PODRĘCZNIK

Zapobieganie niezgodnemu z prawem profilowaniu obecnie i w przyszłości: przewodnik

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Wiele informacji na temat Agencji Praw Podstawowych Unii Europejskiej jest dostępnych w internecie. Można do nich dotrzeć poprzez stronę internetową FRA: fra.europa.eu.

Europe Direct to serwis, który pomoże Państwu znaleźć odpowiedzi na pytania dotyczące Unii Europejskiej.

Numer bezpłatnej infolinii (*):

00 800 6 7 8 9 10 11

(*) Informacje są udzielane nieodpłatnie, większość połączeń również jest bezpłatna (niektórzy operatorzy, hotele lub telefony publiczne mogą naliczać opłaty).

Zdjęcia (okładka i wnętrze przewodnika, od lewej do prawej): © stock.adobe.com-Savvapanf

Więcej informacji o Unii Europejskiej można znaleźć w internecie (http://europa.eu).

Luksemburg: Urząd Publikacji Unii Europejskiej, 2019

Print:	ISBN 978-92-9474-746-4	doi:10.2811/285269	TK-06-18-031-PL-C
PDF:	ISBN 978-92-9474-749-5	doi:10.2811/97776	TK-06-18-031-PL-N

© Agencja Praw Podstawowych Unii Europejskiej, 2019

Powielanie dozwolone pod warunkiem podania źródła. W celu wykorzystywania lub powielania zdjęć lub innych materiałów nieobjętych prawami autorskimi FRA należy zwrócić się o pozwolenie bezpośrednio do właścicieli praw autorskich.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Zapobieganie niezgodnemu z prawem profilowaniu obecnie i w przyszłości: przewodnik

Spis treści

RYSUNKI I TABELE 4
AKRONIMY I SKRÓTY 5
WPROWADZENIE 7
PODSUMOWANIE GŁÓWNYCH KWESTII 11
1 KONTEKST: CZYM JEST PROFILOWANIE? 15
1.1. Definicja profilowania 15
1.1.1. Profilowanie w kontekście ścigania przestępstw i zarządzania granicami 18
1.1.2. Definicja profilowania z wykorzystaniem algorytmu 19
1.2. Kiedy profilowanie jest niezgodne z prawem? 24
1.2.1. Zakaz dyskryminacji 25
1.2.2. Prawo do poszanowania życia prywatnego i ochrona danych osobowych 33
1.3. Jakie potencjalne negatywne konsekwencje ma niezgodne z prawem profilowanie w przypadku ścigania przestępstw i zarządzania granicami? 41
1.3.1. Wpływ na zaufanie do policji i do organów zarządzania granicami oraz dobre stosunki ze społecznością 42
1.3.2. Skuteczność profilowania 53
2 ZGODNE Z PRAWEM PROFILOWANIE: ZASADA I PRAKTYKA 57
2.1. Poszanowanie godności osoby 59
2.2. Rozsądne i obiektywne podstawy 63
2.2.1. Unikanie uprzedzeń 64
2.2.2. Jasne wytyczne dla funkcjonariuszy 65
2.2.3. Ukierunkowane szkolenie 66
2.2.4. Rozsądne podstawy do podejrzeń: wykorzystywanie danych wywiadowczych i uzyskanych informacji 73
2.2.5. Formularze zatrzymania i rewizji w odniesieniu do profilowania przez organy ścigania 82
2.3. Odpowiedzialność 86
2.3.1. Monitorowanie wewnętrzne 89
2.3.2. Kamery nasobne 93
2.3.3. Mechanizmy wnoszenia skarg 100
3 PROFILOWANIE Z WYKORZYSTANIEM ALGORYTMU 107
3.1. Ramy ochrony danych regulujące profilowanie z wykorzystaniem algorytmu 111
3.1.1. Przetwarzanie danych musi się odbywać w określonym celu 112
3.1.2. Należy informować osoby fizyczne 115
3.1.3. Bezpieczne przechowywanie danych: rejestry, ewidencje i zasady przechowywania 117
3.1.4. Należy wykrywać niezgodne z prawem przetwarzanie i zapobiegać mu 118
3.2. Wielkoskalowe bazy danych do celów zarządzania granicami i bezpieczeństwa 123
3.2.1. Minimalizowanie zagrożenia dla praw podstawowych podczas przetwarzania danych w wielkoskalowych bazach danych 127
WNIOSEK 132
ZAŁĄCZNIK 133
ŹRÓDŁA 135

Rysunki i tabele

Tabela 1: Cechy działań policji opartych na szczegółowych danych wywiadowczych i opartych na prognozowaniu 19
Tabela 2: Wymogi w zakresie ochrony danych – różnice między dyrektywą dotyczącą policji a RODO 36
Tabela 3: Rodzaje i cechy wytycznych i zaangażowanie zainteresowanych stron 65
Tabela 4: Określenie odpowiednich ram prawnych w zależności od celu przetwarzania 113
Tabela 5: Obowiązek przekazania osobie fizycznej informacji na temat profilowania: rodzaj danych, środki komunikacji i wyjątki 115
Tabela 6: Wybrane instrumenty UE wymagające przetwarzania dużych ilości danych do celów zarządzania granicami i ścigania przestępstw 124
Tabela 7: Istniejące lub planowane wielkoskalowe unijne systemy informatyczne 133

Wykres 1: Proces profilowania z wykorzystaniem algorytmu w kontekście ścigania przestępstw i zarządzania granicami 21
Wykres 2: Naruszenie prawa do prywatności i do ochrony danych – proces oceny 39
Wykres 3: Ostatnie zatrzymania przez policję postrzegane jako profilowanie etniczne wśród osób zatrzymanych w ciągu ostatnich pięciu lat przed przeprowadzeniem badania EU-MIDIS II, według państw członkowskich i grup, których dotyczyło badanie (%) 47
Wykres 4: Cykl samospełniającej się przepowiedni 52
Wykres 5: Trzy elementy spotkania przeprowadzonego z zachowaniem szacunku 61
Wykres 6: Proces i cele opracowywania ukierunkowanego szkolenia 67
Wykres 7: Wskaźniki uznane za pomocne lub bardzo pomocne w skutecznym rozpoznawaniu osób starających się nielegalnie przekroczyć granicę państwa przed przeprowadzeniem rozmowy z funkcjonariuszem (%) 75
Wykres 8: Łączenie elementów 80
Wykres 9: Elementy niedyskryminacyjnego profilowania 81
Wykres 10: Elementy monitorowania wewnętrznego 91
Wykres 11: Narzędzie online przedstawiające szczegółowe informacje na temat działań zatrzymania i rewizji prowadzonych w Londynie 95
Wykres 12: Przegląd mechanizmów wnoszenia skarg w państwach członkowskich UE 101
Wykres 13: Minimalne wymogi oceny skutków 121

Akronimy i skróty

CCC	wspólny podstawowy program szkoleń
DPIA	ocena skutków dla ochrony danych
EES	system wjazdu/wyjazdu
EIOD	Europejski Inspektor Ochrony Danych
EKPC	Europejska konwencja praw człowieka
ENISA	Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji
ETIAS	europejski system informacji o podróży oraz zezwoleń na podróż
ETPC	Europejski Trybunał Praw Człowieka
EU-MIDIS	badanie Unii Europejskiej na temat mniejszości i dyskryminacji
FRA	Agencja Praw Podstawowych Unii Europejskiej
Frontex	Europejska Agencja Straży Granicznej i Przybrzeżnej
IT	technologie informacyjne
OBWE	Organizacja Bezpieczeństwa i Współpracy w Europie
OHCHR	Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka
ONZ	Organizacja Narodów Zjednoczonych
RODO	ogólne rozporządzenie o ochronie danych
SIS II	System Informacyjny Schengen
TCN	obywatel państwa trzeciego
TSUE	Trybunał Sprawiedliwości Unii Europejskiej
UE	Unia Europejska
UNHRC	Rada Praw Człowieka
VIS	wizowy system informacyjny
WP29	Grupa Robocza Art. 29

Wprowadzenie

Rozwój technologiczny przyczynił się do zwiększonego wykorzystywania profilowania w szerokim zakresie kontekstów, w tym w kontekście marketingu, zatrudnienia, zdrowia, finansów, ścigania przestępstw, kontroli granicznej i bezpieczeństwa. W ostatnich latach państwa członkowskie UE poświęcają więcej uwagi kwestii wykorzystywania narzędzi profilowania do celów wspierania pracy organów ścigania i funkcjonariuszy zarządzania granicami. Przedstawiciele organów ścigania i straż graniczna powszechnie korzystają z profilowania zgodnie z prawem w celu zapobiegania przestępstwom oraz prowadzenia dochodzeń i ścigania przestępstw, a także w celu zapobiegania i wykrywania nielegalnej imigracji. Niezgodne z prawem profilowanie może jednak podważać zaufanie do organów, w szczególności do policji, i stygmatyzować niektóre społeczności. To z kolei może prowadzić do eskalacji napięcia między społecznościami a organami ścigania ze względu na zjawisko postrzegane jako dyskryminacyjne wykorzystywanie profilowania.

W niniejszym przewodniku wyjaśniono, czym jest profilowanie, jakie ramy prawne je regulują oraz dlaczego prowadzenie profilowania w sposób zgodny z prawem jest nie tylko konieczne, aby przestrzegać praw podstawowych, lecz także kluczowe do prowadzenia skutecznych działań policji i skutecznego zarządzania granicami. W przewodniku zawarto również praktyczne wytyczne dotyczące sposobu unikania niezgodnego z prawem profilowania podczas operacji policyjnych i zarządzania granicami. Zawarte w przewodniku zasady i praktyki poparto przykładami, analizami przykładów i orzecznictwem z UE i spoza jej granic.

Dlaczego niniejszy przewodnik jest potrzebny?

