito dei dati deve essere **prevenuto** e **individuato**.

3.1.1. I dati devono essere trattati per una finalità specifica

Qualsiasi trattamento di dati personali deve avere una base giuridica, il che significa che deve essere effettuato per conseguire una **finalità specifica** prevista dalla legge.

Prima che avvenga qualsiasi trattamento, il funzionario deve conoscerne la finalità, quindi deve chiedersi, ad esempio:

- i dati sono trattati per accertare un reato?
- sono trattati per mantenere la sicurezza pubblica?
- sono trattati per contrastare il terrorismo?

Una volta correttamente identificata la finalità, i funzionari sanno quale quadro giuridico si applica e quali sono i relativi obblighi giuridici. La tabella 4 illustra come identificare il quadro giuridico applicabile.

Tabella 4: Come identificare il corretto quadro giuridico in funzione della finalità del trattamento

1. Qual è la finalità del trattamento dei dati?	
• **prevenzione, indagine, accertamento e perseguimento di reati** • **esecuzione di sanzioni penali** • **salvaguardia della sicurezza pubblica**	• qualsiasi altra finalità
⇩	⇩
2. Si applica la direttiva di polizia	**2. Si applica il regolamento generale sulla protezione dei dati**
⇩	⇩
3. Il diritto dell'Unione o nazionale definisce (*):	**3. Il trattamento è consentito solo se:**
• **quali dati personali possono essere trattati;** • **le finalità specifiche del trattamento dei dati.**	• l'interessato ha espresso il proprio **consenso**; • è necessario all'esecuzione di un **contratto**; • è necessario per adempiere un **obbligo legale**; • è necessario per la salvaguardia degli **interessi vitali** di una persona o • è necessario per l'**interesse pubblico**.
⇩	⇩

4. La finalità della profilazione è esentata dalla direttiva di polizia?	4. La finalità della profilazione è esentata dal GDPR?
Il diritto di essere informato, di accedere ai propri dati personali e di richiederne la modifica o la cancellazione può essere limitato (in tutto o in parte) nei seguenti casi: • **per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;** • **per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;** • **per proteggere la sicurezza pubblica;** • **per proteggere la sicurezza nazionale;** • **per proteggere i diritti e le libertà altrui.**	Gli obblighi (di trasparenza, informazione e notifica delle violazioni) e i diritti (di accesso, rettifica, cancellazione, opposizione o di non essere sottoposto a una decisione automatizzata) stabiliti nel GDPR **possono essere limitati** dal diritto nazionale o dell'UE al fine di salvaguardare: • la sicurezza nazionale, la difesa o la sicurezza pubblica; • la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; • altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; • la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; • le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; • una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri in casi specifici; • la tutela dell'interessato o dei diritti e delle libertà altrui; • l'esecuzione delle azioni civili.

(*) *Le leggi nazionali di recepimento della direttiva sono consultabili nel sito EUR-Lex.*

Fonte: *FRA (2018)*

3.1.2. Le persone fisiche devono essere informate

L'articolo 13 della direttiva di polizia e gli articoli 13 e 14 del GDPR prevedono che le persone fisiche siano informate quando i loro dati personali sono trattati. La tabella 5 indica come e quando si devono comunicare informazioni alla persona i cui dati sono in corso di trattamento.

Tabella 5: Obbligo di fornire alle persone informazioni sulla profilazione: tipo di dati, mezzi di comunicazione ed eccezioni

Obbligo di notifica — Elenco di controllo	
A chi?	Persona i cui dati sono trattati
Come?	• Linguaggio semplice e chiaro • In forma facilmente accessibile • Nella stessa forma della richiesta, *preferibilmente per via elettronica*
Che cosa?	**Informazioni sul trattamento**: • nome e dati di contatto della propria autorità • dati di contatto del proprio responsabile della protezione dei dati • finalità del trattamento • base giuridica del trattamento • periodo massimo di conservazione dei dati • tipi di persone/organizzazioni che riceveranno i dati **Informazioni sui diritti degli interessati:** • diritto di **proporre reclamo** a un'autorità di controllo e dati di contatto dell'autorità di controllo • diritto di chiedere l'**accesso** ai propri dati personali • **rettifica** e/o **cancellazione** dei dati personali • diritto di chiedere la **limitazione** del trattamento
Eccezioni	• Richieste eccessive (ossia ripetitive) o manifestamente infondate • Quando l'identità del richiedente non può essere confermata in modo chiaro • Quando la comunicazione delle informazioni comprometterebbe le indagini • Quando la comunicazione delle informazioni comprometterebbe la prevenzione/l'indagine su reati • Per tutelare la sicurezza pubblica o nazionale • Per tutelare i diritti di altre persone

Fonte: *FRA (2018)*

Sotto la lente: «diritto a una spiegazione»

In caso di profilazione, il GDPR impone di fornire all'interessato «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento». Tali informazioni dovrebbero essere fornite al momento della raccolta dei dati (notifica) e quando l'interessato chiede ulteriori informazioni (diritto di accesso). Questo diritto non è esplicitamente menzionato nella direttiva di polizia; tuttavia, il considerando 38 specifica che «[il trattamento automatizzato] dovrebbe essere subordinato a garanzie adeguate, compresi il rilascio di specifiche informazioni all'interessato [...] in particolare [...] di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione».

Questo «diritto a una spiegazione» può risultare difficile da attuare nella pratica. Alcune persone possiedono l'alfabetizzazione digitale necessaria per comprendere il codice di un algoritmo; per altre, invece, possono bastare informazioni semplificate sulla finalità del trattamento e sulle interconnessioni dei dati utilizzati. L'elemento che permette di valutare la significatività della spiegazione fornita è il suo obiettivo. La persona interessata dovrebbe ricevere informazioni sufficienti per comprendere le finalità, le motivazioni e i criteri che hanno portato all'adozione della decisione.

Il diritto a una spiegazione non è assoluto (cfr. fase 4 della tabella 4). Gli Stati membri possono limitarlo in diversi casi, ad esempio per motivi di sicurezza nazionale, difesa, sicurezza pubblica, prevenzione, indagine, accertamento o perseguimento di reati, esecuzione di sanzioni penali, protezione dell'interessato o dei diritti e delle libertà altrui, esecuzione delle azioni civili.

Ciò nondimeno, è buona regola fornire informazioni ragionevoli sulla finalità e sulle conseguenze previste del trattamento. L'elaborazione di metodi semplici per spiegare la logica e i criteri utilizzati per giungere a una decisione permette in definitiva di migliorare la trasparenza e la responsabilità.

Per ulteriori informazioni, cfr. GDPR, articoli 13-15 (diritto di informazione e diritto di accesso), articolo 22 (processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) e articolo 23 (limitazioni); e direttiva di polizia, articolo 11 (processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) e articoli 13-15 (diritto di informazione e diritto di accesso).

Cfr. anche gruppo di lavoro articolo 29 per la protezione dei dati (2018a).

3.1.3. Garantire la sicurezza dei dati: registri, registrazioni e norme sulla conservazione

Le autorità che raccolgono e trattano dati personali a fini di profilazione devono non solo trattare i dati in modo lecito, ma anche garantire che non siano:

- oggetto di accesso da parte di persone non autorizzate;
- utilizzati per finalità diverse dalla finalità originaria; o
- conservati più a lungo del necessario.

A tal fine, le autorità di contrasto e di gestione delle frontiere e i relativi funzionari devono provvedere affinché siano attuate misure adeguate per proteggere l'integrità e la sicurezza dei dati. In particolare, devono tenere traccia di ogni accesso ai dati e ogni utilizzo degli stessi mediante la creazione e il mantenimento di registri di tutte le attività di trattamento o di tutte le categorie di attività di trattamento (articolo 30 del GDPR e articolo 24 della direttiva di polizia). I registri devono contenere:

- il **nome** e i **dati di contatto** delle autorità e del responsabile della protezione dei dati;
- le **finalità** del trattamento;
- le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- il **ricorso alla profilazione**;
- un'indicazione della **base giuridica** del trattamento;
- ove possibile, i **termini ultimi** previsti per la cancellazione delle diverse categorie di dati personali;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del GDPR o all'articolo 29, paragrafo 1, della direttiva di polizia.

