European Court of Human Right, sez. terza, sentenza 20 febbraio 2024, ricorso n. 43868/18 e 25883/21; Pres. Padre Pastore Vilanova - Est. Milan Blaško - W.B. (avv. Zihlmann) c. Svizzera (sig. Chablais)

Discriminazione etnica – Profilazione razziale – Controllo di identità – Violazione C.e.d.u. – Direttiva 2016/680/UE – Trattamento di categorie particolari di dati – Predictive policing

Condurre accertamenti sull'identità personale di persone di "carnagione scura", in assenza di presupposti oggettivi legittimanti l'esistenza di un fondato dubbio circa la commissione di un illecito, rappresenta un'attività discriminatoria e lesiva della vita privata ai sensi dell'art. 8 C.e.d.u., in combinato disposto con l'art. 14 C.e.d.u., in quanto posta in essere in base ad un meccanismo di profilazione razziale non giustificato. Al fine di dimostrare la condotta discriminatoria, il ricorrente ha l'onere di provare, anche mediante indizi e dati statistici, la sussistenza prima facie di un episodio discriminatorio, mentre verte sullo Stato convenuto l'onere di provare che il trattamento differenziato sia legittimo.

Profilazione razziale e violazione degli artt. 8 e 14 C.e.d.u.: l'intervento della Corte europea dei diritti dell'uomo e le derive della discriminazione algoritmica nelle attività di *law enforcement*

Razmik Vardanian
Dottore in Giurisprudenza Università di Trento e praticante avvocato

Sommario: 1. Il caso: il complesso equilibrio tra la legittimità dei controlli di identità ed i trattamenti discriminatori. – 2. L'orientamento interpretativo della Corte EDU in merito agli artt. 8 e 14 C.e.d.u. – 3. Il trattamento di dati personali nelle attività di *law enforcement*. – 4. I rischi della profilazione nelle attività delle LEA: la profilazione razziale. – 5. Considerazioni conclusive.

Sinossi: La sentenza annotata offre l'occasione di approfondire gli eventuali profili discriminatori derivanti dalle attività delle *law enforcement authorities* ("LEA"). La Corte ha ribadito come i controlli di identità condotti su gruppi di minoranze etniche, mancando i presupposti oggettivi, si traducono in una mera profila-

ISSN 3035-0492

zione razziale comportando un'interferenza ingiustificata nella vita privata e una violazione del divieto di discriminazione. L'utilizzo di dati capaci di rivelare l'origine razziale o etnica da parte delle LEA determina un trattamento di dati personali; per tale ragione, il principio elaborato dalla Corte può essere pacificamente applicato in tale ambito. Il commento, quindi, è dedicato all'analisi delle implicazioni normative di cui alla Direttiva 2016/680/UE e dei rischi che il trattamento di tali dati può comportare.

Abstract: *The annotated judgement provides an opportunity to delve into possible discriminatory profiles arising from the activities of law enforcement authorities ("LEAs"). The Court reiterated how identity checks conducted on ethnic minority groups, lacking the objective prerequisites, result in mere racial profiling entailing unwarranted interference in private life and a violation of the prohibition of discrimination. The use of data capable of revealing racial or ethnic origin by LEAs results in the processing of personal data; consequently, the principle developed by the Court can be peacefully applied in this domain. The commentary, therefore, is devoted to analysing the regulatory implications set forth in Directive 2016/680/EU and the risks that the processing of such data may entail.*

1. Il caso: il complesso equilibrio tra la legittimità dei controlli di identità ed i trattamenti discriminatori

La questione sottesa al caso, risolto dalla Corte europea dei diritti dell'uomo (d'ora in avanti anche solo "Corte", "Corte EDU" o "Corte di Strasburgo"), è relativa alla qualificazione, o meno, della condotta degli agenti di polizia come profilazione razziale[1] a seguito di un controllo di identità apparentemente discriminatorio – e cioè in violazione dell'art. 14 della C.e.d.u. – nonché se quest'ultima potesse determinare una violazione del diritto al rispetto della propria vita privata ai sensi dell'art. 8 C.e.d.u.

Il fatto concreto riguarda il controllo e il fermo del sig. Wa Baile, cittadino svizzero di origini africane, nella stazione centrale di Zurigo da parte della polizia municipale. Tale controllo sembra essere stato condotto solo sulla base della carnagione scura del fermato e dalla circostanza che egli avesse distolto lo sguardo dagli agenti, determinando in questi il sospetto che lo stesso potesse essere autore di una violazione della legge svizzera sugli stranieri e l'integrazione[2]. Solo a seguito della perquisizione personale dell'uomo – con il conseguente rinvenimento del suo documento di identità – è stato consentito allo stesso di allontanarsi, a nulla essendo servite le sue richieste di delucidazioni sulle ragioni del controllo e del fermo. In seguito, l'uomo è stato condannato al pagamento di una sanzione pecuniaria per il mancato rispetto degli ordini della polizia.

[1] L'utilizzo dei termini "razza", "origine razziale" o "profilazione razziale" nella regolamentazione e giurisprudenza internazionale ed europea, non implica l'accettazione di teorie che tentano di dimostrare l'esistenza di razze umane distinte.

[2] Sul punto si intende fare riferimento al Capitolo 16 della Legge federale sugli stranieri e la sua integrazione n. 142.20 del 16 dicembre 2005, il quale disciplina le sanzioni amministrative e penali che possono essere irrogate per gli stranieri irregolari.

Questo provvedimento ha dato avvio ad un lungo procedimento giurisdizionale prima espletatosi in sede penale e in seguito in seno alla giustizia amministrativa svizzera.
Con riguardo al primo, il Tribunale Cantonale di Zurigo ha riscontrato che, sebbene il motivo del controllo addotto dagli agenti fosse discutibile, si dovesse, comunque, concludere per la sua legittimità. Gli ufficiali, infatti, avevano a disposizione un tempo limitato per decidere se fosse opportuna una verifica dell'identità, e non si poteva negare che avessero percepito indizi i quali, in quel frangente, apparivano sufficienti a giustificare tale controllo. Infine, il Giudice ha ritenuto che non vi fosse alcun elemento che consentisse di dimostrare come il colore della pelle fosse stato determinante nell'eseguire il controllo. Tuttavia, per il Tribunale, anche qualora ciò fosse stato riscontrato, questo non avrebbe eliminato l'obbligo per il ricorrente di sottoporsi comunque ad esso. Tale sentenza è stata poi confermata – congiuntamente al provvedimento sanzionatorio – in sede di appello e di legittimità, nonostante fosse stato accertato che il comportamento del sig. Wa Baile non rappresentava una base sufficiente per ritenere che lo stesso avesse commesso un reato e, conseguentemente, legittimare la decisione di sottoporlo a un controllo di identità.
Nel successivo processo amministrativo, invece, il Tribunale amministrativo del Cantone di Zurigo ha riscontrato l'illegittimità del controllo e del fermo. Il motivo alla base di tale decisione è relativo alla circostanza per cui l'aver distolto lo sguardo dagli agenti non poteva, di per sé, giustificare il controllo di identità, anche alla luce del particolare contesto della stazione ferroviaria di Zurigo (elemento, questo, che verrà tenuto in considerazione dalla Corte EDU per valutare l'esistenza *prima facie* di una discriminazione)[3]. Di conseguenza, il Tribunale rinvenendo a monte l'illegittimità del controllo, ha ritenuto di non pronunciarsi sulla questione dell'eventuale discriminazione fondata sul colore della pelle del ricorrente. Pertanto, nonostante l'esito sostanzialmente positivo del giudizio, il sig. Wa Baile adiva la Corte di Strasburgo – a seguito anche all'impugnazione, dichiarata inammissibile, condotta presso il Tribunale Federale Svizzero – al fine di ottenere una pronuncia sulla possibile discriminazione razziale subita.
La decisione della Corte EDU ha evidenziato gravi lacune nelle indagini delle autorità svizzere riguardo a possibili motivi discriminatori nel controllo di identità del ricorrente e ha riconosciuto la violazione dei suoi diritti fondamentali. In particolare, ha ritenuto che il caso rientrasse a pieno titolo nell'ambito dell'art. 8 C.e.d.u., in combinato disposto con l'art. 14 C.e.d.u., in ragione del verificarsi di un'illegittima profilazione razziale da parte delle forze dell'ordine nella scelta del soggetto da sottoporre a controllo. Tale situazione è stata determinata, secondo la Corte, a causa delle notevoli carenze nell'ordinamento giuridico svizzero – nonché nelle prassi amministrative interne – mancando norme chiare e precise poste a evitare trattamenti potenzialmente discriminatori nelle attività di *law enforcement*.