Profilowanie wzbudza szereg obaw dotyczących praw podstawowych[1]. Niektóre praktyki w zakresie profilowania niosą ryzyko naruszenia ugruntowanych zasad prawnych, w tym równości i niedyskryminacji, oraz praw do poszanowania życia prywatnego i ochrony danych osobowych. Ponadto podnosi się kwestie dotyczące jego skuteczności w zwalczaniu nielegalnych działań, a także możliwych negatywnych konsekwencji w relacjach między organami (w tym policją i organami zarządzania granicami) a społecznościami, którym organy te służą.

W odpowiedzi na te obawy Agencja Praw Podstawowych Unii Europejskiej (FRA) opublikowała w 2010 r. przewodnik zatytułowany *Podniesienie skuteczności działań policji – Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu*. W przewodniku tym, skupiającym się na wykorzystywaniu profilowania przez policję, skoncentrowano się w szczególności na wykonywaniu uprawnień w zakresie zatrzymywania i rewizji. Przewodnik miał na celu dostarczenie funkcjonariuszom średniego szczebla narzędzi pozwalających uniknąć dyskryminacyjnego profilowania opartego na pochodzeniu etnicznym.

Rozwój technologiczny, jaki miał miejsce od tamtego momentu, istotnie zmienił charakter profilowania. Znaczna część profilowania opiera się aktualnie na wynikach komputerowej analizy dużych zbiorów danych. Z prawnego punktu widzenia zmienione – bardziej restrykcyjne – przepisy w zakresie ochrony danych obowiązujące w UE od maja 2018 r. określiły nowe standardy gromadzenia, analizy i wykorzystywania danych osobowych.

W niniejszym zaktualizowanym przewodniku uwzględniono te istotne zmiany, aby opierając się na przewodniku z 2010 r. i rozszerzając go, odzwierciedlić nową prawną i praktyczną rzeczywistość. Zastosowano w nim bardziej kompleksowe podejście do niezgodnego z prawem profilowania, włączając:

- profilowanie w kontekście zarządzania granicami;
- dyskryminacyjne profilowanie, które oprócz pochodzenia etnicznego uwzględnia wszystkie inne podstawy, w tym narodowość, wiek i płeć; oraz
- profilowanie z wykorzystaniem algorytmów lub komputerów.

Niniejsza wersja z 2018 r. zawiera również nowe przykłady i analizy przykładów mające na celu odzwierciedlenie zmian i innowacji dotyczących profilowania.

1 Zob. FRA (2018e), s. 85–87; FRA (2017c), s. 88–89; oraz FRA (2016), s. 83–85.

Do kogo skierowany jest niniejszy przewodnik?

Niniejszy przewodnik opracowano przede wszystkim dla osób odpowiedzialnych za szkolenie funkcjonariuszy organów ścigania i zarządzania granicami. Może on również służyć bezpośredniemu wsparciu funkcjonariuszy średniego szczebla w zgodnym z prawem wdrażaniu technik profilowania. Ma przyczynić się do lepszego zrozumienia profilowania w teorii i w praktyce oraz zilustrować na konkretnych przykładach, w jaki sposób można prowadzić profilowanie, przestrzegając praw podstawowych.

Niniejszy przewodnik obejmuje profilowanie wykonywane przez funkcjonariuszy policji pierwszej linii kontroli – np. podczas zatrzymania i rewizji – oraz kontrole powadzone przez straż graniczną na przejściach granicznych, a konkretnie w momencie podejmowania decyzji o skierowaniu osoby do dokładniejszej kontroli drugiej linii. W kontekście zarządzania granicami stanowi on pomoc szkoleniową dla osób prowadzących szkolenia dla straży granicznej uwzględniające wspólny podstawowy program szkoleń na podstawie art. 36 ust. 5 rozporządzenia w sprawie Europejskiej Straży Granicznej i Przybrzeżnej (rozporządzenia (UE) 2016/1624).

W przewodniku omówiono również profilowanie na podstawie analizy dużych zbiorów danych, w tym podlegających regulacjom prawa Unii. Profilowanie w innych sytuacjach, np. prowadzone w sektorze prywatnym do celów handlowych, nie jest objęte zakresem niniejszego przewodnika. FRA prowadzi dalsze badania na ten temat[2].

Jak korzystać z niniejszego przewodnika?

W niniejszym przewodniku przedstawiono przegląd głównych zasad i praktyk dotyczących profilowania w kontekście ścigania przestępstw i zarządzania granicami. Można go odczytywać jako całość lub wykorzystywać jako źródło odniesienia wspierające działania szkoleniowe.

Przewodnik zawiera trzy rozdziały. W rozdziale 1 wyjaśniono pojęcie profilowania, wskazano, kiedy profilowanie staje się niezgodne z prawem, i opisano jego możliwy negatywny wpływ na osoby fizyczne, społeczności oraz na wykonywanie uprawnień w ramach działań policyjnych i związanych z zarządzaniem granicami. W rozdziale 2 wyszczególniono zasady i praktyki, którymi powinni kierować się funkcjonariusze organów ścigania i straży granicznej przy realizacji zgodnych

2 Zob. projekt FRA Artificial Intelligence, Big Data and Fundamental Rights.

z prawem działań w zakresie profilowania. W rozdziale 3 skupiono się na profilowaniu z wykorzystaniem algorytmów. Ponieważ praktyki w tym obszarze nie są bardzo rozwinięte, sekcja ta zawiera mniej konkretnych przykładów. Przedstawiono w niej natomiast główne zagrożenia dla praw podstawowych związane z profilowaniem z wykorzystaniem komputerów oraz określono główne wymogi prawne ustanowione w ogólnym rozporządzeniu o ochronie danych (RODO) i w dyrektywie dotyczącej policji.

Różne kwestie poruszone w przewodniku zilustrowano za pomocą elementów wizualnych. W żółtych oknach wyróżniono kluczowe kwestie podsumowujące główne informacje. W jasnoniebieskich oknach wyróżniono podstawowe aspekty ram prawnych, a w zielonych oknach przedstawiono praktyczne przykłady. W innych oknach wyróżniono ważne kwestie, na których należy się skupić, analizy przykładów i przykłady orzecznictwa. Pomimo starań o zróżnicowanie analiz przykładów nieproporcjonalna liczba przykładów dotyczy Zjednoczonego Królestwa. Wynika to z faktu, że Zjednoczone Królestwo zajmowało się kwestią niezgodnego z prawem profilowania od lat 80., a w innych państwach zaczęto poruszać ten problem później. Oznacza to, że Zjednoczone Królestwo opracowało w tej dziedzinie obszerne i ugruntowane polityki i praktyki, z których można czerpać przykłady.

W jaki sposób opracowano niniejszy przewodnik?

FRA zorganizowało spotkanie z ekspertami z różnych dziedzin, aby omówić wstępny zarys przewodnika oraz aby skorzystać z ich pomocy przy stworzeniu produktu końcowego.

W tym względzie FRA pragnie podziękować ekspertom z Biura Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka (OHCHR), Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex), Biura Instytucji Demokratycznych i Praw Człowieka (ODIHR), Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), Amnesty International, Europejskiej Sieci przeciwko Rasizmowi (European Network Against Racism, ENAR), Międzynarodowego Ośrodka Rozwoju Polityki Migracyjnej (International Centre for Migration Policy Development, ICMPD), FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, European Digital Rights, Open Society Initiative for Europe oraz przedstawicielom francuskiego rzecznika praw obywatelskich, niderlandzkich, duńskich i austriackich organów policyjnych oraz polskiej straży granicznej za ich wartościowy wkład w opracowanie niniejszego przewodnika.

Podsumowanie głównych kwestii

1. Cechy chronione nigdy nie mogą stanowić jedynej podstawy profilowania

- Profilowanie obejmuje **kategoryzowanie osób** według ich cech.
- W celu gromadzenia i przetwarzania **danych osobowych** organy ścigania i organy zarządzania granicami muszą zapewnić, aby gromadzenie i przetwarzanie danych miały podstawy prawne, ważny i prawnie uzasadniony cel oraz aby były niezbędne i proporcjonalne.
- **Cechy chronione**, takie jak rasa, pochodzenie etniczne, płeć lub religia, mogą znaleźć się wśród czynników uwzględnianych przez organy ścigania i straż graniczną w celu wykonywania swoich uprawnień, **nie mogą one jednak stanowić jedynego lub głównego powodu wyróżnienia osoby**. (Aby uzyskać więcej informacji na temat „cech chronionych", zob. sekcja 1.2.1).
- Profilowanie, które opiera się wyłącznie lub głównie na co najmniej jednej cesze chronionej, jest równoznaczne z bezpośrednią dyskryminacją, **narusza zatem prawa i wolności jednostki** i jest **niezgodne z prawem**.

2. Podczas każdego kontaktu z osobą fizyczną należy okazać szacunek, profesjonalizm i chęć udzielenia informacji

- Sama **dobra jakość kontaktu** nie wyeliminuje profilowania opartego na uprzedzeniach, istnieje jednak większe prawdopodobieństwo, że kontakt taki będzie bardziej udany, a możliwe negatywne skutki zatrzymania przez funkcjonariusza policji lub straży granicznej będą mniejsze. W odniesieniu do zarządzania granicami zachowanie okazujące profesjonalizm i szacunek wyraźnie traktuje się jako obowiązek prawny.
- **Zachowanie okazujące profesjonalizm i szacunek** zwiększa co do zasady zadowolenie osoby związane ze spotkaniem.
- **Wyjaśnienie osobie powodów zatrzymania** pomaga w zwiększeniu zaufania społecznego względem operacji prowadzonych przez policję i organy zarządzania granicami oraz ogranicza postrzeganie profilowania jako opartego na uprzedzeniach.
- Szacunek i uprzejmość **nie mogą jednak nigdy stanowić uzasadnienia dla niezgodnych z prawem kontroli granicznych i działań zatrzymania i rewizji**.