Inoltre, quando la profilazione computerizzata viene effettuata per finalità contemplate dalla direttiva di polizia (cfr. sezione 3.2), le autorità devono tenere registrazioni dei seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione dei dati.

I registri e le registrazioni sono utili ai funzionari per dimostrare di aver rispettato le prescrizioni di legge nei controlli interni ed esterni. Se una persona presenta un reclamo, ad esempio, le autorità di contrasto e di gestione delle frontiere sono tenute a provvedere affinché i registri e le registrazioni siano messi a disposizione delle autorità nazionali per la protezione dei dati.

I dati personali non dovrebbero essere conservati più a lungo di quanto necessario per conseguire la finalità legittima stabilita. La conservazione per periodi più lunghi deve essere adeguatamente motivata e quando viene attuata le autorità dovrebbero garantire un riesame periodico della conservazione al fine di garantirne l'integrità e la sicurezza.

3.1.4. Il trattamento illecito deve essere accertato e prevenuto

Accertare e prevenire il trattamento illecito dei dati personali è complesso. Poiché per comprendere algoritmi complicati e banche dati di grandi dimensioni servono competenze specialistiche, è difficile garantire controlli adeguati.

Proprio per questo motivo, il GDPR e la direttiva di polizia prevedono garanzie per guidare i funzionari delle autorità di contrasto e di gestione delle frontiere prima, durante e dopo il trattamento dei dati. Tali garanzie riguardano:

- le valutazioni d'impatto sulla protezione dei dati; e
- la protezione dei dati fin dalla progettazione e per impostazione predefinita.

Valutazioni d'impatto

Il quadro giuridico dell'UE prevede che le autorità di polizia e di gestione delle frontiere effettuino una valutazione d'impatto prima di procedere a qualsiasi trattamento di dati che possa presentare un rischio elevato per i diritti delle persone (articolo 35 del GDPR e articolo 27 della direttiva di polizia). Le valutazioni d'impatto

devono quindi essere effettuate non solo quando il risultato del trattamento può violare le norme sulla protezione dei dati o sulla privacy, ma in qualsiasi situazione che possa comportare una violazione di *qualsiasi diritto fondamentale*, tra cui: uguaglianza e non discriminazione; libertà di espressione e di informazione; libertà di pensiero, di coscienza e di religione; istruzione; assistenza sanitaria; asilo; protezione in caso di allontanamento, di espulsione e di estradizione. Le valutazioni d'impatto sono particolarmente importanti quando la profilazione può avere conseguenze giuridiche per le persone. In tali casi sono espressamente prescritte dal GDPR e dalla direttiva di polizia.

Le valutazioni d'impatto devono essere effettuate prima di procedere al trattamento automatizzato; il loro obiettivo, comunque, è duplice:

- *a priori:* prima del trattamento dei dati, l'effettuazione di una valutazione d'impatto sulla qualità dei dati e/o sull'algoritmo su cui si basa il trattamento aiuta a individuare e, se del caso, porre rimedio a potenziali violazioni dei diritti fondamentali;

- *a posteriori:* una volta che il trattamento dei dati è stato effettuato, il funzionario può essere tenuto a dimostrare di avere agito in modo lecito e la valutazione d'impatto può aiutarlo a dimostrare che sono state attuate tutte le misure necessarie per garantire il rispetto della legge.

Le valutazioni d'impatto aiutano inoltre i funzionari a individuare distorsioni occulte che possono rappresentare una violazione del diritto alla protezione dei dati e alla non discriminazione e avere un impatto sulla qualità della profilazione (cfr. sezione 1.3.2).

Sotto la lente: i rischi legati all'uso di «algoritmi dinamici»

Gli «algoritmi dinamici» sono algoritmi che vengono costantemente ridefiniti e «migliorati» sulla base di «anelli di retroazione», che sono creati dagli stessi sistemi algoritmici e non possono essere adeguatamente compresi o addirittura espressi in linguaggio semplice (cfr. articolo 35 del GDPR e articolo 27 della direttiva di polizia). A differenza degli «algoritmi statici», che si basano su criteri prestabiliti, gli «algoritmi dinamici» generano **nuove correlazioni** ridefinendosi costantemente.

Con gli algoritmi dinamici esiste il rischio che programmatori esperti a un certo punto non sappiano più qual è la logica alla base dell'algoritmo. Si crea così un **rischio** significativo di **riprodurre involontariamente pregiudizi esistenti** e di perpetuare disuguaglianze sociali e la stigmatizzazione di alcuni gruppi. In questi casi, diventa molto difficile garantire la rendicontabilità e la riparazione alle persone interessate.

L'uso di «algoritmi dinamici» dovrebbe quindi essere **evitato o ridotto** per ridurre al minimo il rischio di perdere il controllo dei criteri di valutazione. Ciò consente ai revisori interni ed esterni di valutare gli algoritmi e di modificarli, qualora risultino illeciti. Se l'uso di algoritmi dinamici è giustificato, gli indicatori di rischio devono essere riesaminati e verificati per garantire che non comportino una profilazione illecita.

Per ulteriori informazioni, cfr. Gandy, O. (2010) e Korff, D. (2015).

Una valutazione d'impatto può variare notevolmente a seconda del tipo e del volume dei dati personali trattati, nonché del tipo e della finalità del trattamento. Può comprendere il controllo della qualità dei dati, controlli tecnici dell'algoritmo o degli algoritmi di trattamento dei dati e/o un riesame completo degli obiettivi del trattamento ecc. La figura 13 indica i criteri minimi che dovrebbero essere valutati.

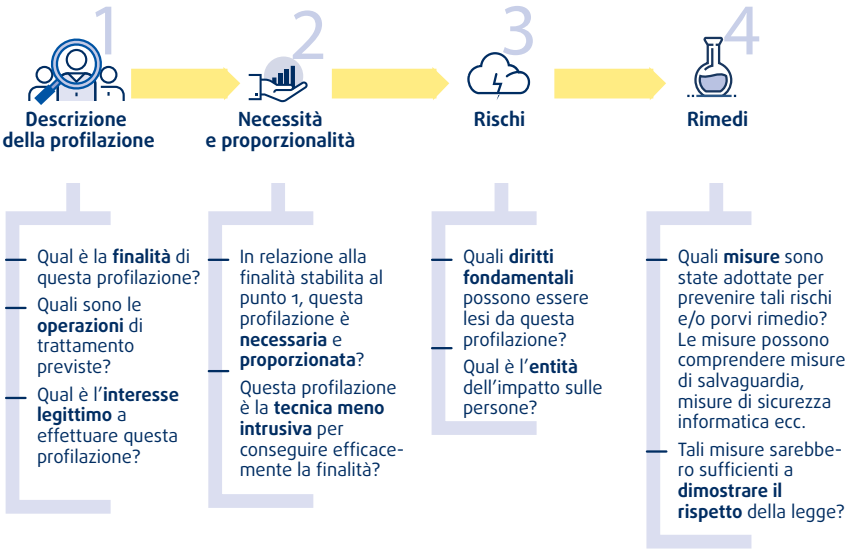
Il gruppo di lavoro articolo 29 per la protezione dei dati (ora sostituito dal comitato europeo per la protezione dei dati), che riunisce le autorità nazionali per la protezione dei dati negli Stati membri dell'UE, ha elaborato linee guida che forniscono ulteriori informazioni in merito alle valutazioni d'impatto sulla protezione dei dati. Le linee guida comprendono una panoramica dettagliata dei criteri da utilizzare per effettuare le valutazioni d'impatto ([40]).