[3] V. *infra*.

2. L'orientamento interpretativo della Corte EDU in merito agli artt. 8 e 14 C.e.d.u.

La profilazione è una tecnica che prevede il trattamento automatizzato di dati personali al fine di utilizzarli 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]. Tale metodologia può essere implementata per sviluppare servizi di *predictive policing*[5] al fine di migliorare la prevenzione dei crimini in ottica prospettica, evitando, così, la commissione di reati, e identificare le aree ad alta concentrazione di crimini o sviluppare profili criminali individuali. L'espletamento delle attività di *law enforcement* con tali modalità, tuttavia, può avere forti implicazioni sulla vita privata delle persone, determinando diversi rischi in grado di impattare su diritti e libertà fondamentali. Uno fra tutti concerne il rischio di trattamenti discriminatori fondati sulla razza o etnia: in tali ipotesi si parla, per l'appunto, di profilazione etnica o razziale. Questa può essere definita come l'uso o l'influenza di stereotipi razziali, etnici e religiosi, ovvero sulla discendenza, sull'origine nazionale o sulla lingua di un individuo, da parte delle forze di polizia nelle proprie attività; in particolare, tali stereotipi possono influenzare le decisioni concernenti il fermo, l'arresto, la perquisizione, l'identificazione ed il controllo dei documenti delle persone, l'inserimento di dati personali in *database*, la raccolta di informazioni di *intelligence* e rispetto ad altre tecniche investigative, indipendentemente dalla valutazione di un suo comportamento potenzialmente criminale[6]. Seguendo tale concezione è evidente come la profilazione razziale possa essere legata a stereotipi e pregiudizi, determinando un deterioramento dei diritti fondamentali

[4] Cfr. art. 4 Reg. 2016/679/UE 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» o «GDPR»), pubblicato in G.U.U.E. il 4 maggio 2016, il cui testo è consultabile in: http://data.europa.eu/eli/reg/2016/679/oj; art. 3, par. 4, Dir. 2016/680/UE.

[5] Cfr. Pietrocarlo, *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in *Sistema Penale*, 2023, 2, in https://www.sistemapenale.it/it/articolo/pietrocarlo-predictive-policing-criticita-e-prospettive-dei-sistemi-di-identificazione-dei-potenziali-criminali. Nello specifico, questa è definita come metodo di analisi previsionale-statistico che consente di individuare i luoghi di futura commissione di reati ovvero i potenziali autori o vittime, orientando le attività di polizia alla prevenzione, più che alla sola repressione del crimine.

[6] Cfr. Cerd, *General recommendation No. 36 on preventing and combating racial profiling by law enforcement officials (CERD/C/GC/36)*, 2020; Ecri, *General Policy Recommendation n. 11 on combating racism and racial discrimination in policing*, 2007; Goldston, *Ethnic Profiling and Counter-Terrorism Trends, Dangers and Alternatives*, in *Open Society Justice Initiative – Anti-Racism and Diversity Intergroup*, 2006, 1, in https://www.justiceinitiative.org/publications/ethnic-profiling-and-counter-terrorism-trends-dangers-and-alternatives. In Italia, una simile definizione è rinvenibile nell'art. 43 d.lgs. 25 luglio 1998, n. 286 (Testo Unico sull'Immigrazione), che stabilisce le condotte considerate discriminatorie nei confronti dei cittadini stranieri a causa della loro condizione di stranieri, appartenenti a una specifica razza, religione, etnia o nazionalità.

dell'uomo, fra cui il rispetto del principio di non discriminazione e il rispetto della vita privata[7].

La Corte di Strasburgo pone l'accento su questi concetti nel dirimere il caso Wa Baile c. Svizzera. La vicenda, come suesposto, riguarda l'accertamento se le autorità di polizia svizzere avessero effettuato un controllo di identità sul ricorrente, cittadino svizzero di carnagione scura, basandosi su un processo di profilazione razziale, inosservando il principio di non discriminazione.

Tale principio trova fondamento in diverse fonti di carattere internazionale e sovrannazionale: esso, infatti, è richiamato nell'art. 5 della Convenzione internazionale delle Nazioni Unite sull'eliminazione di tutte le forme di discriminazione razziale, nell'art. 26 della Convenzione internazionale sui diritti civili e politici, e, per l'appunto, nell'art. 14 della C.e.d.u. Parallelamente, a livello europeo, troviamo l'art. 21 della Carta di Nizza, il quale garantisce il diritto di non subire discriminazioni, incluse quelle basate sulla razza e sull'origine etnica, e la Direttiva 2000/43/CE (c.d. direttiva antidiscriminazione)[8]. Da ciò, dunque, discende che nel condurre le attività di accertamento, controllo e repressione dei reati, le autorità competenti devono attenersi a modelli e valori etici improntati al rispetto delle diversità e della dignità di un individuo, rendendosi necessario prevedere un sistema di garanzie adeguate ed efficaci contro condotte arbitrarie e casi di abuso della forza capaci di sfociare in incidenti evitabili.

Tali canoni non sono stati rispettati dalle autorità svizzere nel caso in questione, poiché il controllo di identità è stato effettuato esclusivamente basandosi sul colore della pelle del ricorrente, senza altre ragioni apparenti o giustificazioni ragionevoli sufficienti a costituire un fondato sospetto da parte delle autorità. Questo tipo di controllo costituisce a tutti gli effetti una profilazione razziale, che viola, pertanto, il principio di non discriminazione e il rispetto della dignità umana.

L'accertamento di una violazione del principio di non discriminazione comporta una particolare valutazione da parte della Corte EDU. In base al proprio consolidato orientamento interpretativo, infatti, l'art. 14 C.e.d.u. integra le altre clausole normative della Convenzione e dei suoi protocolli. Tale principio non ha un'esistenza autonoma, poiché si applica solo in relazione al godimento di altri diritti e libertà garantite dalla Convenzione e nel cui ambito di applicazione rientrino i fatti di causa[9].

[7] Cfr. Ecri, op. cit., par. 34, nel quale si sottolinea che «la profilazione razziale può generare un senso di umiliazione e ingiustizia tra alcuni gruppi di persone e porta alla loro stigmatizzazione e alienazione, deteriorando il rapporto tra la polizia e questi gruppi, a causa della perdita di fiducia che dovrebbero avere in loro».

[8] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, *Wa Baile c. Svizzera*, § 44-56. Il testo di tutte le sentenze della Cedu citate è consultabile in https://www.echr.coe.int/home. Con riguardo alla direttiva antidiscriminazione v. Dir. 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, pubblicata in G.U.U.E. il 19 luglio 2000, il cui testo è disponibile in https://eur-lex.europa.eu/eli/dir/2000/43/oj/ita.

[9] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 68. Inoltre, sul punto v. le sentenze Cedu, 5 settembre 2017, ric. n. 78117/2013, *Fábián c. Ungheria*, § 112; Cedu, 11 ottobre 2022, ric. n. 78630/2012, *Beeler c. Svizzera*, § 48; Dolso,

Per questo motivo, l'attenzione della Corte si è concentrata sull'esame della presunta violazione dell'art. 8 C.e.d.u. in merito alla pratica di profilazione adottata dagli agenti di polizia. Come avvenuto nel caso di specie, infatti, i controlli di identità basati su motivi prettamente discriminatori possono interferire con la vita privata di una persona. La Corte riconosce che la nozione di "vita privata" è ampia e comprende aspetti dell'identità fisica e sociale di un individuo, includendovi anche il diritto allo sviluppo personale e il diritto di stabilire e mantenere relazioni con altri esseri umani e con il mondo esterno. Questo è essenziale per la convivenza in una società democratica e può includere l'interazione in contesti pubblici[10]. In tale scenario, le attività di *law enforcement*, per loro natura, possono avere un impatto particolarmente invasivo nella vita personale degli individui: anche un semplice controllo di identità può incidere negativamente sul diritto alla vita privata, causando pregiudizi irrimediabili e violando la sfera personale degli individui, specialmente quando si sospetta che tale controllo sia basato su un trattamento discriminatorio[11]. Di conseguenza, come già precisato in numerosi precedenti[12], una denuncia di profilazione razziale basata su un controllo di identità discriminatorio può rientrare nell'ambito del diritto al rispetto della vita privata ai sensi dell'art. 8 della Convenzione[13].