3. Profilowanie powinno mieć obiektywne i uzasadnione podstawy

- Aby zatrzymanie i skierowanie do kontroli drugiej linii było zgodne z prawem, muszą **istnieć uzasadnione i obiektywne podstawy** podejrzeń.
- Cechy indywidualne można stosować jako zgodne z prawem czynniki na potrzeby profilowania. Aby można jednak było uniknąć stosowania dyskryminacji, **musi *również* istnieć uzasadniona podstawa podejrzeń** oparta na innych informacjach niż cechy chronione.
- Gdy ściganie przestępstw i prowadzenie działań związanych z zarządzaniem granicami odbywa się w oparciu o **określone i aktualne dane wywiadowcze**, ma ono większe szanse na bycie **obiektywnym**.
- Istotne jest, aby decyzja o zatrzymaniu lub skierowaniu osoby do kontroli drugiej linii **nie opierała się wyłącznie na *przeczuciu* funkcjonariusza** co do tej osoby, gdyż istnieje wtedy ryzyko, że decyzja taka będzie się opierać się na stronniczości, stereotypach lub uprzedzeniach.

4. Niezgodne z prawem profilowanie ma negatywny wpływ na prowadzenie działań przez policję i na zarządzanie granicami

- **Niezgodne z prawem profilowanie podważa zaufanie do policji i straży granicznej**. Może ono spowodować pogorszenie stosunków między policją/strażą graniczną a członkami mniejszości i innych społeczności, którzy mogą czuć się wyodrębnieni. Takie poczucie niesprawiedliwości może prowadzić do utraty zaufania do policji i innych organów przez niektóre osoby fizyczne i grupy, co może skutkować rzadszym zgłaszaniem przestępstw policji i ograniczoną współpracą z organami. Organy mogą natomiast postrzegać niektóre grupy z podejrzliwością, przez co praktyki niezgodnego z prawem profilowania mogą się stać częstsze.
- **Niezgodne z prawem profilowanie podważa skuteczność samego profilowania**, gdyż współczynnik zatrzymywania osób przez policję albo na granicy niekoniecznie odpowiada wskaźnikom występowania naruszeń wśród poszczególnych grup.
- Istnieje ryzyko wystąpienia **samospełniającej się przepowiedni**, jeżeli policja lub funkcjonariusze zajmujący się zarządzaniem granicami ukierunkowują swoje działania na mniejszości, co skutkuje wyższą liczbą aresztowań i kontroli na granicy.

5. Niezgodne z prawem profilowanie pociąga za sobą konsekwencje prawne i finansowe, za które odpowiedzialni są funkcjonariusze

- Organy ścigania i funkcjonariusze zajmujący się zarządzaniem granicami są **odpowiedzialni** za to, aby profilowanie odbywało się zgodnie z prawem.
- **Gromadzenie rzetelnych, dokładnych i aktualnych danych** jest kluczowe dla zapewnienia takiej odpowiedzialności.
- **Skuteczne mechanizmy wnoszenia skarg** mogą zarówno zwalczać nadużycia, jak i pomagać w zabezpieczeniu i odbudowaniu zaufania względem operacji prowadzonych przez policję i organy zarządzania granicami.
- **Spotkania z członkami społeczeństwa mające na celu uzyskanie informacji zwrotnych** – słuchanie ich opinii, omawianie kwestii profilowania i gromadzenie informacji zwrotnych na temat operacji – dają sposobność wyciągnięcia istotnych wniosków i poprawy działań związanych z profilowaniem.

6. Profilowanie z wykorzystaniem algorytmu wymaga stosowania określonych zabezpieczeń ochrony danych

- Przy opracowywaniu i stosowaniu profilowania z wykorzystaniem algorytmu wprowadzenie **uprzedzeń** może nastąpić na każdym etapie procesu. Aby uniknąć takiej sytuacji oraz kolejnych potencjalnych naruszeń praw podstawowych, zarówno **specjaliści w dziedzinie informatyki, jak i funkcjonariusze zajmujący się interpretacją danych powinni w pełni rozumieć prawa podstawowe**.
- Niezwykle istotne jest korzystanie z **rzetelnych danych**. Wprowadzanie do algorytmu danych, które odzwierciedlają uprzedzenia lub pochodzą z nierzetelnych źródeł, przyniesie nieobiektywne i nierzetelne wyniki.
- Profilowanie z wykorzystaniem algorytmu musi być **zgodne z prawem, konieczne** i **proporcjonalne**.
- Przetwarzanie danych musi służyć **konkretnemu celowi**.
- Osoby fizyczne mają **prawo zostać poinformowane** poprzez otrzymanie informacji na temat danych osobowych, które są gromadzone i przechowywane, przetwarzania tych danych i celu takiego przetwarzania, oraz przysługujących im praw.
- Dane należy **gromadzić, przetwarzać i przechowywać w bezpieczny sposób**. Oczekuje się, że organy będą prowadziły rejestr działań obejmujących przetwarzanie danych (w tym rodzaju operacji wykonywanych na danych) i związanych z nimi logów (w tym informacji dotyczących osoby lub osób uzyskujących dostęp o danych).
- Należy **zapobiegać** niezgodnemu z prawem przetwarzaniu danych i **wykrywać je**: 1) prowadząc wcześniej ocenę skutków; oraz 2) stosując narzędzia ochrony prywatności wbudowane w algorytm już na etapie projektowania.

Przydatne strony internetowe

Unia Europejska
Trybunał Sprawiedliwości Unii Europejskiej (TSUE): http://www.curia.eu
Przepisy UE: http://eur-lex.europa.eu/
Agencja Praw Podstawowych Unii Europejskiej (FRA): http://www.fra.europa.eu
Parlament Europejski: http://www.europarl.europa.eu

Rada Europy
Komitet Ministrów Rady Europy: http://www.coe.int/cm
Europejski Trybunał Praw Człowieka: http://www.echr.coe.int

Organizacja Narodów Zjednoczonych
Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka (OHCHR): http://www.ohchr.org

Walka z dyskryminacją
Europejska Komisja przeciwko Rasizmowi i Nietolerancji (ECRI): http://www.coe.int/ecri
Europejska sieć organów ds. równości (Equinet): http://www.equineteurope.org/
Krajowe organy ds. równości: http://www.archive.equineteurope.org/-Equinet-Members-

Ochrona danych
Europejski Inspektor Ochrony Danych (EIOD): https://edps.europa.eu/
Europejska Rada Ochrony Danych (EROD): https://edpb.europa.eu
Krajowe organy ochrony danych: https://edpb.europa.eu/about-edpb/board/members_pl

Ściganie przestępstw
Sieć niezależnych organów rozpatrujących skargi na policję (Independent Police Complaints Authorities' Network, IPCAN): https://ipcan.org/
Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL): https://www.cepol.europa.eu/
Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (EUROPOL): https://www.europol.europa.eu/

Zarządzanie granicami
Europejska Agencja Straży Granicznej i Przybrzeżnej (FRONTEX): https://frontex.europa.eu/
Europejski Urząd Wsparcia w dziedzinie Azylu (EASO): https://www.easo.europa.eu/

Wielkoskalowe bazy danych
Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA): https://www.eulisa.europa.eu/

1 Kontekst: Czym jest profilowanie?

W niniejszym rozdziale opisano, co rozumiemy pod pojęciem profilowania, i wyjaśniono główne prawa podstawowe, na które może mieć ono wpływ. Przedstawiono profilowanie w kontekście działań związanych ze ściganiem przestępstw i zarządzaniem granicami, przyglądając się trzem podstawowym elementom:

- koncepcji profilowania i jego stosowania przez organy ścigania i organy zajmujące się zarządzaniem granicami. W sekcji tej przedstawiono także kilka różnych rodzajów profilowania;
- głównym zasadom z zakresu praw podstawowych, których należy przestrzegać, aby profilowanie było prowadzone w sposób zgodny z prawem, mianowicie niedyskryminacji i prawom do poszanowania życia prywatnego i do ochrony danych;
- potencjalnemu negatywnemu wpływowi profilowania, w tym możliwym konsekwencjom dla osób fizycznych i konsekwencjom dotyczącym stosunków ze społecznościami, oraz zaufaniu do policji i do organów zarządzania granicami.

1.1. Definicja profilowania

Profilowanie obejmuje **kategoryzowanie osób** według ich cech osobowych. Cechy te mogą być „niezmienne" (np. wiek lub wzrost) lub „zmienne" (np. ubiór, zwyczaje, upodobania i inne elementy zachowania). Profilowanie obejmuje eksplorację danych, w ramach której poszczególne osoby kategoryzuje się **„na podstawie ich niektórych obserwowalnych cech, aby móc wywnioskować,**

z zachowaniem pewnego marginesu błędu, inne cechy, które nie są możliwe do zaobserwowania"[3].

Najważniejsze kwestie

- Profilowanie obejmuje **kategoryzowanie osób** według ich wydedukowanych cech osobowych.
- Istnieją dwa główne cele profilowania w kontekście ścigania przestępstw i zarządzania granicami: **identyfikacja znanych osób na podstawie danych wywiadowczych dotyczących konkretnej osoby** oraz jako **metoda prognozowania** pozwalająca na identyfikację „nieznanych" osób, które mogą interesować organy ścigania i organy zarządzania granicami. W przypadku obu celów można ulec świadomym lub nieświadomym uprzedzeniom, które mogą być dyskryminujące względem danych osób.
- Na działania profilowania prowadzone przez straż graniczną i organy ścigania mogą wpływać uprzedzenia wynikające z ich własnych doświadczeń albo z doświadczeń instytucji. Uprzedzenia te mogą stać się podstawą oceny dotyczącej profilowania i wpływać na nią, oddziałując zarówno na legalność, jak i skuteczność działań policji.
- Stereotypy mogą odzwierciedlać pewną prawdę statystyczną. Nawet w takich przypadkach są one jednak **problematyczne**, jeżeli w rezultacie daną osobę traktuje się jako członka grupy, nie zaś indywidualnie, na podstawie jej osobistej sytuacji.
- Przy opracowywaniu i stosowaniu profilowania z wykorzystaniem algorytmu wprowadzenie **uprzedzeń może nastąpić na każdym etapie procesu**. Aby uniknąć tych oraz kolejnych potencjalnych naruszeń praw podstawowych, zarówno specjaliści w dziedzinie informatyki opracowujący algorytmy, jak i funkcjonariusze zajmujący się gromadzeniem i interpretacją danych powinni w pełni rozumieć prawa podstawowe oraz sposoby ich stosowania w tym kontekście.