Prevedere la liceità del trattamento «fin dalla progettazione» e «per impostazione predefinita»

Indipendentemente dal fatto che una valutazione d'impatto abbia o meno individuato la possibilità di una violazione dei diritti fondamentali, possono essere adottate misure per prevenire ulteriormente ogni rischio di illiceità. Tali misure sono la

([40]) Gruppo di lavoro articolo 29 (2017a).

Figura 13: Requisiti minimi delle valutazioni d'impatto



Fonte: *FRA (2018)*

«protezione dei dati fin dalla progettazione» e la «protezione dei dati per impostazione predefinita» (articolo 25 del GDPR e articolo 20 della direttiva di polizia).

La protezione dei dati fin dalla progettazione mira a garantire che, *prima* e *durante* il trattamento dei dati, siano attuate misure tecniche e organizzative per garantire i principi di protezione dei dati. Ad esempio, i dati personali potrebbero essere «pseudonimizzati», se possibile. La pseudonimizzazione è una misura mediante la quale i dati personali non possono essere ricondotti alla persona a cui si riferiscono se non con informazioni aggiuntive, che sono conservate separatamente. La «chiave» che consente la re-identificazione della persona deve essere conservata separatamente e al sicuro ([41]). Contrariamente ai dati anonimizzati, i dati pseudonimizzati rimangono dati personali e devono quindi rispettare le norme e i principi in materia di protezione dei dati.

([41]) FRA, GEPD e Consiglio d'Europa (2018), pag. 83.

La protezione dei dati per impostazione predefinita garantisce che «siano trattati [...] solo i dati personali necessari per ogni specifica finalità del trattamento» ([42]). Ciò ha un impatto su:

- la quantità di dati personali raccolti e conservati;
- i tipi di trattamento che possono riguardare dati personali;
- il periodo massimo di conservazione;
- il numero di persone autorizzate ad accedere a tali dati personali.

Sotto la lente: rendicontabilità

L'obiettivo principale della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita è sostenere le autorità di contrasto e di gestione delle frontiere e il relativo personale nella progettazione di programmi di profilazione algoritmica che rispettino i requisiti in materia di diritti fondamentali, in particolare i principi di **liceità**, **trasparenza** e **sicurezza**.

Misure di questo genere, tuttavia, possono anche dimostrare in che modo le autorità rispettano il requisito giuridico della **rendicontabilità**. Le autorità che effettuano il trattamento di dati sono giuridicamente tenute a mettere in atto «misure tecniche e organizzative adeguate» per dimostrare la loro conformità al diritto dell'UE. Ad esempio, se una persona presenta un reclamo, le autorità nazionali giudiziarie e di protezione dei dati possono chiedere alle autorità di dimostrare ciascuno di questi punti:

- la legittimità, necessità e proporzionalità della profilazione computerizzata;
- la liceità della finalità;
- le informazioni fornite alle persone;
- l'integrità e la sicurezza dei dati;
- le misure di qualità e i controlli effettuati prima e durante le operazioni di profilazione.

([42]) Regolamento generale sulla protezione dei dati, articolo 25.

3.2. Banche dati su larga scala per la gestione delle frontiere e la sicurezza

L'UE ha sviluppato diversi sistemi informatici su larga scala o meccanismi per la raccolta e il trattamento dei dati che possono essere utilizzati per la gestione delle frontiere e della migrazione e, in una certa misura, a fini di contrasto. Tali sistemi o meccanismi fungono da esempi per illustrare alcune delle sfide comuni legate all'uso della profilazione algoritmica, nonché le possibili garanzie.

La tabella 6 presenta sinteticamente questi sistemi informatici e meccanismi dell'UE. L'allegato presenta una panoramica dettagliata dei sistemi informatici su larga scala esistenti e in programma nell'UE, al marzo 2018.

I sistemi informatici su larga scala dell'UE sono utilizzati in varie procedure legate alla migrazione, tra cui la procedura di valutazione dei rischi prima dell'arrivo, la procedura di asilo, la procedura per la domanda di visto, durante le verifiche di frontiera, per il rilascio del permesso di soggiorno, quando vengono fermati migranti in situazione irregolare, durante le procedure di rimpatrio e per il rilascio dei divieti d'ingresso. I sistemi informatici istituiti dall'UE, compresi quelli creati inizialmente per la gestione dell'asilo e della migrazione, sono utilizzati sempre più spesso anche nel contesto della sicurezza interna, ad esempio per i controlli di polizia e la lotta contro i reati gravi e il terrorismo.

La maggior parte dei sistemi istituiti dal diritto dell'UE mira a consentire l'identificazione di una persona specifica confrontando dati alfanumerici o biometrici (attualmente impronte digitali) con informazioni già presenti nel sistema. Salvo qualche eccezione significativa (cfr. «Sotto la lente: profilazione algoritmica negli strumenti dell'UE»), tali sistemi non contengono essi stessi un algoritmo che consenta di confrontare una persona a un profilo; possono tuttavia essere utilizzati per produrre statistiche anonimizzate, anche per caratteristiche che sono considerate motivi protetti quali il sesso o l'età (cfr. sezione 1.2.1).

Tali statistiche potrebbero essere impiegate per definire profili di rischio utilizzati nelle future decisioni in materia di gestione delle frontiere o di attività di polizia. Nell'ambito del più ampio sistema per l'interoperabilità dei sistemi informatici dell'UE, l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) sarà responsabile della gestione dell'archivio centrale di relazioni e statistiche. Tale archivio si baserà

Tabella 6: Alcuni strumenti UE che prevedono il trattamento di grandi quantità di dati per la gestione delle frontiere e l'attività di contrasto

Banca dati	Sigla	Finalità principale
Sistema d'informazione Schengen	*SIS II*	Inserimento e trattamento di segnalazioni delle persone ricercate o scomparse al fine di salvaguardare la sicurezza, inserimento e trattamento di segnalazioni su cittadini di paesi terzi ai fini del rifiuto dell'ingresso o soggiorno, inserimento e trattamento di segnalazioni su cittadini di paesi terzi oggetto di una decisione di rimpatrio.
Sistema di informazione visti	*VIS*	Agevolazione dello scambio di dati sulle domande di visto tra Stati membri Schengen.
Sistema europeo di dattiloscopia	*Eurodac*	Determinazione dello Stato membro competente per l'esame della domanda di protezione internazionale e assistenza nel controllo dell'immigrazione irregolare e dei movimenti secondari.
Sistema di ingressi/uscite	*EES*	Calcolo e monitoraggio della durata del soggiorno autorizzato dei cittadini di paesi terzi e identificazione dei soggiornanti fuoritermine.
Codice di prenotazione	*PNR*	Raccolta, trattamento e scambio di dati dei passeggeri dei voli provenienti da paesi terzi («voli extra-UE») (*). In senso stretto, utilizzato unicamente per finalità di contrasto.
Informazioni anticipate sui passeggeri	*API*	Raccolta e trattamento dei dati dei passeggeri dei voli provenienti da paesi terzi («voli extra-UE») per finalità di gestione delle frontiere e contrasto.
Sistema europeo di informazione e autorizzazione ai viaggi	*ETIAS*	Valutazione volta ad accertare se un cittadino di paese terzo esente dall'obbligo di visto rappresenti un rischio in termini di sicurezza, migrazione irregolare o salute pubblica.
Sistema europeo di informazione sui casellari giudiziali a carico di cittadini di paesi terzi e apolidi	*ECRIS-TCN*	Condivisione di informazioni sulle condanne precedenti di cittadini di paesi terzi.