Tuttavia, affinché possa essere riscontrata una violazione del suddetto articolo, è necessario che situazioni o comportamenti particolarmente invasivi superino una soglia di gravità tale da essere considerate intollerabili e illegittime. L'individuo interessato, infatti, deve dimostrare di essere stato preso di mira a causa delle sue caratteristiche fisiche o etniche. Richiamando i precedenti dei casi *Basu c. Germania* e *Muhammad c. Spagna*[14], la Corte ha evidenziato come una simile censura può sussistere qualora l'interessato sostenga di essere stato l'unico individuo oggetto di controllo o di fermo, ovvero qualora questi non fossero giustificati da alcun dato o motivo obiettivo, oppure quando le motivazioni addotte dall'agente di polizia dimostrino che essi si basavano su specifiche ragioni fisiche o

Spitaleri, *Art. 14 Convenzione europea dei diritti dell'uomo*, in Bartole, De Sena, Zagrebelsky (a cura di) *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Wolters Kluwer, 2012, 519-522.

10 V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 69.

11 V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 76-77, nel quale viene fatto, altresì, riferimento al caso Cedu, 12 gennaio 2010, ric. n. 4158/2005, *Gillan e Quinton c. Regno Unito*.

12 V. Cedu, 19 gennaio 2021, ric. n. 14065/2015, *Lacatus c. Svizzera*, § 54; Cedu, 14 gennaio 2020, ric. n. 41288/15, *Beizaras e Levickas c. Lituania*, § 117; Cedu, 30 aprile 2009, ric. n. 13444/04, *Glor c. Svizzera*, § 52.

13 La pianificazione e la conduzione di attività di contrasto nei confronti di comunità minoritarie – giustificate sulla base di una presunta connessione tra l'appartenenza etnica e la tendenza al comportamento criminale – è stata, peraltro, più volte sanzionata dalla Corte, quale attività di profilazione razziale, contraria al divieto di discriminazione sancito dall'art. 14 C.e.d.u. A tal proposito v. Cedu, 16 aprile 2019, ric. n. 48474/2014, *Lingurar c. Romania*.

14 V. Cedu, 18 ottobre 2022, ric. n. 215/2019, *Basu c. Germania*, relativo ad un caso di profilazione etnica nel controllo di identità della polizia su un treno condotto verso un cittadino tedesco di origini indiane. Nel caso in questione la Corte non è stata in grado di accertare il movente razziale della polizia a causa dell'insufficiente materiale istruttorio. Inoltre, v. Cedu 18 ottobre 2022, ric. n. 34085/2017, *Muhammad c. Spagna*.

etniche. Inoltre, può essere riconosciuta una certa valenza anche al fatto che tali controlli avvengono in uno spazio aperto al pubblico[15].

Nel caso di specie, la Corte EDU ha riscontrato come le condizioni sopra evidenziate risultassero tutte integrate, con la diretta conseguenza che le azioni della polizia di Zurigo fossero da considerarsi sopra la soglia di gravità necessaria per essere valutate un'intollerabile intrusione nella vita privata del sig. Wa Baile. Alla luce tanto delle circostanze fattuali in base ai quali il controllo di identità ha avuto origine – ossia il fatto che il ricorrente non avesse tenuto alcun comportamento potenzialmente sospetto, se non quello, irrilevante, di aver distolto lo sguardo dagli agenti che lo stavano osservando – quanto del luogo – la stazione ferroviaria di Zurigo – in cui tale controllo è avvenuto, la Corte di Strasburgo ha riscontrato una violazione dell'art. 8 C.e.d.u. Tale infrazione è stata constatata a fronte dell'illegittima conduzione di una profilazione discriminatoria da parte delle LEA nella scelta degli individui da sottoporre a controllo, in quanto condotta in base al colore della pelle.

Un'ulteriore questione dibattuta riguarda l'assegnazione dell'onere probatorio nelle controversie relative a ipotesi di discriminazione razziale. Generalmente, i giudizi di accertamento di una condotta discriminatoria si articolano in due fasi, ciascuna con una diversa attribuzione dell'onere probatorio. Nella prima fase di ricognizione, il ricorrente ha l'onere di dimostrare, innanzitutto, l'esistenza di una disparità di trattamento contraria ai principi della Convenzione. Tali elementi di prova possono essere reperiti tramite un insieme di indizi o presunzioni non confutate, sufficientemente gravi, precise e concordanti, derivanti dalle circostanze concrete della vicenda. Particolare importanza assume la valutazione dei dati statistici, che possono evidenziare come i fatti di causa derivino da una disparità di trattamento dovuta a una discriminazione sistematica conseguente ad una determinata pratica statale o a una generalizzata situazione di fatto[16]. Spesso i dati statistici prodotti dalle parti assumono un'importanza cruciale in tali giudizi, poiché la Corte si basa frequentemente su di essi per dimostrare la disparità di trattamento tra due gruppi. Inoltre, può tenere conto anche delle relazioni fornite da organismi di vigilanza nazionali e internazionali indipendenti[17]. Una volta che il ricorrente abbia dimostrato la disparità di trattamento, spetta al Governo resistente provare l'inesistenza di tale disparità o che essa

[15] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 71.

[16] Nello specifico la discriminazione sistematica può essere definita come «una situazione in cui le norme giuridiche, le politiche, le pratiche o gli atteggiamenti culturali predominanti nel settore pubblico o privato generano svantaggi per alcuni gruppi e privilegi per altri gruppi». Questa, come visto, può concernere una pratica statale o una generalizzata situazione fattuale esistente in una data comunità, come le sue procedure, le abitudini, le credenze e la cultura. Cfr. Comitato dei diritti economici, sociali e culturali delle Nazioni Unite, *Commento generale n. 20 - Non discriminazione a livello dei diritti economici, sociali e culturali. Individuare e prevenire la discriminazione sistemica a livello locale*, 2009, 5-6; Dolso, Spitaleri, *Art. 14 Convenzione europea dei diritti dell'uomo*, op. cit., 536-538.

[17] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 114-123.

fosse giustificata sulla base di elemento oggettivi[18]. In particolare, lo Stato convenuto deve vincere la presunzione relativa instaurata *prima facie* dal ricorrente, dimostrando che nessun motivo discriminatorio abbia influenzato l'adozione di una misura o azione, mediante un adeguato corredo probatorio idoneo ad escludere la presenza di una disparità di trattamento ingiustificata[19].

Con riguardo al caso di specie, la Corte ha considerato le prove fornite dal ricorrente – comprese le dichiarazioni degli agenti di polizia coinvolti e i rapporti di organismi internazionali che manifestavano la seria presenza di profilazione razziale da parte delle forze dell'ordine in Svizzera[20] – come sufficienti a dimostrare l'esistenza di un caso di discriminazione razziale. Attribuito al Governo svizzero l'onere di escludere l'esistenza di tale disparità, la Corte ha osservato come quest'ultimo non sia stato in grado di confutare in modo convincente la presunzione di trattamento discriminatorio. Nello specifico, le autorità amministrative e giurisdizionali nazionali non avevano svolto un'indagine adeguata a determinare se il controllo fosse stato effettuato sulla base della carnagione del ricorrente. In seso alla polizia svizzera, inoltre, non vi erano procedure o *policy* volte a regolamentare e/o a fornire delle indicazioni oggettive agli operatori sulla cui base poter condurre un controllo di identità su un soggetto in modo da evitare condotte potenzialmente discriminatorie, rendendo, pertanto, il contesto operativo delle autorità di pubblica sicurezza particolarmente ambiguo e legato a scelte pienamente discrezionali.