Praktyki profilowania stosuje się w celu:

- tworzenia wiedzy dzięki analizowaniu istniejących danych, aby sformułować założenia na temat danej osoby. Wykorzystuje się tutaj wcześniejsze doświadczenia i analizę statystyczną, aby ustalić korelacje między niektórymi cechami a konkretnymi wynikami lub konkretnym zachowaniem;

- wspierania procesów decyzyjnych dzięki wykorzystywaniu tych korelacji do podejmowania decyzji dotyczących podejmowanych działań.

3 Dinant J.M., Lazaro C., Poullet Y., Lefever N. i Rouvroy A. (2008), s. 3.

Sprawia to, że profilowanie jest skutecznym narzędziem dla organów ścigania i straży granicznej. Jego stosowanie wiąże się jednak z pewnymi istotnymi zagrożeniami:

- profilowanie ustala ogólne korelacje, które mogą nie być prawdziwe w przypadku każdej osoby. Każda z osób może być „wyjątkiem od reguły";
- profile mogą tworzyć nieprawidłowe korelacje, zarówno dotyczące poszczególnych osób, jak i grup;
- profile mogą budować szkodliwe stereotypy i prowadzić do dyskryminacji;
- niektóre stereotypy mogą odzwierciedlać pewną prawdę statystyczną. Nawet w takich przypadkach stereotypy są jednak problematyczne, jeżeli w rezultacie daną osobę traktuje się jako członka grupy, nie zaś jako jednostkę.

Przykłady

Potencjalnie błędne profilowanie

Założenie, że „kobiety żyją dłużej niż mężczyźni", jest poparte merytorycznymi badaniami; którykolwiek konkretny mężczyzna może jednak żyć dłużej niż którakolwiek konkretna kobieta. W związku z tym podejmowanie jakiejkolwiek decyzji dotyczącej kobiety na podstawie tego założenia niesie ze sobą ryzyko, że decyzja ta będzie błędna w tym szczególnym przypadku i byłaby prawidłowa wyłącznie w ujęciu uśrednionym.

Niektórzy mogą pozwalać rodzinie lub przyjaciołom korzystać z ich samochodu, sprawiając, że profil ryzykownych zachowań na drodze opierający się na właścicielu samochodu będzie błędny.

1.1.1. Profilowanie w kontekście ścigania przestępstw i zarządzania granicami

Przedstawiciele organów ścigania i straż graniczna powszechnie i zgodnie z prawem korzystają z profilowania w celu zapobiegania przestępstwom oraz prowadzenia dochodzeń i ścigania przestępstw, a także w celu zapobiegania i wykrywania nielegalnej imigracji.

Profilowanie oznacza „dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się”[4]. Wyniki takiego przetwarzania danych stosuje się w celu ukierunkowania działań z zakresu zarządzania granicami i ścigania przestępstw, takich jak zatrzymanie i rewizja, aresztowania, odmowa dostępu do niektórych obszarów lub skierowanie na granicy do dokładniejszej kontroli drugiej linii. Istnieją dwa główne zastosowania profilowania:

- identyfikacja osób w oparciu o szczegółowe dane wywiadowcze. Stosuje się tutaj profil obejmujący listę cech konkretnych podejrzanych opartą na zgromadzonych dowodach dotyczących konkretnego zdarzenia;

- jako metoda prognozowania służąca identyfikacji „nieznanych” osób, które mogą interesować organy ścigania i zarządzania granicami. Opiera się ona na analizie danych i założeniach sformułowanych na podstawie informacji wynikających z doświadczenia. Najlepiej, gdyby metody prognozowania skupiały się na zachowaniu. W praktyce skupiają się one jednak nie (lub nie tylko) na zachowaniu, lecz na widocznych cechach fizycznych, takich jak wiek, płeć lub pochodzenie etniczne.

W tabeli 1 przedstawiono porównanie kluczowych cech wspomnianych dwóch rodzajów profilowania w kontekście działań policji.

4 Artykuł 3 pkt 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 (dyrektywa dotycząca policji).

Tabela 1: Cechy działań policji opartych na szczegółowych danych wywiadowczych i opartych na prognozowaniu

	Działania policji oparte na szczegółowych danych wywiadowczych	Działania policji oparte na prognozowaniu
Kontekst	Popełniono przestępstwo lub wydano wpis dotyczący konkretnej osoby	Nie popełniono żadnego przestępstwa ani nie wydano żadnego wpisu dotyczącego konkretnej osoby
Podejście	Reaktywne	Proaktywne
Cel	Zatrzymać podejrzanego lub podejrzanych	Przewidzieć miejsce i czas, w których może dojść do przestępstwa, lub przewidzieć, kto może starać się nielegalnie przekroczyć granicę państwa
Wykorzystywane dane	Szczegółowe dane wywiadowcze związane ze sprawą („profil osoby")	Ogólne dane wywiadowcze związane z kilkoma sprawami
Rodzaj procesu	Połączenie procesów opartych na danych i prowadzonych przez człowieka	Główne procesy oparte na danych („analiza ryzyka")

Źródło: FRA, 2018.

Oba rodzaje profilowania mogą być niezgodne z prawem, jeżeli podczas ich wykonywania nie są stosowane odpowiednie środki ochronne obejmujące określony cel i uzasadnienie profilowania. W rozdziale 2 i rozdziale 3 przedstawiono praktyczne informacje o tym, w jaki sposób zapewnić, aby profilowanie było zgodne zarówno z przepisami, jak i z prawami człowieka.

1.1.2. Definicja profilowania z wykorzystaniem algorytmu

Szybki rozwój technologiczny sprawia, że profilowanie w coraz większym stopniu opiera się na wykorzystywaniu danych przechowywanych w bazach danych i systemach informatycznych (systemach IT). W profilowaniu z wykorzystaniem algorytmu stosuje się różne techniki, aby uzyskać profil osoby na podstawie korelacji danych i zaobserwowanych w nich wzorców. Dzięki profilowaniu z wykorzystaniem algorytmu funkcjonariusze organów ścigania i zarządzania granicami mogą na podstawie analizy danych ukierunkować działania na konkretne osoby lub grupy, które stanowią pewne zagrożenie.

Profilowanie z wykorzystaniem algorytmu wzbudza poważne wątpliwości w kwestiach praw podstawowych, dotyczące między innymi potencjalnej

dyskryminacji i naruszania praw do poszanowania życia prywatnego i do ochrony danych. W niniejszej sekcji przewodnika skupiono się na sposobie, w jaki funkcjonariusze organów ścigania i zarządzania granicami mogą w swojej codziennej pracy wykorzystywać i przetwarzać dane zgodnie z zasadami praw podstawowych.

Przetwarzanie danych osobowych: co mówią przepisy?

Normy prawne dotyczące przetwarzania danych osobowych do celów tworzenia profili określono w unijnych ramach prawnych dotyczących ochrony danych. Zarówno zgodnie z art. 4 pkt 4 ogólnego rozporządzenia o ochronie danych (RODO), jak i z art. 3 pkt 4 dyrektywy dotyczącej policji, „»profilowanie« oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się".

Artykuł 22 ust. 1 RODO stanowi, że profilowanie można zaakceptować tylko pod warunkiem, że decyzja nie opiera się wyłącznie na zautomatyzowanym przetwarzaniu i nie wywołuje wobec osób fizycznych skutków, które istotnie by na nie wpływały.

Profilowanie objęte zakresem stosowania dyrektywy dotyczącej policji (zob. sekcja 3.1 odnosząca się do profilowania z wykorzystaniem algorytmu i ochrony danych) powinno być wykonywane zgodnie z art. 11 ust. 3 dyrektywy dotyczącej policji. Stanowi on, że „[p]rofilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii, o których mowa w art. 10*, jest zabronione zgodnie z prawem Unii".

* Mówiąc o „szczególnych kategoriach danych osobowych", mówimy o „danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej". Zob. art. 10 ust. 1 dyrektywy dotyczącej policji.

Wykres 1: Proces profilowania z wykorzystaniem algorytmu w kontekście ścigania przestępstw i zarządzania granicami

Źródło: *FRA 2018 (adaptowano z/na podstawie Perry, W.L. i in. (2013), s. 11–15 oraz Zarsky, T.Z. (2002–2003), s. 6–18).*

Metoda stosowana do tworzenia profili do celów profilowania z wykorzystaniem algorytmu przypomina technikę znaną jako **„analiza behawioralna"**, w której łączy się niektóre cechy i wzorce zachowań. Wykres 1 przedstawia sposób, w jaki można wykorzystywać algorytmy do prognozowania.

Koncentracja na sposobie wykorzystywania algorytmów do wspierania procesu decyzyjnego

Dzięki większej dostępności i większemu wykorzystaniu danych znacznie ułatwiono proces decyzyjny lub zastąpiono go metodami modelowania predyktywnego, określanymi często jako wykorzystanie algorytmów. Algorytm to sekwencja komend dla komputera służących przekształceniu danych wejściowych w dane wyjściowe. Wiele algorytmów opiera się

na metodach statystycznych i wykorzystuje techniki służące obliczaniu powiązań pomiędzy różnymi zmiennymi. Na przykład dane na temat ilości alkoholu spożywanego przez grupę osób i dane dotyczące średniego trwania życia w tej samej grupie można wykorzystać razem do obliczenia średniego wpływu spożywania alkoholu na średnią długość życia.