(*) *Inoltre, l'articolo 2 della direttiva (UE) 2016/681 conferisce agli Stati membri la facoltà di trattare i dati dei voli intra-UE.*

Fonte: *FRA (2018)*

sui dati provenienti dalle banche dati esistenti dell'UE (sistema di ingressi/uscite, ETIAS, sistema d'informazione Schengen e sistema di informazione visti) per generare statistiche e relazioni analitiche per gli organismi dell'UE e nazionali ([43]).

Sotto la lente: profilazione algoritmica negli strumenti dell'UE

Alcuni degli attuali strumenti dell'UE prevedono l'uso di statistiche basate sui propri dati per generare profili di rischio. Oltre a consentire l'identificazione di specifici sospetti «noti», essi contengono una funzione di profilazione algoritmica che permette di identificare persone «non note» che potrebbero rivestire interesse per le autorità di contrasto e di gestione delle frontiere.

Il **sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)** ([44]), adottato nel settembre 2018 ma non ancora operativo al momento della stesura della presente guida, valuterà se i cittadini di paesi terzi esenti dall'obbligo di visto presentino un rischio in termini di migrazione irregolare, sicurezza o salute pubblica prima di concedere l'autorizzazione ai viaggi. Le informazioni fornite dai viaggiatori durante il processo di presentazione della domanda saranno automaticamente confrontate con le pertinenti banche dati dell'UE e internazionali e con una serie di indicatori di rischio («regole di esame») contenuti nel sistema ETIAS stesso. Un algoritmo sviluppato da Frontex metterà a confronto il profilo individuale del viaggiatore (basato su indicatori quali l'età, il sesso, la nazionalità, il luogo di residenza, il livello di istruzione e l'occupazione) con tali indicatori di rischio per stabilire se la domanda debba essere oggetto di trattamento manuale.

I **dati del codice di prenotazione (PNR)** sono raccolti dai vettori aerei in base alle informazioni fornite dai passeggeri nei sistemi di prenotazione dei voli,

([43]) Commissione europea (2017), Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (frontiere e visti) e che modifica la decisione 2004/512/CE del Consiglio, il regolamento (CE) n. 767/2008, la decisione 2008/633/GAI del Consiglio, il regolamento (UE) 2016/399 e il regolamento (UE) 2017/2226, COM(2017) 793 final del 12 dicembre 2017; Commissione europea (2017), Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (cooperazione giudiziaria e di polizia, asilo e migrazione), COM(2017) 794 final del 12 dicembre 2017.

([44]) Commissione europea (2018), 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, COM(2016) 731 final del 16 novembre 2016, articolo 33, paragrafo 5.

quali le date e l'itinerario del viaggio, le coordinate di contatto e informazioni sui pagamenti, informazioni relative al bagaglio e altre «osservazioni generali», quali le preferenze alimentari. Non esiste una banca dati centrale dell'UE che raccolga tali dati, ma la direttiva PNR dell'UE ([45]) prevede che i vettori aerei debbano fornire i dati alle unità nazionali d'informazione sui passeggeri (UIP), che successivamente analizzano le informazioni ai fini della lotta contro il terrorismo e i reati gravi. Oltre che per individuare i movimenti transfrontalieri di persone note, questi dati possono essere utilizzati per identificare minacce ancora non note trattando i dati dei passeggeri sulla base di indicatori di rischio specifici («criteri prestabiliti»). Tali criteri sono stabiliti dalle UIP e aggiornati sulla base dei nuovi dati e modelli disponibili nel sistema.

3.2.1. Ridurre al minimo i rischi per i diritti fondamentali derivanti dal trattamento dei dati nelle banche dati su larga scala

Dati completi sui viaggiatori quali la nazionalità, il sesso e l'età saranno utilizzati per la profilazione, compresa la profilazione algoritmica, su una scala che in passato non era possibile. Anche se tali dati sono anonimizzati, il loro trattamento non è privo di rischi. Preconcetti e distorsioni consapevoli o inconsapevoli nella selezione degli indicatori di rischio, nella progettazione degli algoritmi o nell'interpretazione dei risultati potrebbero condurre a interventi operativi che potrebbero comportare la discriminazione di determinate categorie di persone ([46]).

La presente sezione esamina alcuni di questi rischi e propone alcuni modi per ridurli al minimo. Si basa sulle dodici considerazioni operative della FRA relative ai diritti fondamentali per le autorità di contrasto quando effettuano il trattamento dei dati PNR (cfr. caso di studio). Tali considerazioni sono state elaborate nel contesto specifico del trattamento dei dati PNR; alcune di esse hanno tuttavia un'applicabilità più generale e possono essere considerate come garanzie volte ad attenuare i rischi derivanti dalla profilazione algoritmica.

([45]) 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 (GU L 119 del 4.5.2016, pag. 132), articolo 6, paragrafo 4.

([46]) Per ulteriori informazioni, cfr. FRA (2017e) e FRA (2018a).

Caso di studio

Orientamenti operativi della FRA per l'istituzione di sistemi PNR nazionali

Nel 2014, in assenza di norme legislative dell'UE in materia di PNR, la Commissione europea ha chiesto alla FRA di fornire indicazioni pratiche sul trattamento dei dati PNR per finalità di contrasto a beneficio degli Stati membri che intendessero istituire un proprio sistema PNR nazionale. Le indicazioni formulate vertevano sul rispetto della vita privata (articolo 7 della Carta), sulla protezione dei dati personali (articolo 8 della Carta) e sulla non discriminazione (articolo 21 della Carta). Alcune delle garanzie proposte sono state successivamente introdotte nella direttiva PNR dell'UE.

Le dodici considerazioni relative ai diritti fondamentali di cui tenere conto nelle attività di contrasto quando si effettua il trattamento di dati PNR sono le seguenti:

- utilizzare i dati PNR solo per combattere il terrorismo e i reati gravi di natura transnazionale;
- limitare l'accesso alla banca dati PNR a un'unità specializzata;
- non chiedere l'accesso alle banche dati delle compagnie aeree;
- cancellare i dati PNR sensibili;
- istituire garanzie rigorose in materia di sicurezza e rintracciabilità contro gli abusi;
- ridurre la probabilità di segnalazioni di falsi positivi;
- essere trasparenti nei confronti dei passeggeri;
- consentire alle persone di accedere ai propri dati PNR e rettificarli;
- non consentire l'identificazione degli interessati o la conservazione dei dati per un periodo più lungo del necessario;
- trasferire i dati estratti dai PNR solo alle autorità pubbliche nazionali competenti;
- subordinare a condizioni rigorose il trasferimento a paesi terzi dei dati estratti dal PNR;
- effettuare una valutazione obiettiva e trasparente del sistema PNR.

Per ulteriori informazioni, cfr. FRA (2014c).

Il trattamento di dati che rivelano caratteristiche protette deve essere necessario e proporzionato

Per effetto della natura stessa della profilazione algoritmica, l'uso delle caratteristiche personali che sono legate a motivi protetti comporta un rischio particolarmente elevato di discriminazione ([47]). Nel contesto dell'UE, sia la legislazione ETIAS che quella PNR vietano di basare gli indicatori di rischio su criteri che comportano un rischio elevato di discriminazione, tra cui la razza, l'origine etnica o le convinzioni religiose. Tuttavia, anche in assenza di tali dati, altri tipi di dati possono essere strettamente correlati a tali caratteristiche e costituire a tutti gli effetti indicatori surrogati di caratteristiche protette. Ad esempio, la categoria «osservazioni generali» del PNR, che potrebbe contenere le preferenze alimentari dei viaggiatori, può rivelare determinate convinzioni religiose.