Di conseguenza, la Corte ha ritenuto che la mancanza di un quadro giuridico e amministrativo sufficientemente chiaro possa aver determinato l'effettuazione di controlli di identità – anche nel caso di specie – sulla base di una profilazione razziale, in violazione degli artt. 8 e 14 C.e.d.u.[21].

[18] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 132-133. La Corte ha confermato il proprio precedente *D.H. e altri c. Repubblica Ceca*, in cui era stato stabilito che le autorità dovessero fornire spiegazioni soddisfacenti e convincenti quando vi sono accuse di discriminazione. Tale imputazione vale ancor di più rispetto ad eventi discriminatori i cui fatti storici sono noti esclusivamente alle autorità. Cfr. Cedu, 13 novembre 2007, ric. n. 57325/2000, D.*H. e altri c. Repubblica Ceca*; Dolso, Spitaleri, *Art. 14 Convenzione europea dei diritti dell'uomo*, op. cit., 541-543.

[19] Cfr. Henrard, *The European Court of Human Rights and the 'Special' Distribution of the Burden of Proof in Racial Discrimination Cases: The Search for Fairness Continues*, in *European Convention on Human Rights Law Review*, 2023, Vol. 4, 429-442, in https://doi.org/10.1163/26663236-bja10065.

[20] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 120-127, ove è stato dato particolare rilievo al rapporto pubblicato da *Amnesty International* sul tema delle pratiche di polizia in Svizzera, il quale denunciava atteggiamenti razzisti da parte di alcuni agenti di polizia nei confronti di persone sottoposte a controlli di identità. Inoltre, anche il CERD, nelle sue osservazioni conclusive del 27 dicembre 2021 sul rapporto della Svizzera, ha ritenuto che la formazione degli agenti di polizia svizzeri fosse insufficiente a prevenire efficacemente i casi di profilazione razziale.

[21] V. Cedu, 20 febbraio 2024, ric. n. 43868/2018 e 25883/2021, cit., § 133-134.

3. Il trattamento di dati personali nelle attività di law enforcement

Il caso Wa Baile c. Svizzera evidenzia l'urgente necessità di riformare le pratiche di *law enforcement* per garantire il rispetto della dignità umana e per prevenire il rischio della conduzione di profilazioni discriminatorie. Sebbene il divieto di discriminazione possa avere un effetto diretto, sono il diritto alla protezione dei dati e il diritto alla privacy a rappresentare i pilastri fondamentali per garantirne l'attuazione. L'adozione di pratiche decisionali profilatorie, quindi, solleva preoccupazioni anche in merito alla conformità con i principi cardini della disciplina sulla protezione dei dati[22], oltre che in merito alla violazione dei diritti fondamentali sanciti dalla C.e.d.u., in particolare il suo art. 8. Infatti, come evidenziato dalla Corte EDU nel caso *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*: «tale articolo prevede il diritto a una forma di autodeterminazione informativa, che consente alle persone di invocare il loro diritto alla riservatezza di dati che, benché neutrali, sono raccolti, trattati e diffusi collettivamente e in forma o maniera tale da riguardare i diritti delle persone interessate ai sensi dell'articolo 8»[23]. Inoltre, l'uso improprio e discriminatorio dei dati personali può perpetuare un ciclo di sorveglianza mirato e ingiustificato, aggravando ulteriormente le disuguaglianze esistenti e compromettendo la fiducia delle persone nelle istituzioni di sicurezza pubblica.

Con riguardo a ciò, già il Consiglio d'Europa promosse nel 1987 una raccomandazione volta a regolamentare l'uso dei dati personali nel settore della polizia, fornendo un insieme generale di principi per garantire il rispetto del diritto alla vita privata e la protezione dei dati[24]. La raccomandazione includeva una norma più severa sul trattamento delle categorie di dati sensibili, come la razza, prescrivendo che la raccolta di tali dati, se non prescritta espressamente dalla legge, dovesse essere proibita[25]. Tuttavia, queste previsioni non hanno avuto un impatto significativo nell'assicurare che le attività di *law enforcement* si svolgessero in modo trasparente e conforme ai principi di equità e proporzionalità[26].

[22] A livello internazionale questi possono essere ricondotti alla Convenzione 108 del Consiglio d'Europa, la quale ha riconosciuto la *data protection* come prerogativa specifica dell'individuo e distinta dal diritto alla riservatezza (la Convenzione è stata poi rimodernata nel 2018 con il Protocollo di modifica). In seguito, il diritto alla protezione dei dati personali è stato meglio declinato e ampliato – a livello Europeo – dalla Dir. 46/95/CE e, successivamente, dal GDPR. Quest'ultimo, in particolare, mediante il fenomeno del c.d. *Brussels Effect* ha contribuito – come *benchmark* di riferimento – a migliorare significativamente la disciplina e le prassi relative alla protezione dei dati a livello internazionale. Sul punto cfr. Bradford, *The Brussels Effect: How the European Union Rules the World*, in *Oxford Academic*, 2020, 25-66, in https://doi.org/10.1093/oso/9780190088583.001.0001.

[23] V. Cedu, 27 giugno 2017, ric. n. 931/2013, *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, § 136-138; Pitea, Tomasi, *Art. 8 Convenzione europea dei diritti dell'uomo*, in Bartole, De Sena, Zagrebelsky (a cura di) *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Wolters Kluwer, 2012, 315-319.

[24] Cfr. Council of Europe, *Recommendation R (87) 15, Regulating the Use of Personal Data in the Police Sector*, 1987.

[25] Cfr. Council of Europe, *Recommendation R (87) 15*, op. cit., Principle 2 - Collection of data (§ 43-48).

[26] Il contesto successivo non è migliorato dopo degli eventi dell'11 settembre 2001, in conseguenza dei quali sono state introdotte politiche finalizzate a profilare i cittadini di tutto il mondo al fine di costruire dei profili terroristici per il tramite

Nell'ambito dell'Unione europea, si è giunti ad un traguardo significativo con l'emanazione della Direttiva 2016/680/UE, conosciuta anche come *Law Enforcement Directive* ("LED")[27]. Questo strumento normativo disciplina in modo dettagliato il trattamento dei dati personali da parte delle autorità competenti per la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati, nonché per l'esecuzione delle sanzioni penali, promuovendo parallelamente la libera circolazione di tali dati[28]. Come suggerisce il suo nome, la LED riguarda il trattamento dei dati personali da parte di titolari del trattamento per «finalità di applicazione della legge», esulando dal campo di applicazione del GDPR[29]. Tuttavia, in concreto, le finalità della LED possono riguardare attività che non rientrano specificamente nell'ambito penale ma che riguardano le funzioni di polizia svolte prima della commissione di un reato[30].

Nonostante la Confederazione Elvetica non sia membro dell'Unione europea, la Dir. 2016/680/UE si applica comunque al Paese come parte del processo di sviluppo dell'*acquis* di Schengen[31]. L'*acquis* di Schengen rappresenta l'insieme di norme, accordi e regolamenti che costituiscono la base della cooperazione Schengen, un sistema progettato per

delle autorità di sicurezza. Il *profiling* basato su caratteristiche psico-sociologiche asseconda un grande rischio di discriminazione. Cfr. Hayes, *A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe*, in *Open Society Justice Initiative*, 2005, 33-37, in https://www.statewatch.org/media/documents/news/2005/jun/ben-hayes-A-Fai.pdf.

27 V. Dir. 2016/680/UE 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, pubblicata in G.U.U.E. il 4 maggio 2016, il cui testo è consultabile in: http://data.europa.eu/eli/dir/2016/680/oj. La *Law Enforcement Directive* faceva parte del pacchetto legislativo sui dati diramato dalla Commissione UE a partire dal 2016, comprendente il GDPR, la LED, la Dir. 2016/681/UE, sull'uso dei dati del codice di prenotazione aereo per le attività di contrasto ("PNR"), e il Reg. 2018/1725/UE relativo alle norme applicabili al trattamento dei dati personali da parte delle istituzioni, organi e organismi dell'Unione europea. Sul punto cfr. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *QCost*, 3, 2016, 587-589.