Dane wyjściowe algorytmu stanowią zawsze prawdopodobieństwo, co oznacza, że istnieje pewien stopień niepewności co do utworzonych powiązań lub klasyfikacji. Na przykład dostawcy poczty elektronicznej korzystają z algorytmów w celu identyfikowania wiadomości, które są spamem, i umieszczania ich w folderze kosza. Algorytmy te działają dobrze, nie są jednak bezbłędne. Czasami spam nie zostanie wykryty i wyląduje w skrzynce odbiorczej; jest to wynik fałszywie ujemny (tj. wiadomość jest fałszywie zidentyfikowana jako niebędąca spamem). Rzadziej prawidłowa wiadomość e-mail może zostać wychwycona przez filtr antyspamowy i umieszczona w folderze kosza; jest to wynik fałszywie dodatni.

Rozumienie podstaw tego, w jaki sposób algorytmy wspierają proces decyzyjny, umożliwia praktykom określanie i zadawanie właściwych pytań na temat potencjalnych problemów z wykorzystywaniem algorytmów, w tym możliwości dyskryminacji i naruszania praw do poszanowania życia prywatnego i do ochrony danych.

Aby uzyskać więcej informacji, zob. FRA (2018b).

Tworzenie algorytmów do celów prognozowania to skomplikowany proces, który wymaga podejmowania wielu decyzji przez szereg osób zaangażowanych w ten proces. Jako takie odnosi się ono nie tylko do zasad, zgodnie z którymi postępuje komputer, lecz także do procesu gromadzenia, przygotowywania i analizy danych. Jest to proces realizowany przez człowieka i obejmujący kilka etapów, wymagający podejmowania decyzji przez osoby opracowujące algorytm i zarządzające procesem. Metoda statystyczna jest tylko częścią procesu służącego opracowaniu ostatecznych zasad stosowanych do celów prognozowania, klasyfikacji lub podejmowania decyzji[5]. W każdym razie sposób gromadzenia i wykorzystywania danych może być dyskryminujący.

5 FRA (2018b), s. 4.

Przykład

Aby oprogramowanie służące do rozpoznawania twarzy było skuteczne i dokładne, należy do niego wprowadzić ogromne ilości zdjęć i danych. Im więcej uzyska ono danych, tym dokładniejsze będą wytwarzane przez nie wyniki. Jak dotychczas zdjęcia wprowadzone do algorytmów jako dane treningowe przedstawiają jednak w większości białych mężczyzn, w porównaniu z niewielką liczbą kobiet lub osób o innym pochodzeniu etnicznym. W rezultacie uzyskane wyniki są mniej precyzyjne i istnieje w ich przypadku większe prawdopodobieństwo niedokładności w odniesieniu do osób należących do wspomnianych grup. W przypadku gdy organy ścigania lub straż graniczna będą z nich korzystały do celów profilowania osób i podejmowania decyzji np. dotyczących ich aresztowania, może to doprowadzić do błędów mających potencjalnie duży wpływ na prawa i wolności danej osoby.

Aby uzyskać więcej informacji, zob. Center on Privacy and Technology at Georgetown Law (2016); oraz Buolamwini J., Gebru T. (2018).

Wprowadzenie uprzedzeń może nastąpić na każdym etapie procesu profilowania z wykorzystaniem algorytmu. Aby uniknąć dyskryminacyjnych uprzedzeń i naruszania praw do ochrony danych i do prywatności, zarówno osoby opracowujące algorytmy, jak i funkcjonariusze organów ścigania i odpowiedzialni za zarządzanie granicami, którzy gromadzą i interpretują dane, powinni w pełni rozumieć prawa podstawowe i ich zastosowanie w tym kontekście.

Niezwykle istotne jest korzystanie z rzetelnych danych. Podczas profilowania z wykorzystaniem algorytmu jakość danych musi podlegać ocenie w celu zapewnienia ich rzetelności: im mniej są one zróżnicowane, tym są rzetelniejsze. Wykorzystywanie do stworzenia algorytmu danych, które odzwierciedlają uprzedzenia lub pochodzą z nierzetelnych źródeł, przyniesie nieobiektywne i nierzetelne wyniki. Błędy mogą się również pojawiać podczas prognozowania na podstawie danych.

- Wyniki fałszywie dodatnie odnoszą się do przypadków wyodrębnienia osób i poddania ich dalszej obserwacji na podstawie błędnej prognozy, że stanowią one zagrożenie.

- Wyniki fałszywie ujemne odnoszą się do osób, które stanowią realne zagrożenie w kontekście operacji ścigania przestępstw i zarządzania granicami, lecz system nie zidentyfikował ich jako takich.

1.2. Kiedy profilowanie jest niezgodne z prawem?

Najważniejsze kwestie

- Cechy indywidualne można wykorzystywać na potrzeby profilowania jako czynniki zgodne z prawem. Aby można jednak było uniknąć dyskryminacyjnego, a więc niezgodnego z prawem profilowania, musi *również* istnieć uzasadniona podstawa do podejrzeń oparta na innych informacjach niż **cechy chronione**.
  - Cechy chronione obejmują płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek i orientację seksualną.
  - Cechy chronione można ujawnić, wywnioskować lub przewidzieć na podstawie innych danych osobowych.
- W celu gromadzenia i przetwarzania **danych osobowych** organy ścigania i organy zarządzania granicami muszą zapewnić, aby gromadzenie i przetwarzanie danych miały podstawy prawne, ważny i prawnie uzasadniony cel oraz aby były niezbędne i proporcjonalne.
  - Dane osobowe to wszelkie informacje, które można wykorzystać, aby – bezpośrednio lub pośrednio – zidentyfikować osobę, takie jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, lub czynniki określające tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną osoby fizycznej.

Profilowanie stosowane zgodnie z prawem jest **uzasadnioną techniką dochodzeniową**. Aby było ono zgodne z prawem, **uzasadnienia będące jego podstawą muszą być obiektywne i rozsądne**, i musi być ono wykonywane z przestrzeganiem praw podstawowych, takich jak prawo do niedyskryminacji i do ochrony danych osobowych. Uznaje się, że profilowanie nie ma obiektywnego i rozsądnego usprawiedliwienia, „jeżeli nie dąży do osiągnięcia prawnie uzasadnionego celu, albo jeżeli nie ma rozsądnego stosunku proporcjonalności między zastosowanymi środkami i celem, który ma być zrealizowany”[6].

Profilowanie może dotyczyć wielu różnych praw podstawowych. W niniejszej sekcji skupiono się na prawach podstawowych, na które niezgodne z prawem profilowanie ma największy wpływ: prawie do niedyskryminacji i prawach do

6 Europejska Komisja przeciwko Rasizmowi i Nietolerancji (ECRI) (2007), pkt 28.

poszanowania prywatności i do ochrony danych. Profilowanie uznaje się za niezgodne z prawem, jeżeli:

- obejmuje ono działania nieuzasadnionego zróżnicowanego traktowania osób na podstawie cech chronionych (zob. sekcja 1.2.1); lub

- niepotrzebnie ingeruje w życie prywatne osób lub jest niezgodne z przepisami w zakresie przetwarzania danych osobowych (zob. sekcja 1.2.2).

1.2.1. Zakaz dyskryminacji

Zakaz dyskryminacji: co mówią przepisy?

„**Zakazana jest wszelka dyskryminacja w szczególności ze względu na** płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną”*.

Artykuł 21 Karty praw podstawowych UE

„**Korzystanie z każdego prawa ustanowionego przez prawo powinno być zapewnione bez dyskryminacji wynikającej z takich powodów**, jak płeć, rasa, kolor skóry, język, religia, przekonania polityczne lub inne, pochodzenie narodowe lub społeczne, przynależność do mniejszości narodowej, majątek, urodzenie lub z jakichkolwiek innych przyczyn. Nikt nie może być dyskryminowany przez jakiekolwiek władze publiczne z któregokolwiek z powodów wymienionych w ustępie 1”.

Artykuł 1 Protokołu nr 12 do Europejskiej konwencji praw człowieka

* Należy zauważyć, że w praktyce wiele państw członkowskich rozszerzyło ochronę przeciwko dyskryminacji ponad podstawy ujęte w Karcie i w Europejskiej konwencji praw człowieka (EKPC).

Dyskryminacja występuje, „gdy osobę traktuje się mniej przychylnie niż traktuje się, traktowano lub traktowano by inną osobę w porównywalnej sytuacji” ze względu

na postrzegane lub rzeczywiste cechy osobowe[7]. W prawie antydyskryminacyjnym cechy te nazywa się „cechami chronionymi". Więcej informacji na temat europejskiego prawa i orzecznictwa w obszarze niedyskryminacji jest dostępnych w *Podręczniku europejskiego prawa o niedyskryminacji* z 2018 r., opublikowanego wspólnie przez FRA i Radę Europy[8].

Istnieje kilka rodzajów dyskryminacji:

Dyskryminacja bezpośrednia ma miejsce, gdy osoba jest traktowana mniej przychylnie *wyłącznie lub głównie* ze względu na cechę chronioną, taką jak rasa, płeć, wiek, niepełnosprawność lub pochodzenie etniczne[9].

Przykład

W odpowiedzi na zagrożenie terrorystyczne policja dostała uprawnienia do przeprowadzenia zatrzymania i rewizji każdej osoby, która może być według niej zaangażowana w działania terrorystyczne. Policja uważa, że zagrożenie pochodzi ze strony organizacji terrorystycznej działającej aktywnie w pewnym regionie świata, nie istnieją jednak żadne bardziej szczegółowe dane wywiadowcze. Jeżeli funkcjonariusz policji zatrzymałby mężczyznę wyłącznie lub głównie ze względu na to, że jego wygląd zewnętrzny wskazuje na możliwe pochodzenie z tego samego regionu świata, działanie takie stanowiłoby bezpośrednią dyskryminację i byłoby niezgodne z prawem.