Anche combinazioni specifiche di dati utilizzate dall'algoritmo possono porre una determinata categoria di persone in posizione di svantaggio: ad esempio, possono recare pregiudizio a particolari persone a causa della loro origine etnica o sociale o dell'appartenenza a una minoranza nazionale, che sono caratteristiche protette ai sensi dell'articolo 21 della Carta. Ad esempio, un profilo di rischio nell'ETIAS relativo al rischio di migrazione irregolare e basato sulla combinazione di una determinata nazionalità e un determinato gruppo professionale può indurre a concentrare l'attenzione su un gruppo etnico o una nazionalità che in un determinato paese tipicamente lavora in un particolare settore economico, come quello edile o agricolo ([48]).

- Il trattamento di dati che rivelano caratteristiche protette dall'articolo 21 della Carta dovrebbe essere proporzionato e limitato a quanto strettamente necessario e non dovrebbe mai tradursi in una discriminazione. Prima di effettuare qualsiasi trattamento, l'autorità competente dovrebbe valutare i dati per identificare eventuali caratteristiche protette ed eliminare qualsiasi dato il cui trattamento non sia lecito. Sarebbe buona regola inoltre utilizzare un programma di ricerca ed eliminazione con un glossario di «termini sensibili» regolarmente aggiornato.

([47]) Garante europeo della protezione dei dati (2018).

([48]) Cfr. anche FRA (2017a).

I criteri di profilazione dovrebbero essere specifici e mirati

Un altro fattore di rischio deriva dall'uso di **criteri di profilazione generali**. Gli attuali strumenti dell'UE consentono un notevole margine di discrezionalità nello sviluppo degli algoritmi di profilazione. Per valutare il rischio di migrazione irregolare, l'ETIAS prevede l'uso di statistiche nazionali e dell'UE sul tasso di soggiorni fuoritermine e respingimenti. Per i rischi per la sicurezza, tuttavia, l'ETIAS fa riferimento solo in maniera generale a informazioni riguardanti indicatori di sicurezza specifici e minacce per la sicurezza. La direttiva PNR offre indicazioni generali per la progettazione di algoritmi, ma non specifica quali criteri utilizzare per identificare le persone potenzialmente coinvolte in reati di terrorismo o in reati gravi, o quale peso attribuire a un criterio specifico.

Criteri eccessivamente generali portano a un numero significativo di «falsi positivi», il che significa che molte persone sono erroneamente associate a un determinato profilo di rischio. Alcuni di questi «falsi positivi» possono essere anche discriminatori. Ad esempio, con una definizione ampia del criterio «precedenti condanne penali», le persone LGBT sarebbero tenute a segnalare precedenti penali associati a determinati comportamenti sessuali qualificati come reato da alcuni paesi terzi.

- I criteri di valutazione dovrebbero essere predefiniti, mirati, specifici, proporzionati e basati sui fatti. Inoltre dovrebbero essere verificati su campioni anonimizzati. Dovrebbero anche essere sottoposti periodicamente a revisione da parte di un revisore interno per stabilire se siano ancora giustificati dai loro obiettivi specifici.

- Prima di trasmettere una segnalazione basata su un trattamento automatizzato per ulteriori azioni, l'autorità competente dovrebbe riesaminare manualmente i dati insieme ad altre informazioni per determinare se la persona corrisponda al profilo di rischio ed eliminare i falsi positivi. I destinatari dei dati dovrebbero fornire un feedback sul seguito dato alla segnalazione.

I dati trattati devono essere esatti e affidabili

La ricerca della FRA conferma che i sistemi informatici su larga scala esistenti contengono una quantità significativa di dati inesatti ([49]). I **dati inesatti o inattendibili** possono avere molteplici effetti negativi nel contesto della profilazione algoritmica per la gestione delle frontiere o per attività di contrasto. I dati inesatti possono incidere negativamente sulle persone, ma anche indurre a correlazioni errate e un quadro distorto, compromettendo l'efficacia del lavoro di polizia e di gestione delle frontiere.

Ciò è particolarmente importante nel caso di dati inseriti dai cittadini, come nel caso dei dati PNR e delle domande ETIAS, che possono essere più soggetti a errori rispetto ai dati ufficiali. Analogamente, l'esame degli account sui social media, previsto da alcuni sistemi di autorizzazione ai viaggi al di fuori dell'UE, comporta un rischio elevato di introdurre informazioni inattendibili nel processo di profilazione e il rischio specifico di raccogliere dati che rivelino informazioni personali sensibili protette dalla Carta, quali le opinioni politiche o informazioni relative alla vita sessuale.

- Fornire alle persone informazioni accurate sulla raccolta, la conservazione e il trattamento dei loro dati e sui principi di protezione dei dati applicabili. Le persone dovrebbero essere informate dei loro diritti, compresi i meccanismi di ricorso a loro disposizione.

- Consentire alle persone di rettificare i propri dati nei casi in cui i dati sono inesatti e di sapere se i dati sono stati rettificati o cancellati.

- Prevedere un ricorso effettivo in sede amministrativa e giudiziaria nei casi in cui il diritto alla protezione dei dati sia stato violato, compresi i casi in cui l'accesso sia stato negato o i dati inesatti non siano stati rettificati o cancellati.

([49]) Cfr. FRA (2018c), pagg. 81-98.

Conclusione

La profilazione è uno strumento legittimo utilizzato dai funzionari delle autorità di contrasto e dalle guardie di frontiera a fini di prevenzione, indagine e perseguimento di reati, nonché di prevenzione e accertamento dell'immigrazione irregolare.

Per essere lecita, equa ed efficace, la profilazione deve essere utilizzata entro i confini della legge. In particolare, deve rispettare i requisiti in materia di parità di trattamento e protezione dei dati personali.

Tale obiettivo può essere conseguito combinando tra loro diversi elementi. Qualsiasi profilazione dovrebbe:

- trattare le persone in modo equo e rispettoso, salvaguardando la loro dignità;
- evitare di profilare le persone sulla base di preconcetti;
- essere ragionevole, oggettiva e basata su informazioni di intelligence; e
- proteggere adeguatamente i dati personali e la vita privata delle persone.

I funzionari di polizia e le guardie di frontiera dispongono di diversi strumenti per garantire che tali principi siano conosciuti, compresi e rispettati nella pratica:

- prima di effettuare la profilazione, i funzionari dovrebbero ricevere orientamento e formazione;
- durante la profilazione, i dettagli dell'attività dovrebbero essere verbalizzati e registrati;
- dopo la profilazione, le azioni dei funzionari dovrebbero essere monitorate e valutate per individuare le aree di miglioramento.

La prevenzione della profilazione illecita non solo permette ai funzionari delle autorità di contrasto e alle guardie di frontiera di mantenersi entro i confini della legge, ma assicura anche che le loro azioni siano comprese e accettate dalla popolazione. Il rafforzamento della fiducia nelle attività di contrasto e di gestione delle frontiere migliora l'efficacia delle attività di polizia e gestione delle frontiere e contribuisce pertanto a migliorare la sicurezza e la protezione della società nel suo complesso.