28 Con riguardo all'ambito materiale di applicazione, il considerandum n. 18 LED evidenzia che le protezioni della Direttiva dovrebbero impiegarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Il caso in commento, dunque, rientrerebbe ragionevolmente in questo secondo ramo applicativo, in quanto i dati identificativi del sig. Wa Baile, raccolti manualmente dalle autorità svizzere, saranno stati certamente inseriti all'interno degli archivi della polizia.

29 V. considerandum n. 19 GDPR.

30 V. art. 1 LED; cfr. Gallo, *Implications of Artificial Intelligence in the Field of Law*, in *i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2023, Vol. 16 n. 1, 18-19, in https://i-lex.unibo.it/article/view/17200. Le finalità coperte dalla LED possono quindi includere attività preventive della polizia durante manifestazioni, eventi sportivi e/o mantenimento dell'ordine pubblico, con correlati trattamenti di dati personali effettuati per tali scopi.

31 V. consideranda n. 102-103 LED. Al contrario, il GDPR non è applicabile alla Svizzera, la quale ha adottato una propria legge federale sulla protezione dei dati personali, da ultimo revisionata nel 2020 con la *New Federal Act on Data Protection* ("nFADP"). Inoltre, è importante considerare che ognuno dei 26 Cantoni ha emanato una propria legislazione in merito alla protezione dei dati personali. Cfr. Collina, *Il GDPR in una prospettiva cross-border. Cenni all'applicazione del nuovo regolamento a tutela della privacy in Svizzera*, in Bertoli, Ferrari, Ripamonti, Tiberi (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, Giappichelli, 156-164. In ogni caso, la Commissione UE ha rinnovato la Decisione di adeguatezza 2000/518/CE originariamente emessa durante la vigenza della Dir. 95/46/CE, confermando la sostanziale equivalenza della disciplina relativa alla protezione dati nel territorio svizzero rispetto al GDPR. V. European Commission, *Report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC*, 2024, 14-15, in https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161.

garantire la libera circolazione delle persone all'interno delle frontiere interne dei paesi aderenti[32]. In sintesi, tale insieme di norme consiste nell'Accordo di Schengen del 1985, nella Convenzione di applicazione e completamento del 1990, nei successivi trattati di adesione[33], nelle misure compensative applicabili[34] nelle ulteriori normative applicabili in virtù degli accordi di Schengen[35]. Il recepimento della Direttiva, pertanto, è avvenuto in Svizzera originariamente con la legge federale sulla protezione dei dati personali nell'ambito dell'applicazione dell'*acquis* di Schengen in materia penale (RU 2019 639) e dalle varie leggi locali approvate dai singoli Cantoni[36]. Tale impianto normativo, tuttavia, è stata abrogato nel 2023, quando è entrata in vigore la nFADP che – tenendo conto degli sviluppi sul piano internazionale, con la riforma della Convenzione 108+ del Consiglio d'Europa e su quello europeo, con il GDPR – ha riordinato la disciplina interna, incorporando al proprio interno anche le previsioni di recepimento della LED[37].

Come per il GDPR, la LED ha introdotto un quadro normativo articolato volto a stabilire le garanzie e i principi in base ai quali può realizzarsi un trattamento di dati personali, stabilendo precisi obblighi tecnici ed organizzativi, nonché ad assicurare agli interessati la possibilità di esercitare un controllo sui propri dati – nonostante il contesto delicato – mediante l'attribuzione di una serie di diritti. In modo schematico, di seguito alcuni degli obblighi principali previsti dalla Direttiva:

- dover distinguere chiaramente tra le diverse categorie di interessati (indagati, condannati, vittime di reato) per consentire una gestione più efficace e attenta dei dati (art. 6);
- dover verificare l'accuratezza, la pertinenza e tempestività dei dati, anche mediante procedure organizzative volte a individuare e correggere eventuali errori, al fine di garantire che le decisioni basate su di essi siano qualitativamente affidabili (art. 7);

[32] Cfr. Bellucci, *Schengen nel nuovo millennio,* Laurus Robuffo, 161-168; Guild, Brouwer, Groenendijk, Carrera, *What is happening to the Schengen borders?*, in *CEPS Paper in Liberty and Security in Europe*, n. 86, 2015, 1-3, disponibile in https://hdl.handle.net/2066/150061; Marinai, *Il controllo delle frontiere e la lotta all'immigrazione Irregolare*, in Aa.Vv. (a cura di), *Lineamenti di diritto internazionale ed europeo delle migrazioni*, Wolters Kluwer, 2021, 204-221.

[33] Per l'adesione della Svizzera v. G.U.U.E. L 53 del 27.2.2008, 52 e ss.

[34] Per mantenere un alto livello di sicurezza, l'*acquis* di Schengen include misure come la cooperazione tra le forze di polizia e giudiziarie, il sistema d'informazione Schengen (SIS) per lo scambio di informazioni su persone e beni, e norme comuni in materia di visti e asilo. Rientrando proprio nel primo tra questi ambiti, la Dir. 2016/680/UE mira a facilitare la cooperazione nella lotta contro la criminalità in Europa, armonizzando la protezione dei dati personali da parte delle autorità incaricate dell'applicazione della legge negli Stati membri dell'Unione europea e nei paesi Schengen.

[35] Sul punto v. Decisione Consiglio dell'Unione europea che definisce l'*acquis* di Schengen (1999/435/CE), pubblicato in G.U.U.E il 10 luglio 1999 e disponibile in http://data.europa.eu/eli/dec/1999/435/oj.

[36] Cfr. Costa, *Evoluzione del diritto cantonale della protezione dei dati – quo vadis?*, in Bernasconi, Pasucci (a cura di), *Protezione dei dati personali: orizzonte 2023, Atti della giornata di studio del 3 giugno 2022*, 2023, 234-238, in https://www4.ti.ch/can/sgcds/pd/pubblicazioni/collane-della-cfpg. Sul punto si riporta l'esempio del Cantone Ticino, v. Consiglio di Stato, *Messaggio n. 8281 del 17 maggio 2023 - Revisione totale della legge cantonale sulla protezione dei dati personali* in https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/M8281_Revisione_totale_LPDP.pdf.

[37] Il testo della nFADP è consultabile in https://fedlex.data.admin.ch/eli/fga/2020/1998. Cfr. Schneider, Sturny, Reeves, Switzerland, in Raul (edit by), *The Privacy, Data Protection and Cybersecurity Law Review*, 2022, 413-416.

- dover prefissare – ciascuno Stato membro all'interno del proprio ordinamento – con sufficiente precisione gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento necessario per le attività di contrasto alla criminalità (art. 8);
- dover adottare misure tecniche e organizzative mirate ad assicurare la sicurezza e l'integrità dei dati, nonché la capacità di dimostrare tale conformità in caso di verifica (art. 19);
- dover implementare dei principi della *data protection by design* e *by default* (art. 20).

Una specifica rilevanza viene assegnata anche al trattamento di categorie particolari di dati da parte delle LEA, come quelli idonei a rivelare l'origine razziale o etnica. Già a livello internazionale, ai sensi dell'art. 8 C.e.d.u. e della Convenzione 108+[38], il trattamento di tali categorie di dati – potenzialmente capaci di ledere il diritto al rispetto della vita privata – dev'essere limitato solamente ai casi prescritti dalla legge. In aggiunta, in un'ottica di maggiore garanzia, tali trattamenti possono ritenersi legittimi solo qualora costituiscano una misura necessaria e proporzionata in una società democratica a tutelare gli interessi della sicurezza nazionale, della sicurezza pubblica, degli interessi economici e finanziari, per la prevenzione dei reati e la difesa dell'ordine pubblico o per la protezione di diritti e libertà altrui. Al fine di prevenire interferenze indebite, è necessario adottare misure adeguate a mitigare il rischio di discriminazione, bilanciando attentamente il diritto alla riservatezza con l'esigenza di contrastare il crimine. Queste misure devono considerare lo scopo dell'indagine, il contesto circostante e la sensibilità dei dati, al fine di determinare l'ammissibilità e l'entità del trattamento da parte delle autorità di polizia[39]. Questo orientamento è stato recepito anche nella LED, il cui art. 10 prevede che categorie particolari di dati possano essere trattate solo se strettamente necessarie e adottando adeguate garanzie per tutelare i diritti e le libertà dell'interessato, ed in ogni caso esclusivamente: *i*) se espressamente autorizzato dal diritto dell'Unione o dello Stato membro; *ii*) se diretto a salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; *iii*) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.