Dyskryminacja pośrednia (zwana również dyskryminacją z racji odmiennego wpływu w kontekście ścigania przestępstw i zarządzania granicami) ma miejsce, gdy przepis, kryterium lub praktyka, które są *pozornie neutralne*, mogą doprowadzić do szczególnie niekorzystnej sytuacji dla osób posiadających konkretną chronioną cechę w stosunku do innych osób, chyba że taki przepis, takie kryterium lub taka praktyka są obiektywnie uzasadnione zgodnym z prawem celem, a środki mające

7 Artykuł 2 dyrektywy Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzającej w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne, Dz.U. L 180; oraz art. 2 dyrektywy Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiającej ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy, Dz.U. L 303.

8 FRA i Rada Europy (2018).

9 *Ibid.*, s. 43.

służyć osiągnięciu tego celu są konieczne i proporcjonalne[10]. Co do zasady w przypadku dyskryminacji pośredniej wymagane jest zastosowanie statystyki, aby ocenić, czy dana osoba była w praktyce traktowana w sposób niekorzystny w porównaniu z inną osobą ze względu na jej przynależność do grupy o konkretnych cechach chronionych.

Przykład

W ramach prowadzenia rutynowej kontroli organy ścigania zadecydowały, że będą zatrzymywać co dziesiąty samochód w mieście X w godzinach 21.00–1.00; 60 % populacji miasta X poruszających się w tych godzinach samochodem to osoby pochodzenia afrokaraibskiego, tymczasem populacja afrokaraibska miasta i otaczających go obszarów nie przekracza 30 %. Ponieważ istnieje prawdopodobieństwo, że działania policji będą miały większy wpływ na tę grupę niż na pozostałe, sytuacja taka stanowiłaby dyskryminację pośrednią.

Rozpatrywanie kwestii dyskryminacji na podstawie jednej cechy nie pozwala na adekwatne odzwierciedlenie różnych przejawów nierównego traktowania. Pojęcie **„dyskryminacji z wielu przyczyn jednocześnie"** odnosi się do dyskryminacji, która występuje z powodu kilku cech funkcjonujących osobno. Na przykład osoba może doświadczać dyskryminacji nie tylko ze względu na swoje pochodzenie etniczne, lecz również ze względu na wiek i płeć[11]. Pojęcie **„dyskryminacji intersekcjonalnej"** odnosi się do sytuacji, w której kilka cech funkcjonuje i wzajemnie na siebie wpływa w tym samym czasie w taki sposób, że są one nierozerwalne i wywołują określone rodzaje dyskryminacji (zob. ramkę z przykładem).

Przykład

Funkcjonariusz policji zatrzymuje młodego mężczyznę pochodzenia afrykańskiego i przeprowadza rewizję, nie mając uzasadnionego podejrzenia, że mężczyzna ten popełnił przestępstwo. Mężczyzna doświadcza dyskryminacji nie tylko ze względu na swój wiek – policja nie zatrzymuje wszystkich młodych osób – lub pochodzenie etniczne – policja nie zatrzymuje wszystkich osób pochodzenia afrykańskiego, lecz właśnie ze względu na kombinację bycia młodym i pochodzenia afrykańskiego.

10 Artykuł 2 dyrektywy Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiającej ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy, Dz.U. L 303 (dyrektywa w sprawie równego traktowania w zakresie zatrudnienia i pracy); zob. również FRA i Rada Europy (2018), s. 53.

11 FRA i Rada Europy (2018), s. 59.

Dyskryminacja może również wynikać ze zautomatyzowanego przetwarzania danych osobowych i stosowania profilowania z wykorzystaniem algorytmu. Dyskryminacja może pojawić się podczas opracowywania i wdrażania algorytmów za sprawą uprzedzeń włączanych – świadomie lub nie – do algorytmu, a także podczas podejmowania decyzji na podstawie uzyskanych informacji.

Artykuł 9 ust. 1 RODO wyraźnie stanowi, że zabrania się przetwarzania szczególnych kategorii danych osobowych ujawniających takie cechy osobowe, jak pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe (aby uzyskać pełen wykaz cech chronionych, zob. wykres 9 w sekcji 2.2.4). Zakaz ten można uchylić w szczególnych przypadkach, takich jak ochrona interesu publicznego, pod warunkiem że wyłączenie takie ma podstawę prawną, jest proporcjonalne i konieczne oraz przewiduje odpowiednie środki ochrony[12].

Podobnie w kontekście zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych, w art. 11 ust. 3 dyrektywy dotyczącej policji dotyczącym zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach zakazane jest „profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii", w tym danych osobowych ujawniających pochodzenie rasowe lub etniczne i przekonania religijne oraz dane genetyczne i biometryczne[13]. W niektórych przypadkach dozwolone są również wyjątki od tego zakazu, profilowanie musi być jednak konieczne, musi mieć podstawę prawną albo być niezbędne dla ochrony żywotnych interesów osoby fizycznej i muszą zostać zastosowane odpowiednie środki ochrony[14].

12 Artykuł 9 ust. 2 lit. g) ogólnego rozporządzenia o ochronie danych.

13 Aby uzyskać więcej informacji, zob. Grupa Robocza Art. 29 (2017b).

14 Artykuł 10 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 (dyrektywa dotycząca policji).

Zakaz dyskryminacyjnego profilowania: co mówią przepisy?

„**Profilowanie skutkujące dyskryminacją** osób fizycznych **na podstawie danych osobowych**, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, **powinno być zakazane** na warunkach określonych w art. 21 i 52 Karty [praw podstawowych]".

Motyw 38 dyrektywy dotyczącej policji

„**Profilowanie skutkujące dyskryminacją** osób fizycznych na podstawie danych osobowych szczególnych kategorii, o których mowa w art. 10*, **jest zabronione** zgodnie z prawem Unii".

Artykuł 11 ust. 3 dyrektywy dotyczącej policji

* Artykuł 10 dyrektywy dotyczącej policji: „danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej".

„Podczas dokonywania odprawy granicznej straż graniczna **nie może dyskryminować** osób ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną".

Artykuł 7 kodeksu granicznego Schengen

Zakaz dyskryminacji nie oznacza, że nie wolno wykorzystywać cech osobowych jako legalnych czynników na potrzeby profilowania w kontekście postępowania przygotowawczego lub kontroli granicznych (zob. sekcja 2.3). Musi jednak istnieć uzasadniona podstawa do podejrzeń oparta na innych informacjach niż cechy chronione. Na przykład osoba może pasować do konkretnego opisu podejrzanego lub wygląd zewnętrzny tej osoby może nie odpowiadać informacjom widniejącym w jej dokumencie podróży[15].

15 Zjednoczone Królestwo, Izba Lordów (2006), Lord Scott, Opinie Lordów w sprawie odwołania od wyroku w sprawie *R (on the application of Gillan et al.) przeciwko Commissioner of Police for the Metropolis et al.* [2006] UKHL 12, 8 marca 2006 r., pkt 67.

Koncentracja na dyskryminacji ze względu na narodowość

W art. 21 Karty praw podstawowych UE **ograniczono zakaz dyskryminacji ze względu na narodowość do obywateli UE**. W dyrektywie w sprawie równości rasowej wśród cech chronionych nie ujęto narodowości.

Państwa członkowskie w różny sposób rozszerzyły zakres zakazu dyskryminacji tak, aby ujmował on narodowość. Jedną z takich metod jest uznanie, że narodowość stosuje się czasem jako zamiennik pojęcia rasy, pochodzenia etnicznego lub religii. W niektórych przypadkach „różnice w traktowaniu ze względu na narodowość [...] [będą] uznane za naruszenie przepisów zakazujących dyskryminacji w oparciu o te cechy" (zob. europejska sieć ekspertów prawnych w dziedzinie równości kobiet i mężczyzn i niedyskryminacji, 2016, s. 99). W praktyce często trudno rozróżnić dyskryminację ze względu na narodowość i dyskryminację ze względu na pochodzenie etniczne.

Fakt, że w art. 21 Karty nie wymieniono bezpośrednio narodowości jako potencjalnej podstawy dyskryminacji, odzwierciedla przede wszystkim różny status obywateli UE (i innych osób korzystających z prawa do swobodnego przemieszczania się zgodnie z prawem Unii) i obywateli państw trzecich zgodnie z prawem Unii. Ma to szczególne znaczenie w procedurach granicznych, w których narodowość jest decydującym czynnikiem przy określaniu, czy osoba będzie podlegała dokładnej kontroli lub czy musi posiadać wizę, aby wjechać do strefy Schengen lub przez nią przejechać.

Jednocześnie istnieje ryzyko, że systematyczne kierowanie wszystkich osób określonej narodowości do kontroli drugiej linii będzie dyskryminujące. Narodowość może być uzasadnionym elementem profilów ryzyka służących wykrywaniu nielegalnej migracji lub domniemanych ofiar handlu ludźmi, nie może być ona jednak jedyną lub główną przyczyną skierowania do kontroli drugiej linii. Ponadto, tak jak w innych kontekstach, odrębne traktowanie w oparciu o narodowość staje się dyskryminujące, a zatem niezgodne z prawem, gdy jest stosowane jako zamiennik dyskryminowania ze względu na cechy chronione blisko związane z narodowością, takie jak rasa, pochodzenie etniczne czy religia.

W swoich zalecanych zasadach i wytycznych dotyczących praw człowieka na granicach międzynarodowych Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka wymienia narodowość wśród cech chronionych, których nie należy wykorzystywać do celów profilowania migrantów (zasada 8).