Allegato

Tabella 7: Sistemi IT su larga scala esistenti e previsti nell'UE

Sistema IT	Scopo principale	Persone interessate	Applicabilità	Strumento giuridico/proposta	Identificatori biometrici
Sistema europeo per il confronto delle impronte digitali (Eurodac)	Determinare lo Stato membro competente per l'esame di una domanda di protezione internazionale *Agevolare il controllo dell'immigrazione irregolare e dei movimenti secondari*	Richiedenti e beneficiari di protezione internazionale, *migranti in situazione irregolare*	28 SM UE + PAS	Regolamento (UE) n. 603/2013 (regolamento Eurodac) *COM(2016) 272 final (proposta Eurodac)*	
Sistema d'informazione visti (VIS)	Agevolare lo scambio di dati tra Stati membri Schengen sulle domande di visto	Persone che richiedono un visto e garanti	24 SM UE (non CY, HR, IE, UK) (1) + PAS	Regolamento n. 767/2008/CE (regolamento VIS)	
Sistema d'informazione Schengen (SIS II) — Polizia	Garantire la sicurezza nell'UE e negli Stati membri Schengen	Persone scomparse o ricercate	26 SM UE (non CY, IE) (2) + PAS	Decisione 2007/533/GAI del Consiglio (decisione SIS II) *COM(2016) 883 final (proposta SIS II — Polizia)*	
Sistema d'informazione Schengen (SIS II) — Frontiere	Inserire e trattare segnalazioni ai fini del rifiuto di ingresso o di soggiorno negli Stati membri Schengen	Migranti in situazione irregolare	25 SM UE (non CY, IE, UK) (2) + PAS	Regolamento (CE) n. 1987/2006(regolamento SIS II) *COM(2016) 882 final (proposta SIS II — Frontiere)*	
Sistema d'informazione Schengen (SIS II) — Rimpatrio	*Inserire e trattare le segnalazioni per cittadini di paesi terzi oggetto di una decisione di rimpatrio*	*Migranti in situazione irregolare*	*25 SM UE (non CY, IE, UK) (2) + PAS*	*COM(2016) 881 final (proposta SIS II — Rimpatrio)*	
Sistema di ingressi/uscite (EES)	*Calcolare e monitorare la durata del soggiorno autorizzato dei cittadini di paesi terzi e individuare i soggiornanti fuoritermine*	*Viaggiatori che arrivano per un soggiorno di breve durata*	*22 SM UE (non BG, CY, HR, IE, RO, UK) (3) + PAS*	*Regolamento (UE) 2017/2226 (regolamento EES)*	

Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)	*Valutare se un cittadino di un paese terzo esente dall'obbligo di visto rappresenti un rischio in termini di sicurezza, migrazione irregolare o salute pubblica*	*Viaggiatori esenti dall'obbligo di visto*	*26 SM UE (non IE, UK) ([3]) + PAS*	*COM(2016) 731 final (proposta ETIAS)*	*Nessuno*
Sistema europeo di informazione sui casellari giudiziali per i cittadini di paesi terzi (ECRIS-TCN)	*Condividere informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi*	*Cittadini di paesi terzi con precedenti penali*	*27 SM UE (non DK) ([4])*	*COM(2017) 344 final (proposta ECRIS-TCN)*	
Interoperabilità — Archivio comune di dati di identità	*Istituire un quadro per l'interoperabilità tra i sistemi EES, VIS, ETIAS, Eurodac, SIS II ed ECRIS-TCN*	*Cittadini di paesi terzi cui si applicano i sistemi Eurodac, VIS, SIS II, EES, ETIAS ed ECRIS-TCN*	*28 SM UE ([5]) + PAS*	*COM(2017) 793 final (proposta interoperabilità — Frontiere e visti)* *COM(2017) 794 final (proposta interoperabilità — Cooperazione di polizia, asilo e migrazione)*	

Nota: i sistemi previsti e le modifiche previste dei sistemi sono in corsivo.

 *impronte digitali;*  *impronte palmari;*  *immagine del volto;*  *profilo del DNA.*

SM UE: Stati membri dell'UE; PAS: paesi associati Schengen, ossia Islanda, Liechtenstein, Norvegia e Svizzera.

([1]) L'Irlanda e il Regno Unito non partecipano al VIS. La Danimarca non è vincolata dal regolamento, ma ha deciso di partecipare al VIS. Il VIS non si applica ancora alla Croazia e a Cipro e si applica solo in parte alla Bulgaria e alla Romania conformemente alla decisione (UE) 2017/1908 del Consiglio del 12 ottobre 2017.

([2]) Cipro e l'Irlanda non sono ancora collegati al SIS. La Danimarca non è vincolata dal regolamento o dalla decisione del Consiglio, ma ha deciso di partecipare al SIS II e dovrà decidere nuovamente se parteciparvi una volta che saranno state adottate le proposte sul SIS II. Il Regno Unito partecipa al SIS ma non può utilizzare o accedere a segnalazioni per rifiutare l'ingresso o il soggiorno nello spazio Schengen. La Bulgaria, la Romania e la Croazia non possono emettere segnalazioni Schengen per rifiutare l'ingresso o il soggiorno nello spazio Schengen, in quanto non fanno ancora parte dello spazio Schengen.

([3]) La Danimarca potrebbe decidere di partecipare all'EES e all'ETIAS.

([4]) L'ECRIS-TCN non si applica alla Danimarca. Il Regno Unito e l'Irlanda possono decidere di aderirvi.

([5]) La Danimarca, l'Irlanda e il Regno Unito aderiranno in quanto partecipano ai sistemi IT resi interoperabili.

Fonte: FRA, sulla base di strumenti giuridici esistenti e proposti, 2018

Riferimenti bibliografici

Agenzia europea della guardia di frontiera e costiera (2012), *Common core curriculum, EU border guard basic training*, marzo 2012.

Agenzia europea della guardia di frontiera e costiera (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Agenzia europea della guardia di frontiera e costiera (2015), *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Agenzia europea della guardia di frontiera e costiera (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Akhgar, B., Saathoff, G.B., Arabnia, H.R., Hill, R., Staniforth, A. e Bayerl, P.S. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016), *Eight Problems With Police «Threat Scores»,* 13 gennaio 2016.

Belgio, UNIA, *Annual Report 2016*, Bruxelles, settembre 2017.

Belgio, UNIA, *Rapport annuel Convention entre Unia e la police fédérale, Budget 2015*, Bruxelles, 2015.

Big Brother Watch, *Smile you're on body worn camera Part II — Police, The use of body worn cameras by UK police forces,* agosto 2017.

Body-Gendrot, S. (2016), «Making sense of French urban disorders in 2005», *European Journal of Criminology*, vol. 13, n. 5, pagg. 556-572.

Bovens e al. (2014), «Public accountability» in Bovens, M., Schillermans, T. e Goodlin, R.E. (a cura di), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), «Surveillance and system avoidance: criminal justice contact and institutional attachment», *American Sociological Review*, vol. 79, n. 3, pagg. 367-391.

Buolamwini, J., Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab and Microsoft Research, 2018.

Center on Privacy and Technology at Georgetown Law (2016), *The Perpetual Line-up, Unregulated Police Face Recognition in America*, 18 ottobre 2016.

Centre d'analyse stratégique (2006), *Enquête sur les violences urbaines — Comprendre les émeutes de novembre 2005: les exemples de Saint-Denis e d'Aulnay-Sous-Bois*, Parigi, La Documentation française, 2006.

Commissione europea (2017a), *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, febbraio 2017.

Commissione europea (2017b), *Improving the recording of hate crime by law enforcement authorities — Key guiding principles*, dicembre 2017.

Commissione europea contro il razzismo e l'intolleranza (ECRI) (2007), *ECRI General Policy Recommendation N°11 on combating racism and racial discrimination in policing* adottata il 29 giugno 2007, Strasburgo, 4 ottobre 2007.

Consiglio d'Europa, Comitato dei ministri (2001), Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics adopted by the Committee of Ministers, 19 settembre 2001.

Consiglio dell'Unione europea (2009), *Catalogo Schengen UE aggiornato sui controlli alle frontiere esterne, il rimpatrio e la riammissione*, 19 marzo 2009.

Coudert, F., Butin, D. e Le Metayer, D. (2015), «Body-worn cameras for police accountability: opportunities and risks», *Computer Law and Security Review*, vol. 31, pagg. 749-762.

De Hert, P. e Lammerant, H. (2016), «Predictive profiling and its legal limits: effectiveness gone forever?» in van der Sloot, B., Broeders, D. e Schrijvers, E. (a cura di), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, pagg. 145-173.

Défenseur des droits (2017), *Enquête sur l'accès aux droits. Volume 1 — relations police/population: le case des contrôles d'identité*, 2017.