L'apertura al trattamento di dati etnici o razziali – seppur limitata – evidenzia un approccio prudente del Legislatore europeo all'uso di questi dati particolarmente sensibili per la conduzione di attività di contrasto. Tale importazione, come si avrà modo di esporre nel paragrafo che segue, viene, peraltro, confermata nella LED anche con riguardo alla profilazione degli individui mediante l'uso di *dataset* rappresentativi di categorie particolari di dati, con la previsione di specifiche garanzie volte a prevenire il rischio di condotte discriminatorie.

[38] Cfr. Council of Europe, *Convenzione 108+ sulla protezione degli individui rispetto al trattamento di dati personali,* 2018, artt. 6 e 11.

[39] Cfr. Council of Europe, *Practical guide on the use of personal data in the police sector*, 2018, 9.

4. I rischi della profilazione nelle attività delle LEA: la profilazione razziale

L'attenzione crescente che sia l'UE, sia le istituzioni internazionali dedicano alla protezione dei dati è ben nota. Ciononostante, vi sono restrizioni al diritto alla protezione dei dati personali che la C.e.d.u. stessa e la Dir. 2016/680/UE legittimano al fine di salvaguardare la sicurezza pubblica. In questo modo viene legittimato l'utilizzo, da parte della polizia, di tecnologie intrusive, utilizzate per scopi di *predictive policing*. Come suesposto, l'uso di tali tecnologie consente alle LEA di prendere di mira, sia reattivamente che proattivamente, individui o gruppi considerati ad alto rischio di commettere o aver commesso un reato[40]. Le previsioni sull'attività criminale futura comportano operazioni di trattamento che includono la raccolta, la memorizzazione, l'analisi e l'utilizzo dei dati. In particolare, la loro raccolta può avvenire attraverso diverse fonti, come le rilevazioni svolte dalle forze dell'ordine, i dati demografici e le informazioni geografiche; i dati così raccolti potranno poi essere archiviati in database centralizzati tali da permetterne una facile accessibilità e gestione. L'analisi dei dati potrà, poi, essere condotta usufruendo di algoritmi avanzati e modelli di *machine learning* per individuare modelli e tendenze che possono indicare aree a rischio di future attività criminali. Infine, l'utilizzo di tali dati rende possibile l'implementazione di modelli previsionali nelle operazioni di polizia quotidiane, come la pianificazione delle pattuglie e l'allocazione delle risorse.

Per quanto riguarda la LED, questa definisce la profilazione nei medesimi termini del GDPR[41]. Tuttavia, a differenza di quest'ultimo, il quale ammette le decisioni basate unicamente su un trattamento automatizzato e stabilisce diversi principi in merito alla profilazione, la LED adotta un approccio differente. L'art. 11 della Direttiva, infatti, vieta che le autorità di contrasto possano prendere decisioni basate esclusivamente su trattamenti automatizzati, compresa la profilazione, qualora queste producano effetti giuridici o influiscano significativamente sull'interessato. Questa disposizione, tuttavia, è soggetta a diverse limitazioni; in particolare, il processo decisionale automatizzato è ammesso quando previsto dalla legislazione dell'Unione o degli Stati membri. Attraverso l'emanazione di leggi, gli Stati membri possono quindi legittimare l'uso da parte delle autorità di polizia di decisioni completamente automatizzate per fare previsioni sistemiche e/o individualizzate riguardanti futuri comportamenti criminali. In ogni caso è previsto che i titolari forniscano idonee garanzie per i diritti e le libertà degli interessati, fra cui l'obbligo di assicurare un

[40] Cfr. European Union Agency for Fundamental Rights, *Preventing Unlawful Profiling Today and in the Future: A Guide*, 2018, 18-19, in https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide.

[41] V. *supra* nota 1.

intervento umano, ove richiesto, ovvero il diritto dell'interessato di esprimere il proprio punto di vista e contestare la decisione automatizzata[42].
Quando, invece, la decisione automatizzata si basa su dati sensibili, l'art. 11, par. 2, LED specifica che tale decisione non possa avvenire a meno che non siano in atto misure idonee a salvaguardare i diritti, libertà e legittimi interessi dell'interessato i cui dati sono trattati. Infine, è importante notare che al paragrafo 3 viene stabilito anche un divieto espresso alla profilazione basata su dati sensibili che possa portare ad una discriminazione, in conformità con la legislazione antidiscriminazione dell'UE e la Carta di Nizza[43].
L'art. 11 LED prevede espressamente la sua applicazione all'implementazione di un processo decisionale completamente automatizzato che produca effetti giuridici negativi o incida significativamente sull'interessato. Tuttavia, anche nell'impiego circoscritto di algoritmi durante le attività istruttorie o ispettive delle autorità di controllo – ad esempio, attraverso l'individuazione di "zone critiche" a rischio di commissione di reati – persiste un'alea di rischio elevata per i diritti e le libertà degli interessati. Infatti, nonostante l'apparente neutralità di una decisione automatizzata, anche se in un procedimento diretto da una persona fisica, vi è sempre il rischio di un controllo sistematico derivante da una profilazione discriminatoria, capace di stigmatizzare un gruppo sociale. Di conseguenza, non è chiaro se tale effetto sia sufficiente per attivare l'art. 11 LED o se sia, invece, necessario che un individuo dimostri effetti avversi specifici[44]; è, però, evidente che una tecnica di profilazione del genere, che comporterebbe la discriminazione degli individui, sarebbe comunque vietata dal diritto dell'Unione e dalla stessa C.e.d.u.
Come anticipato, anche l'utilizzo di dati apparentemente neutrali per sviluppare modelli algoritmici automatizzati può essere fonte di discriminazione sotto forme diverse. Sul punto, infatti, si suole distinguere tra profilazione diretta, quando elementi come razza ed etnia sono utilizzati come criteri di selezione per guidare le decisioni di sorveglianza, e profilazione indiretta, che si verifica quando criteri apparentemente neutrali, come il parlare una determinata lingua, vengono ingiustificatamente incorporati in un profilo di rischio, portando alla selezione sproporzionata di persone con un determinato *background*. Infatti, può accadere che il *dataset* di addestramento del sistema possa essere contaminato da *bias* concernenti l'etnia degli individui o la loro storia sociale. In queste ipotesi, l'algoritmo, soprattutto in caso di sistemi di apprendimento automatico non supervisionato, potrebbe generare dei risultati distorti producendo un possibile pregiudizio agli interessati[45]. Sul

[42] V. consideranda n. 37, 38, 51 LED.

[43] V. considerandum n. 38 LED. Per approfondire v. Gottschalk, *Automated individual decision-making*, in Kosta, Boehm (a cura di), *The EU Law Enforcement Directive (LED): A Commentary*, 2024, Oxford Academic, 232-240, disponibile in https://doi.org/10.1093/law/9780192855220.003.0011.

[44] Cfr. Lynskey, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, in *International Journal of Law in Context*, 2019, Vol. 15, 172-174, in https://doi.org/10.1017/S1744552319000090.

[45] Cfr. Molaschi, *Algoritmi e discriminazione*, in *Fundamental rights*, 2022, 2(3), 28-31, in https://fundamentalrights.it/wp-content/uploads/2022/10/3-MOLASCHI-impaginato.pdf; Stanzione, *Data Protection and vulnerability, in European Journal*

punto, diversi studi hanno dimostrato che il *profiling* algoritmico prende di mira gruppi marginalizzati, come le minoranze etniche, individui con basso status socio-economico e donne[46]. Spesso tale problematica può persino prescindere dalla questione della discriminazione indiretta[47]. Gli esiti discriminatori possono derivare anche dall'uso di *proxy*, ossia attributi o variabili che, pur non essendo direttamente collegati a dati "sensibili", possono indirettamente causare discriminazione. In questi casi, la discriminazione non si riferisce a caratteristiche personali particolari, ma ad attributi come reddito, codice postale, attività lavorativa, tipo di automobile, ovvero a complesse combinazioni algoritmiche di vari attributi[48]. Quindi, è opportuno che tali sfide siano affrontate con l'applicazione congiunta del diritto alla protezione dei dati e del diritto antidiscriminatorio, responsabilizzando i soggetti attivamente e passivamente interessati dai modelli di *policing profiling*.