Orzecznictwo

W sprawie *Rosalind Williams Lecraft przeciwko Hiszpanii* funkcjonariusz policji zatrzymał na peronie dworca kolejowego w Hiszpanii kobietę i poprosił ją o okazanie dokumentów tożsamości. Kobieta zapytała funkcjonariusza policji, dlaczego jest jedyną osobą zatrzymaną na peronie, i usłyszała w odpowiedzi: „Ponieważ jest pani czarna". W swoim rozstrzygnięciu Komitet Praw Człowieka podkreślił, że co do zasady prowadzenie kontroli tożsamości w interesie bezpieczeństwa publicznego i do celów przeciwdziałania przestępstwom i monitorowania nielegalnej migracji jest zgodne z prawem. Uznał jednak, że „organy podczas prowadzenia takich kontroli nie powinny uznawać cech fizycznych lub etnicznych kontrolowanych osób jako wskazujących na ich możliwą nielegalną sytuację w kraju. Kontroli tożsamości nie należy również prowadzić w taki sposób, aby były one ukierunkowane wyłącznie na osoby o określonych cechach fizycznych lub świadczących o pochodzeniu etnicznym. Postępowanie takie nie tylko miałoby negatywny wpływ na godność osób objętych taką kontrolą, lecz przyczyniłoby się również do szerzenia postaw ksenofobicznych wśród ogółu ludności, a także byłoby niespójne ze skuteczną polityką zwalczania dyskryminacji rasowej".

W 2017 r. podobną skargę wniesiono do Europejskiego Trybunału Praw Człowieka, która to sprawa dotyczyła traktowania obywatela Pakistanu podczas zatrzymania przez policję w Hiszpanii i po tym zatrzymaniu. Trybunał będzie musiał zdecydować, czy skarżący doznał podczas zatrzymania dyskryminacji ze względu na pochodzenie etniczne oraz czy miało miejsce naruszenie art. 8 (prawo do poszanowania życia prywatnego i rodzinnego) ze względu na to, że hiszpańskie organy nie podjęły wszystkich właściwych kroków w celu ujawnienia możliwych rasistowskich motywów zdarzenia. W momencie pisania niniejszego przewodnika sprawa oczekuje na rozstrzygnięcie.

Aby uzyskać więcej informacji, zob. UNHRC, Rosalind Williams Lecraft przeciwko Hiszpanii, Comm. nr 1493/2006 oraz ETPC, Zeshan Muhammad

przeciwko Hiszpanii, nr 34085/17, wniesiona dnia 6 maja 2017 r. Zob. również FRA i Rada Europy (2018).

W sprawie *B.S. przeciwko Hiszpanii* pracownica seksualna pochodzenia nigeryjskiego legalnie mieszkająca w Hiszpanii twierdziła, że hiszpańska policja dopuściła się wobec niej przemocy fizycznej i słownej z powodu jej rasy, płci i zawodu. Kobieta twierdziła, że w przeciwieństwie do innych pracowników seksualnych pochodzenia europejskiego była często poddawana kontrolom policyjnym i doświadczała obraźliwego zachowania o charakterze rasistowskim i seksistowskim. Dwaj interwenienci zewnętrzni z ośrodka AIRE oraz Europejskiej Jednostki ds. Badań Społecznych Uniwersytetu Barcelońskiego zwrócili się do Europejskiego Trybunału Praw Człowieka o stwierdzenie dyskryminacji intersekcjonalnej. Trybunał stwierdził naruszenie art. 3 (zakaz poniżającego lub nieludzkiego traktowania), ale dodatkowo osobno rozpatrzył, czy miało miejsce również zaniechanie zbadania ewentualnego związku przyczynowego między rzekomymi postawami rasistowskimi a aktami przemocy ze strony policji. W tej kwestii Europejski Trybunał Praw Człowieka stwierdził naruszenie art. 14 (zakaz dyskryminacji), ponieważ sądy krajowe nie wzięły pod uwagę szczególnie trudnej sytuacji skarżącej związanej z jej statusem kobiety afrykańskiej będącej pracownicą seksualną. Chociaż Trybunał przyjął podejście intersekcjonalne, w wyroku nie użył on terminu „intersekcjonalność".

Aby uzyskać więcej informacji, zob. ETPC, B.S. przeciwko Hiszpanii, nr 47159/08, 24 lipca 2012 r.

Koncentracja na ciężarze dowodu

W 2016 r. francuski sąd kasacyjny po raz pierwszy wydał orzeczenie w sprawie dyskryminacyjnych kontroli tożsamości. W swojej *decyzji z dnia 9 listopada 2016 r.* sąd stwierdził, że policja prowadziła dyskryminujące kontrole tożsamości w przypadku trzech z 13 mężczyzn pochodzenia afrykańskiego lub arabskiego. Stwierdził, że w tych przypadkach odpowiedzialne było państwo, i nakazał wypłatę zadośćuczynienia na rzecz trzech skarżących. W ośmiu innych przypadkach sąd uznał, że zaskarżone kontrole tożsamości były zgodne z prawem, gdyż opierały się one na obiektywnych, a zatem niedyskryminujących elementach. W dwóch pozostałych sprawach sędziowie

nie wydali orzeczenia i skierowali je z powrotem do sądów niższej instancji do ponownego rozpatrzenia.

Sąd wyjaśnił również, na kim w takich sprawach spoczywa ciężar dowodu. Kontrole tożsamości nie są rejestrowane, jeżeli nie prowadzą do postępowania sądowego lub administracyjnego. Sąd wyjaśnił, że skarżący powinni przedstawić sądom dowody wskazujące na istnienie dyskryminacji. Policja musi udowodnić, że odmienne traktowanie nie miało miejsca podczas prowadzenia kontroli tożsamości albo że odmienne traktowanie było uzasadnione ze względu na obiektywne kwestie.

Ponadto sąd stwierdził, że sędziowie mogą uwzględniać w ramach dowodów badania i informacje statystyczne potwierdzające częstotliwość prowadzenia kontroli tożsamości o charakterze dyskryminacyjnym u tej samej grupy ludności co skarżący (np. widocznych mniejszości określonych na podstawie cech fizycznych wynikających z rzeczywistego lub zakładanego pochodzenia etnicznego). Sam taki dowód nie jest jednak wystarczający do sugerowania dyskryminacji.

W związku z tym sąd uznał, że prowadzenie kontroli tożsamości na podstawie cech fizycznych związanych z rzeczywistym lub zakładanym pochodzeniem etnicznym bez wcześniejszego obiektywnego uzasadnienia stanowi dyskryminację i jest poważnym uchybieniem, za które w przedmiotowych trzech sprawach odpowiedzialność ponosi państwo.

Aby uzyskać więcej informacji, zob. Cour de Cassation, Décision 1245, 9 listopada 2016 r.

1.2.2. Prawo do poszanowania życia prywatnego i ochrona danych osobowych

Na podstawie prawa Unii prawo do poszanowania życia prywatnego (art. 7 Karty) i ochrona danych osobowych (art. 8 Karty) to odmienne, choć blisko powiązane prawa. Prawo do życia prywatnego (lub prawo do prywatności) jest szerszym prawem zakazującym *jakiejkolwiek ingerencji* w prywatne życie osoby fizycznej. Życie prywatne jest rozumiane nie tylko jako to, co dana osoba chciałaby utrzymać jako poufne, lecz również jako środki, za pośrednictwem których osoba wyraża swoją osobowość, np. decydując z kim chce wchodzić w interakcje lub w jaki sposób chce

się ubierać. Ochrona danych osobowych ogranicza się do oceny zgodności z prawem w związku z *przetwarzaniem danych osobowych*[16]. Na potrzeby niniejszego przewodnika te dwa pojęcia stosuje się wymiennie, jeżeli nie odnoszą się konkretnie do prawa Unii. Prawa te nie są bezwzględne i w niektórych okolicznościach mogą zostać ograniczone (zob. art. 8 EKPC i art. 52 Karty).

Prawo do prywatności i ochrona danych osobowych: co mówią przepisy?

„1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób".

Artykuł 8 Europejskiej konwencji praw człowieka

„Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

Artykuł 7 Karty praw podstawowych UE

„1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. (...)".

Artykuł 8 Karty praw podstawowych UE

„1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, **która opiera się wyłącznie na zautomatyzowanym przetwarzaniu**, w tym profilowaniu, i **wywołuje wobec tej osoby skutki prawne lub** w podobny sposób **istotnie na nią wpływa**.

16 FRA, EIOD i Rada Europy (2018).

2. Ustęp 1 nie ma zastosowania, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy [...];

b) jest dozwolona prawem [...], które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą".

Artykuł 22 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych

„Państwa członkowskie zapewniają, by decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, były zakazane, chyba że dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora".

Artykuł 11 ust. 1 dyrektywy dotyczącej policji

W prawie wtórnym Unii rozwinięto kwestię prawa do prywatności i ochrony danych osobowych. Dwa akty prawne określają szczegółowo, w jaki sposób można gromadzić i przetwarzać dane osobowe. W rozporządzeniu 2016/679, czyli ogólnym rozporządzeniu o ochronie danych (RODO), określono ogólne zasady i zabezpieczenia dotyczące przetwarzania danych osobowych. W bardziej szczegółowym ujęciu w dyrektywie 2016/680, zwanej dyrektywą dotyczącą policji, określono zasady przetwarzania danych osobowych w kontekście operacji ścigania przestępstw do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych. Najważniejsze zasady i niektóre kluczowe różnice między tymi dwoma aktami zilustrowano w tabeli 2. Poszczególne przepisy ustanawiające duże bazy danych UE wykorzystywane do celów zarządzania granicami, takie jak wizowy system informacyjny (VIS), system wjazdu/wyjazdu (EES) czy europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS), również zawierają specjalne ramy prawne w zakresie ochrony danych (zob. sekcja 3.2 dotycząca wielkoskalowych baz danych).