Dinant, J.-M., Lazaro, C., Poullet Y., Lefever, N. e Rouvroy, A. (2008), *Application of Convention 108 to the Profiling Mechanism — Some ideas for the future work of the consultative committee (T-PD)*, doc. T-PD 01, pag. 3.

Farrar, T. (2018), *Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force*, Police Foundation, 2018.

FRA (Agenzia dell'Unione europea per i diritti fondamentali) (2013), *Formazione del personale di polizia basata sui diritti fondamentali — Manuale per formatori di personale di polizia*, Lussemburgo, Ufficio delle pubblicazioni, dicembre 2013.

FRA (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Lussemburgo, Ufficio delle pubblicazioni, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Lussemburgo, Ufficio delle pubblicazioni, 2014.

FRA (2014c), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, febbraio 2014.

FRA (2016), *Fundamental Rights Report 2016*, Lussemburgo, Ufficio delle pubblicazioni, 2016.

FRA (2017a), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, parere FRA — 2/2017 [ETIAS], giugno 2017.

FRA (2017b), *Second European Union Minorities and Discrimination Survey — Main results*, Lussemburgo, Ufficio delle pubblicazioni, dicembre 2017.

FRA (2017c), *Fundamental Rights Report 2017*, Lussemburgo, Ufficio delle pubblicazioni, maggio 2017.

FRA (2017d), *Seconda indagine su minoranze e discriminazioni nell'Unione europea — Musulmani: una selezione di risultati*, Lussemburgo: Ufficio delle pubblicazioni, 2017.

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Lussemburgo, Ufficio delle pubblicazioni, maggio 2017.

FRA (2018a), *Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, parere FRA — 1/2018 [interoperabilità], aprile 2018.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, documento tematico FRA, maggio 2018.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Lussemburgo, Ufficio delle pubblicazioni, febbraio 2018.

FRA (2018d), *Hate crime recording and data collection practice across the EU*, Lussemburgo, Ufficio delle pubblicazioni, giugno 2018.

FRA (2018e), *Fundamental Rights Report 2018*, Lussemburgo, Ufficio delle pubblicazioni, giugno 2018.

FRA e Consiglio d'Europa (2018), *Handbook on European non-discrimination law — 2018 edition*, Lussemburgo, Ufficio delle pubblicazioni, febbraio 2018.

FRA (Agenzia dell'Unione europea per i diritti fondamentali), Garante europeo della protezione dei dati (GEPD) e Consiglio d'Europa (2018), *Manuale sul diritto europeo in materia di protezione dei dati — edizione 2018*, Lussemburgo, Ufficio delle pubblicazioni, maggio 2018.

Francia, ministero dell'Interno (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 giugno 2018.

Garante europeo della protezione dei dati (GEPD) (2015), *Opinion 5/2015 — Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Bruxelles, 24 settembre 2015.

Garante europeo della protezione dei dati (GEPD) (2018), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Bruxelles, 18 aprile 2018.

Gruppo di lavoro articolo 29 per la protezione dei dati (2014), *Parere 01/2014 sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto*, 536/14/IT, WP 211, Bruxelles, 27 febbraio 2014.

Gruppo di lavoro articolo 29 per la protezione dei dati (2017a), *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, 4 ottobre 2017.

Gruppo di lavoro articolo 29 per la protezione dei dati (2017b), *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, 7 dicembre 2017.

Gruppo di lavoro articolo 29 per la protezione dei dati (2018a), *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, WP251rev.01, 6 febbraio 2018.

Gruppo di lavoro articolo 29 per la protezione dei dati (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Bruxelles, 23 aprile 2018.

Harcourt, B. (2004), «Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally», *University of Chicago Law Review*, vol. 71, 2004.

Harris, D. (2002), «Flying While Arab: Lessons from the Racial Profiling Controversy», *Civil Rights Journal*, vol. 6, n. 1, inverno 2002.

Harris, D. (2003), *Profiles in Injustice; Why Racial Profiling Cannot Work*, The New Press, 2003.

Hildebrandt, M. e de Vries, K. (2013), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, New York, Routledge, 2013.

Hildebrandt, M. e Gutwirth, S. (a cura di) (2008), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlin, Springer, 2008.

Hörnqvist, M. (2016), «Riots in the welfare state: The contours of a modern-day moral economy», *European Journal of Criminology*, vol. 13, n. 5, pagg. 573–589.

Hunt, P., Saunders, J. e Hollywood, J.S. (2014), *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.

Gandy, O. (2010), «Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems», *J Ethics Inf Technol*, vol. 12, n. 1, 2010, pagg. 29-42.

Gross, S.R. (2002), «Racial Profiling under Attack», D. Livingston, co-autore. *Colum. L.* rev. 102, n. 5, pagg. 1413-1438.

Jobard, F. (2008), «The 2005 French urban unrests: data-based interpretations», *Sociology Compass*, vol. 2, n. 4, pagg. 1287-1302.

Kádár, A., Körner, J., Moldova, Z. e Tóth, B. (2008), *Control(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS) Project*, Budapest, pag. 23.

Keskinen, S. e al. (2018), *The Stopped — Ethnic Profiling in Finland*, Swedish School of Social Science, University of Helsinki, Helsinki, 3 aprile 2018.

Korff, D. (2015), *Passenger Name Records, data mining & data protection: the need for strong safeguards*, T-PD(2015)11, Strasburgo, 15 giugno 2015.

Miller, J. e Alexandrou, B. (2016), *College of policing stop and search training experiment: Impact evaluation*, College of Policing Limited, 2016.

Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. e Floridi, L. (2016), «The ethics of algorithms: Mapping the debate», *Big Data & Society*, 1º dicembre 2016.

Mohler, G.O., Short, M.B., Malinowski, S., Johnson, M., Tita, G.E., Bertozzi, A.L. e Brantingham, P.J. (2016), *Randomized Controlled Field Trials of Predictive Policing*, 15 gennaio 2016.

Nazioni Unite (ONU) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29 gennaio 2007.

Nisbet, R., Elder, J. e Miner, G. (2009), *Handbook of Statistical Analysis & Data Mining Applications*, Sydney (Canada), Elsevier, 2009.

Open Society Justice Initiative (2018a), *Regulating Police Stop and Search: An Evaluation of the Reasonable Grounds Panel*, dicembre 2018.

Open Society Justice Initiative (2018b), *The Recording of Police Stops: Methods and Issues*, dicembre 2018.

Osservatorio europeo dei fenomeni di razzismo e xenofobia (2016), *Perceptions of discrimination and islamophobia — Voices from members of Muslim communities in the European Union*, 2006.

Oswald, M., Grace, J., Urwin, S. e Barnes, G. (2017), «Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality», *Information & Communications Technology Law*, 31 agosto 2017.

Regno Unito, Camden e London Prepared (2006), *Major Incident Procedures, What businesses and the voluntary sector need to know*, aprile 2006.

Regno Unito, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29 settembre 2016.

Regno Unito, Equality and Human Rights Commission (2009), *Police and racism: what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

Regno Unito, Her Majesty's Inspectorate of Constabulary (2013), *Stop and Search Powers: Are the police using them effectively and fairly?*, 2013.

Regno Unito, Her Majesty's Inspectorate of Constabulary (2016), *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, febbraio 2016.

Regno Unito, Home Office (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, febbraio 1999.

Regno Unito, Home Office (2014a), *CODE A: Revised code of practice for the exercise by: police officers of statutory powers of stop and search; police officers and police staff of requirements to record public encounters*, Norwich, The Stationery Office (TSO), 2014.

Regno Unito, Home Office (2014b), *Best use of stop and search scheme*, 2014.

Regno Unito, House of Commons Home Affairs Committee (2009), *The Macpherson Report — Ten Years On*, dodicesima relazione della sessione 2008–09, 22 luglio 2009.