Nonostante l'adozione di sistemi di profilazione e polizia predittiva possa essere considerato legittimo, l'assenza di linee guida relative alle modalità di addestramento, alla qualità dei *dataset* di addestramento, sul quando e in che contesto operativo applicarli e sulle modalità di verifica dei risultati genererebbe una grave carenza in punto di legalità dell'attività eventualmente condotta. La mancanza di previsioni – anche di natura organizzativa – chiare, tassative e determinate comporterebbe l'attribuzione di un'area di discrezionalità eccessivamente ampia, tale per cui possono essere presi a riferimento indicatori – come quello dell'origine razziale – che esulano dallo svolgimento di una legittima attività di verifica da parte della polizia. Ciò genererebbe delle differenze di trattamento meramente discriminatorie rispetto ai luoghi in cui questi sistemi possono essere impiegati e alle categorie di persone che li frequentano.

Il rischio ulteriore della realizzazione di una profilazione discriminatoria – mediante l'utilizzo di categorie particolari di dati – è quello che può condurre al compimento di una sorveglianza di massa, dove ogni individuo è costantemente sorvegliato, restringendo ogni possibile valenza di riservatezza e rispetto della vita privata[49]. Ogni persona può diventare

of Privacy Law and Technologies, 2, 2020, 8-15. Gli algoritmi, infatti, sono sviluppati in base alla logica "*garbage in/garbage out*", comportando che l'introduzione di dati incongruenti, inaccurati o non aggiornati produrrà necessariamente decisioni inaffidabili e inaccurate. Sul punto v. Open Data Science, *Garbage In, Garbage Out: Automated Machine Learning Begins with Quality Data*, in https://medium.com/@ODSC/garbage-in-garbage-out-automated-machine-learning-begins-with-quality-data-70471cb33748. Nel contesto delle attività di contrasto, tale problematica è particolarmente impattante sugli individui, aggravando potenzialmente le possibilità di discriminazione indiretta.

[46] Cfr. Mann, Matzner, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, in *Big Data & Society*, 2019, 6(2), 2, in https://doi.org/10.1177/2053951719895805. Inoltre, v. Gerards, Xenidis, *Algorithmic discrimination in Europe: challenges and opportunities for gender equality and non-discrimination law*, in *Publications Office*, 2021, https://data.europa.eu/doi/10.2838/544956.

[47] Sulla distinzione tra discriminazione diretta e indiretta si rimanda a Consiglio, *Che cosa è la discriminazione? Un'introduzione teorica al diritto antidiscriminatorio*, 2020, Giappichelli, 79-104.

[48] Cfr. Mann, Matzner, *Challenging algorithmic profiling*, op. cit., 4. Tale forma di discriminazione è definita come discriminazione emergente. Per degli esempi, v. Grasso, *The Bad Algorithm,* 2021, Edizioni Scientifiche Italiane, 37.

[49] Cfr. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, in *European Journal on Criminal Policy and Research*, 2023, Vol. 29, 519-520, in https://doi.org/10.1007/s10610-022-09512-y.

un sospettato, e persino comportamenti casuali (come indossare grandi occhiali da sole, nascondere il viso o guardare il terreno) potrebbero essere considerati sospetti a causa di *bias* o percezioni stereotipate[50]. Al fine di soddisfare il diritto alla riservatezza, dignità e rispetto della vita privata, sarebbe fondamentale che i meccanismi di polizia predittiva fossero utilizzati alla luce di due criteri principali: il principio della finalità legittima e il principio della proporzionalità[51]. Il principio della finalità legittima è riconosciuto all'art. 4, par. 1, lett. *b*) LED, all'art. 8 par. 2 della CDFUE, all'art. 6 della Convenzione 108+ e all'art. 5, par. 1, lett. *b*) GDPR e comporta che il trattamento dei dati debba perseguire scopi ritenuti leciti dall'ordinamento giuridico[52]. Il principio di proporzionalità, declinato nelle sue sottodimensioni di proporzionalità in senso stretto, necessità ed efficacia concerne la ponderazione tra l'ingerenza della misura adottata, rispetto alla vita privata di un individuo, e l'obiettivo che dev'essere raggiunto mediante essa[53]. Tali concetti possono essere mutuati anche nel ragionamento della Corte nel caso Wa Baile c. Svizzera. L'attività della polizia, di per sé legittima, dev'essere improntata a principi di proporzionalità e necessità in caso di attività di controllo nei confronti di persone appartenenti a gruppi minoritari. La raccolta e il trattamento di dati etnici, o idonei a rilevare l'origine razziale – così come di altre categorie particolari di dati, come quelli biometrici o relativi all'orientamento sessuale – dev'essere considerato eccessivo e sproporzionato rispetto alla tutela della sicurezza, se non giustificate dall'esistenza di un fondato sospetto e, soprattutto, se lo scopo del trattamento di tali dati può essere raggiunto con misure meno invasive.

Nel valutare l'interferenza della profilazione algoritmica – anche a fini di polizia – con il divieto di discriminazione e il diritto alla protezione dei dati, un elemento critico è la possibilità di riscontrare la presenza di falsi positivi. La possibile incidenza di risultati erronei o distorsivi, se non compiutamente rilevata, minaccia l'adeguatezza delle attività di *policing profiling*, rischiando di risolversi in un trattamento discriminatorio e in una possibilità di profilazione razziale. Un errore nell'identificazione di un potenziale criminale – in base alla sua etnia – può portare a esiti come la detenzione e la divulgazione pubblica dell'identità della persona, causando discredito sociale e danni alla reputazione. Inoltre, la presenza di *bias* nei dati di addestramento può danneggiare sistematicamente le persone appartenenti a minoranze etniche, a fronte di risultati erronei[54]. Questo fenomeno finisce

[50] Cfr. CNIL, *Reconnaissance Faciale – Pour Un Debat À La Hauteur des Enjeux*, 2019, 6-8, in https://www.cnil.fr/sites/cnil/files/atoms/files/reconnaissance_faciale.pdf.

[51] Cfr. Edps, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 2019, in https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en.

[52] Cfr. Bianchedi, Modica, *Il principio di liceità*, in Bravo (a cura di), *Dati personali protezione, libera circolazione e governance - 1. Principi*, Pacini Editore, 2023, 65-69.

[53] Cfr. Scaccia, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle corti europee*, in *Associazione Italiana dei Costituzionalisti*, 2017, Vol. 3, 5-7, in https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/gino-scaccia/proporzionalit-e-bilanciamento-tra-diritti-nella-giurisprudenza-delle-corti-europee.

[54] Cfr. Dushi, *The use of facial recognition technology in EU law enforcement: Fundamental rights implication*, in *Policy*

per creare ulteriori fenomeni di stigma contro frange già fragili della popolazione, aggravando la loro situazione nei confronti delle forze dell'ordine e alimentando la discriminazione[55]. Per superare tali problematiche, è necessario che i dati utilizzati per addestrare gli algoritmi siano accurati e aggiornati, nonché controllati per verificare la possibile esistenza di *bias*, al fine di soddisfare l'art. 4, par. 1, lett. *d)* della LED e l'art. 5, par. 1, lett. *d)* del GDPR. Sul punto è stato sottolineato come l'utilizzo di dati sintetici[56] possa potenzialmente identificare le distorsioni esistenti in un campione di dati ed escluderli al fine di formare un *dataset* di qualità, realizzando dei modelli decisionali più accurati e privi di possibili pregiudizi discriminatori[57].

Oltre a tale misura tecnica, anche meccanismi organizzativi possono essere adottati per ridurre il rischio di risultati discriminatori, come la revisione manuale delle decisioni algoritmicamente assunte. Quest'ultima, nello specifico, dev'essere guidata da regole trasparenti e precise stabilite dagli Stati membri[58]. Tuttavia, la stessa revisione umana può essere fonte di criticità, rischiando di affidarsi eccessivamente all'*output* dei sistemi algoritmici con potenziali effetti distorsivi o discriminatori delle decisioni di sorveglianza e controllo adottate dalle LEA[59].

Per evitare anche questa possibilità, le autorità competenti dovrebbero documentare le loro attività di trattamento e garantire che ogni decisione venga presa sulla base di una politica chiara, prevedibile e comunicabile[60]. Inoltre, dev'essere garantita piena accessibilità ai criteri che costituiscono il parametro valutativo dell'algoritmo da parte dei soggetti interessati, con importanti implicazioni in tema di diritto di informativa e accesso[61], in mo-

Briefs, 2020, 4-5, in http://dx.doi.org/10.25330/528.

55 Cfr. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe,* op. cit., 527-528.

56 I dati sintetici sono dati generati artificialmente che riproducono fedelmente le caratteristiche e i comportamenti dei dati reali, senza però contenere informazioni sensibili. Per approfondire cfr. Finocchiaro, Landi, Polifrone, Ruffo, Torlontano, *Il futuro regolatorio dei dati sintetici, La sintetizzazione dei dati come risorsa per ricerca scientifica, innovazione e politiche pubbliche nel panorama giuridico europeo*, in *Diritto Economia e Tecnologie della Privacy*, 3, 2024, disponibile in https://zenodo.org/doi/10.5281/zenodo.12742249.

57 Cfr. Draghi, Wang, Myles, Tucker, *BayesBoost: Identifying and Handling Bias Using Synthetic Data Generators*, in *Proceedings of Machine Learning Research*, 2021, 49–62, in https://proceedings.mlr.press/v154/draghi21a/draghi21a.pdf.

58 Sul punto v. C. giust., 21 giugno 2022, causa C817/19, *Ligue des droits humains*, § 123–125 e 203-206, pronunciatasi in merito all'interpretazione della Direttiva PNR.

59 Cfr. Haitsma, *Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data*, in *Frontiers in Political Science*, 5, 2023, 8, in https://www.frontiersin.org/articles/10.3389/fpos.2023.1232601/full. Tale fenomeno è descritto come pigrizia cognitiva e si riferisce alla tendenza degli utenti a fare affidamento eccessivo su sistemi di AI per compiti cognitivi, riducendo l'impegno mentale e il pensiero critico, in base alla percezione di superiorità o inaffidabilità degli algoritmi.

60 Cfr. Pitea, Tomasi, *Art. 8 Convenzione europea dei diritti dell'uomo*, op. cit., 304-305, secondo cui le ingerenze nella vita privata delle persone siano ammesse solo a condizione che queste siano previste dalla legge e che tali basi giuridiche siano strettamente connesse al principio della certezza del diritto, garantendone l'accessibilità e la prevedibilità.

61 Il diritto ad essere informati – anche nella declinazione del diritto di accesso – dell'uso di sistemi automatizzati è fondamentale, poiché consente l'esercizio successivo di tutti gli altri diritti, come il diritto di richiedere l'accesso ai dati memorizzati. Sul punto, insiste anche la LED, il cui art. 13 (in combinato col considerandum n. 26) prescrive che le autorità hanno il dovere di informare i cittadini soggetti ai trattamenti automatizzati dell'esistenza del trattamento e dei rischi consequenziali ad esso.

do da poter identificare eventuali discriminazioni ed esercitare il loro diritto a un rimedio efficace. Di conseguenza, delle linee guida direzionali per l'utilizzo e il controllo di tali strumenti, ove rese pubbliche, permetterebbero di attestare la legittimità di azioni o interventi della polizia nell'ambito del *policing profiling*, manifestandone chiaramente presupposti, meccanismi e potenziali esiti dell'istruttoria algoritmica eventualmente condotta. La conoscenza dell'uso di un meccanismo di profilazione e del suo funzionamento potrebbe identificare e conseguentemente permettere la correzione di decisioni errate. Tali sistemi, pertanto, devono essere progettati per essere spiegabili a coloro che sono interessati dalle decisioni, assicurando la capacità di comprendere l'iter logico che ha determinato un certo risultato[62].

5. Considerazioni conclusive

I modelli predittivi sollevano gravi preoccupazioni riguardo al potenziale aggravamento di problemi esistenti come la discriminazione. Il caso di profilazione razziale riscontrato dalla Corte EDU solleva poi ulteriori apprensioni su come ancora le LEA si affidino a pregiudizi etnici per lo svolgimento di attività come i controlli di identità, circostanza che comporta anche il trattamento dei relativi dati. A fronte di tale sovraesposizione alle attività di verifica e controllo, desta particolare preoccupazione l'eccessiva rappresentazione di gruppi minoritari nei *dataset* rappresentanti atti potenzialmente criminali utilizzati per l'addestramento di modelli di *policing profiling*, con conseguente esacerbazione della marginalizzazione di tali gruppi vulnerabili.
Dei molti regimi giuridici applicabili in un contesto di intelligenza artificiale, la legge sulla non-discriminazione e la disciplina sulla protezione dei dati sono le due fonti normative più rilevanti per proteggere gli individui contro ipotesi di profilazione razziale, algoritmica o non. In particolare, nel contesto dell'Ue – ma anche in Svizzera a fronte del proprio adattamento alla normativa dell'Unione – proprio con riguardo al GDPR e alla LED, il principio cardine che permette di racchiudere tutte le misure per prevenire e contrastare possibili discriminazioni è rappresentato dal principio di correttezza e trasparenza. Il trattamento di dati personali condotto dalle LEA dovrebbe avvenire, pertanto, nel modo che gli individui – pienamente informati – possono ragionevolmente aspettarsi, perseguendo unicamente i fini previsti dalla legge, e senza che questo possa cagionare ingiustificatamente degli effetti sfavorevoli alle persone[63].

[62] Cfr. European Union Agency for Fundamental Rights, *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, 2020, 13, in https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights.

[63] Cfr. Pastaltzidis, Dimitriou, Quezada-Tavárez, Aidinlis, Marquenie, Gurzawska, Tzovaras, *Data augmentation for fairness-aware machine learning: Preventing algorithmic bias in law enforcement systems*, in *ACM Conference on Fairness, Accountability, and Transparency*, 2022, 2305, in https://doi.org/10.1145/3531146.3534644

In conclusione, si rileva come appaia inevitabile che, in un tempo non troppo remoto, il *policing profiling* diverrà strumento ordinario di indagine di attività criminose. Tuttavia, a fronte dei rischi che questa tecnologia solleva – rispetto alla violazione dei diritti e libertà fondamentali sin qui esaminati – appare necessario adottare una regolamentazione specifica in materia. Tali politiche dovrebbero includere una stretta collaborazione tra agenzie operanti nell'ambito del rispetto dei diritti umani, oltre che esperti, accademici e/o giuristi, e i diversi professionisti coinvolti nel settore della *digital trasformation*, al fine di ridurre al minimo gli errori degli algoritmi e assicurare un controllo umano sui risultati di tale tecnologia[64]. Sul punto, si segnala, infine, che il Regolamento Ue 2024/1689 sull'intelligenza artificiale ("AI Act") ricomprende tra le pratiche di AI vietate i sistemi adoperati dalle LEA al fine di valutare o prevedere la probabilità che una persona fisica possa commettere un reato, unicamente sulla base della profilazione di un individuo o della valutazione dei tratti e delle caratteristiche della personalità. Tale divieto, comunque, non si estende ai sistemi di AI utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi ad un atto criminale, subordinandolo all'adozione di garanzie adeguate[65].

[64] Cfr. Dushi, *The use of facial recognition technology in EU law enforcement*, op. cit., 9.

[65] Cfr. art. 4, par. 1, lett. *d)* AI Act. Il Regolamento, dopo essere stato approvato dal Parlamento europeo il 13 marzo 2024 e dal Consiglio il 21 maggio 2024, è stato pubblicato sulla G.U.U.E. il 12 luglio 2024. Il testo del Regolamento è consultabile in: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.