Regno Unito, House of Lords (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) c. Commissioner of Police for the Metropolis and another (Respondents)*, [2006] UKHL 12, 8 marzo 2006.

Regno Unito, London School of Economics (2011), *Reading the Riots*, dicembre 2011.

Regno Unito, National Policing Improvement Agency (NPIA) (2012), *Stop and search, the use of intelligence and geographic targeting. Findings from case study research*, 2012.

Regno Unito, Northamptonshire Police (2018), *Get Involved — Reasonable Grounds Panel*, accesso effettuato nell'aprile 2018.

Regno Unito, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), *An Independent Report into Stop & Search Encounters by Staffordshire Police*, gennaio 2015.

Regno Unito, Stop Watch (2011), *«Carry on Recording» Why police stops should still be recorded*, maggio 2011.

Regno Unito, West Midlands Police (2012), *Stop and Search Policy*, novembre 2012.

Regno Unito, West Midlands Police (2016), *Stop and Search Recommendations*, luglio 2015 (modificato da ultimo nel giugno 2016).

Regno Unito, West Midlands Police (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, aprile 2017.

Regno Unito, West Midlands Police (2017b), *New «app» set to speed up Stop & Search process*, agosto 2017.

Regno Unito, West Midlands Police (2018), *Stop and Search Scrutiny Panels*, accesso effettuato nell'aprile 2018.

Regno Unito, West Midlands Police e Crime Commissioner (2014), *Stop and Search Action Plan — Outcome of consultation*, gennaio 2014.

Rete europea di esperti giuridici in materia di parità di genere e non discriminazione (2016), *Links between migration and discrimination — A legal analysis of the situation in EU Member States*, luglio 2016.

Schauer, F. (2003), *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007), relatore speciale delle Nazioni Unite sulla promozione e la protezione dei diritti umani nella lotta al terrorismo, *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, documento delle Nazioni Unite n. A/HRC/4/26, 29 gennaio 2007.

The Guardian (2015), *Northamptonshire police ban stop and search by officers who abuse powers*, 18 agosto 2015.

Tóth, B.M. e Kádár, A. (2011), «Ethnic profiling in ID checks by the Hungarian police», *Policing and Society*, vol. 21, n. 4, pagg. 383-394.

Ufficio dell'Alto commissario delle Nazioni Unite per i diritti umani (OHCHR) (2014), *Recommended Principles and Guidelines on Human Rights at International Borders*, 23 luglio 2014.

USA, GAO (General Accounting Office) (2000), *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results,* GAO/GGD-00-38, marzo 2000.

Van Brakel, R. (2016), «Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing» in van der Sloot, B., Broeders, D. e Schrijvers, E. (a cura di), The Netherlands Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*), *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, pagg. 117-141.

Wrench, J. (2007), *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T.Z. (2011), «Governmental Data Mining and its Alternatives», *Penn State Law Review*, vol. 11, n. 2, pagg. 285-330.

Diritto dell'Unione

Diritti fondamentali

Carta dei diritti fondamentali dell'Unione europea (GU C 202 del 7.6.2016, pag. 389).

Spiegazioni relative alla Carta dei diritti fondamentali (GU C 303 del 14.12.2007, pag. 17).

Non discriminazione

Direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica.

Direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

Protezione dei dati

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

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.

Gestione delle frontiere

Decisione 2007/533/GAI, del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 205 del 7.8.2007), pag. 63.

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 (GU L 119 del 4.5.2016, pag. 132).

Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 381 del 28.12.2006, pag. 4).

Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) (GU L 218 del 13.8.2008, pag. 60).

Regolamento (CE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (GU L 180 del 29.6.2013, pag. 1).

Regolamento (UE) n. 1052/2013 del Parlamento europeo e del Consiglio, del 22 ottobre 2013, che istituisce il sistema europeo di sorveglianza delle frontiere (Eurosur) (GU L 295 del 6.11.2013, pag. 11).

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) (GU L 77 del 23.3.2016, pag. 1).

Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea che modifica il regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio e che abroga il regolamento (CE) n. 863/2007 del Parlamento europeo e del Consiglio, il regolamento (CE) n. 2007/2004 del Consiglio e la decisione 2005/267/CE del Consiglio (GU L 251 del 16.9.2016, pag. 1).

Giurisprudenza

CGUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008.

Corte EDU, *S. e Marper c. Regno Unito*, n. 30562/04 e n. 30566/04, 4 dicembre 2008.

Corte EDU, *Gillan and Quinton c. the United Kingdom*, n. 4158/05 2010, 12 gennaio 2010.

Corte EDU, *B.S. c. Spain*, n. 47159/08, 24 luglio 2012.

Francia, *Cour de Cassation*, *Décision 1245*, 9 novembre 2016.

Regno Unito, Camera dei Lord, *R (on the application of Gillan e al.) c. Commissioner of Police for the Metropolis e al.*, [2006] UKHL 12, 8 marzo 2006.

UNHRC, *Rosalind Williams Lecraft c. Spain*, Comm. n. 1493/2006, 30 luglio 2009.

Per contattare l'UE

Di persona

I centri di informazione Europe Direct sono centinaia, disseminati in tutta l'Unione europea. Potete trovare l'indirizzo del centro più vicino sul sito https://europa.eu/european-union/contact_it

Telefonicamente o per email

Europe Direct è un servizio che risponde alle vostre domande sull'Unione europea. Il servizio è contattabile:

— al numero verde: 00 800 6 7 8 9 10 11 (presso alcuni operatori queste chiamate possono essere a pagamento),
— al numero +32 22999696, oppure
— per e-mail dal sito https://europa.eu/european-union/contact_it

Per informarsi sull'UE

Online

Il portale Europa contiene informazioni sull'Unione europea in tutte le lingue ufficiali: https://europa.eu/european-union/index_it

Pubblicazioni dell'UE

È possibile scaricare o ordinare pubblicazioni dell'UE gratuite e a pagamento dal sito http://publications.europa.eu/it/publications
Le pubblicazioni gratuite possono essere richieste in più esemplari contattando Europe Direct o un centro di informazione locale (cfr. https://europa.eu/european-union/contact_it).

Legislazione dell'UE e documenti correlati

La banca dati Eur-Lex contiene la totalità della legislazione UE dal 1952 in poi in tutte le versioni linguistiche ufficiali: http://eur-lex.europa.eu

Open Data dell'UE

Il portale Open Data dell'Unione europea (http://data.europa.eu/euodp/it) dà accesso a un'ampia serie di dati prodotti dall'Unione europea. I dati possono essere liberamente utilizzati e riutilizzati per fini commerciali e non commerciali.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Con il progredire della tecnologia, il ricorso alla profilazione è andato diffondendosi in un'ampia gamma di contesti e gli Stati membri dell'UE da qualche tempo prestano maggiore attenzione all'uso degli strumenti di profilazione per agevolare il lavoro del personale delle autorità di contrasto e di gestione delle frontiere. La profilazione è legittimamente utilizzata per finalità di prevenzione, indagine e perseguimento di reati, nonché di prevenzione e accertamento dell'immigrazione irregolare. D'altro canto, però, se viene effettuata in modo illecito può minare la fiducia nelle autorità e stigmatizzare alcune comunità.

La presente guida spiega che cos'è la profilazione, illustra i quadri giuridici che la disciplinano ed espone i motivi per cui l'applicazione della profilazione entro i limiti stabiliti dalla legge è necessaria per rispettare i diritti fondamentali ed essenziale per un'efficace attività di polizia e gestione delle frontiere. La guida fornisce inoltre indicazioni pratiche su come evitare la profilazione illecita nelle operazioni di polizia e di gestione delle frontiere.

FRA – AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel +43 158030-0 – Fax +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Ufficio delle pubblicazioni
dell'Unione europea