Tabela 2: Wymogi w zakresie ochrony danych – różnice między dyrektywą dotyczącą policji a RODO

Zasada ochrony danych	RODO	Dyrektywa dotycząca policji
Zgodność z prawem, rzetelność, przejrzystość	Dane osobowe muszą być przetwarzane rzetelnie, zgodnie z prawem **i w sposób przejrzysty**.	Dane osobowe muszą być przetwarzane rzetelnie i zgodnie z prawem.
Ograniczenie celu	Danych osobowych gromadzonych w jednym celu nie należy przetwarzać dalej w sposób niezgodny z tym celem; **dalsze przetwarzanie do celów badań naukowych lub historycznych lub do celów statystycznych nie jest niezgodne z pierwotnymi celami**.	Danych osobowych gromadzonych w jednym celu nie należy następnie przetwarzać w sposób niezgodny z tym celem; inne cele nie są niezgodne z pierwotnym celem, jeżeli przetwarzanie takie jest dozwolone prawem, niezbędne i proporcjonalne.
Minimalizacja danych	Gromadzone dane osobowe są adekwatne, stosowne i **ograniczone do tego, co niezbędne** do celów, w których zostały zgromadzone.	Gromadzone dane osobowe są adekwatne, stosowne i **nienadmierne** do celów, dla których zostały zgromadzone.
Ograniczenie przechowywania	Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres niezbędny do osiągnięcia celu, w którym zostały one zgromadzone; **dane osobowe można przechowywać przez okres dłuższy do celów badań naukowych lub historycznych lub do celów statystycznych**.	Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres niezbędny do osiągnięcia celu, w którym zostały one zgromadzone.
Prawidłowość	Gromadzone dane osobowe powinny być prawidłowe i uaktualniane. Nieprawidłowe lub niedokładne dane osobowe powinny zostać usunięte lub sprostowane.	
Integralność i poufność	Dane osobowe należy przechowywać w sposób zapewniający im ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.	

Źródło: *FRA, 2018.*

Przykłady

Funkcjonariusz straży granicznej przesyła listę pasażerów samolotu osobom nieupoważnionym. Po udostępnieniu te dane osobowe mogą zostać wykorzystane do innych lub prywatnych celów. Stanowi to wyraźne naruszenie zasad ochrony danych.

Funkcjonariuszka policji opuszcza swoje biuro, pozostawiając na monitorze swojego komputera wykaz danych osobowych związanych z podejrzanymi. Ponieważ zachowanie takie osłabia zasadę ochrony danych osobowych, stanowi ono naruszenie zasad ochrony danych osobowych.

Orzecznictwo

Orzeczenia sądu stanowią wytyczne dotyczące sposobu stosowania tych zasad w praktyce.

Ograniczenie celu

W sprawie *Heinz Huber przeciwko Bundesrepublik Deutschland* TSUE ocenił zgodność z prawem niemieckiego centralnego rejestru cudzoziemców (*Auslanderzentralregister, AZR*), w którym ujęte są niektóre dane osobowe związane z cudzoziemcami – zarówno obywatelami UE, jak i obywatelami państw trzecich – przebywającymi w Niemczech przez okres powyżej trzech miesięcy. TSUE stwierdził, że dane zgromadzone w konkretnym celu nie mogą być wykorzystywane w innym celu. Trybunał uznał, że wykorzystanie takiego instrumentu jak AZR do celów stosowania przepisów dotyczących prawa pobytu jest uzasadnione oraz że różnica w traktowaniu cudzoziemców i obywateli Niemiec, w przypadku których przechowuje się mniej danych, jest uzasadniona ze względu na określone cele. TSUE stwierdził jednak, że dane przechowywane w AZR nie mogą być wykorzystywane do ogólnego zwalczania przestępczości, gdyż jest to cel odmienny od celu, w którym pierwotnie zgromadzono dane.

Aby uzyskać więcej informacji, zob. TSUE, sprawa C-524/06, Heinz Huber przeciwko Bundesrepublik Deutschland*, 16 grudnia 2008 r.*

Ograniczenie przechowywania

W sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu* skarżący zwrócili się o skasowanie ich danych (odcisków palców, próbek komórkowych i profili DNA) z bazy danych DNA wykorzystywanej do identyfikacji w postępowaniu karnym w Zjednoczonym Królestwie. Toczące się przeciwko nim sprawy zakończyły się uniewinnieniem i obawiali się możliwego wykorzystywania ich danych obecnie lub w przyszłości. Policja odmówiła. ETPC stwierdził, że bezterminowe przechowywanie próbek DNA osób, które zostały aresztowane i następnie uniewinnione, lub w stosunku do których wycofano zarzuty, stanowi naruszenie prawa do prywatności. Trybunał podkreślił istnienie ryzyka stygmatyzacji, gdyż dane osób, które nie zostały skazane za żadne przestępstwo, traktuje się w taki sam sposób jak dane osób skazanych. Trybunał uznał również, że potencjalna krzywda, jaką mogłoby wywołać zatrzymanie takich danych, jest szczególnie istotna w przypadku dzieci z uwagi na znaczenie ich rozwoju i integracji w społeczeństwie.

Aby uzyskać więcej informacji, zob. ETPC, S. i Marper przeciwko Zjednoczonemu Królestwu, sprawy nr 30562/04 i 30566/04, 4 grudnia 2008 r.

W celu gromadzenia danych osobowych do celów profilowania organy ścigania i organy zarządzania granicami muszą przestrzegać czterech podstawowych kryteriów prawnych. Gromadzenie i przetwarzanie danych musi:

- **być zdefiniowane i uregulowane w prawie (*podstawa prawna*)**: jakiekolwiek ograniczenie praw do poszanowania życia prywatnego i do ochrony danych musi być określone w prawie i musi odbywać się z poszanowaniem istoty tych praw. Prawo musi być zgodne z normami przejrzystości i jakości, co oznacza, że prawo jest publicznie dostępne i jest sformułowane w sposób wystarczająco jasny i precyzyjny, aby można było zrozumieć jego zastosowanie i wynikające z niego konsekwencje;

- **mieć ważny, zgodny z prawem i odpowiedni cel (*uzasadniony cel*)**: uzasadnione cele są określone w prawie i nie można rozszerzać ich znaczenia. Mogą się one odnosić do bezpieczeństwa narodowego, zdrowia, porządku publicznego lub zapobiegania przestępczości;

- **być niezbędne do osiągnięcia tego celu (*konieczność*)**: przetwarzanie danych osobowych powinno ograniczać się do tego, co jest konieczne do osiągnięcia celu, w którym zgromadzono dane;

- **nie być nadmierne (*proporcjonalność*)**: organy przetwarzające dane osobowe powinny osiągnąć odpowiednią równowagę między celem a środkami stosowanymi do jego osiągnięcia. Innymi słowy, wartość dodana przetwarzania nie powinna przeważyć nad potencjalnym możliwym wpływem.

W rozdziale 3 wyjaśniono, w jaki sposób zasady te można stosować w praktyce.

Na wykresie 2 przedstawiono, w jaki sposób można wykorzystywać te zasady, aby ocenić, czy działanie może naruszać prawa do poszanowania życia prywatnego i rodzinnego i do ochrony danych (zob. również sekcja 2.3.3 dotycząca mechanizmów zaskarżania). Sprawa dotycząca zatrzymania i rewizji *Gillan i Quinton przeciwko Zjednoczonemu Królestwu* ilustruje, w jaki sposób ETPC zastosowało te zasady, aby ustalić, czy miało miejsce naruszenie prawa do ochrony danych i do prywatności (zob. ramka dotycząca orzecznictwa).

Wykres 2: Naruszenie prawa do prywatności i do ochrony danych – proces oceny

Źródło: *FRA, 2018 (na podstawie Rada Europy (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).*

Orzecznictwo

W sprawie *Gillan i Quinton przeciwko Zjednoczonemu Królestwu* skarżący, dwoje brytyjskich obywateli, ubiegali się o zakwestionowanie legalności użytych w stosunku do nich uprawnień do zatrzymania i rewizji poprzez kontrolę sądową.

Czy przyjęty środek jest przewidziany w prawie? Środek był zgodny z przepisami sekcji 44–47 ustawy o terroryzmie z 2000 r., które stanowiły, że: 1) w celu przeciwdziałania aktom terrorystycznym wyższy rangą funkcjonariusz policji mógł zezwolić każdemu umundurowanemu funkcjonariuszowi policji na danym obszarze na prowadzenie działań zatrzymania i rewizji; 2) zezwolenia podlegały potwierdzeniu przez ministra i były ograniczone czasowo, mogły jednak być odnawiane bezterminowo; 3) chociaż celem takich działań rewizyjnych było znalezienie przedmiotów, które mogły zostać użyte do celów przeprowadzenia aktów terrorystycznych, działania zatrzymania i rewizji nie musiały opierać się na podejrzeniu, że zatrzymana osoba lub zatrzymane osoby posiadały przy sobie tego rodzaju przedmioty; oraz 4) osoby odmawiające poddania się rewizji podlegały karze więzienia lub grzywny, lub obu karom łącznie (*Gillan i Quinton*, pkt 76–80).

Czy przyjęty środek ingeruje w prywatność lub ochronę danych? Użycie środków przymusu przez organy ścigania w celu zatrzymania osoby i przeprowadzenia rewizji jej ubrania i rzeczy stanowi wyraźną ingerencję w prawo do poszanowania życia prywatnego. Powagę jej wzmacnia jeszcze publiczne ujawnienie prywatnych informacji, które ma w sobie element upokorzenia i zażenowania (*Gillan i Quinton*, pkt 63).

Ocena proporcjonalności i konieczności: Trybunał wyraził szereg obaw związanych z proporcjonalnością i koniecznością prawa (*Gillan i Quinton*, pkt 80–86):

- norma ustawowa dotycząca zezwolenia na zatrzymanie nie była uciążliwa;
- zakres ustawowych uprawnień był taki, że osoba fizyczna napotykała niezmierne trudności, aby wykazać, że jakiekolwiek zezwolenie i potwierdzenie wykracza poza uprawnienia danych organów (*ultra vires*) lub stanowi nadużycie uprawnień;
- obszary geograficzne objęte zezwoleniem były bardzo rozległe, a termin był wielokrotnie przedłużany, co sprawia, że zamierzony charakter zezwolenia ulega ograniczeniu;

- ograniczenia dotyczące uznania poszczególnych funkcjonariuszy miały bardziej charakter formalny niż dotyczący istoty sprawy;
- istniały niewielkie szanse na zastosowanie środka zaskarżenia, gdyż funkcjonariusz prowadzący zatrzymanie nie musiał wykazywać zasadności swojego podejrzenia; udowodnienie nieodpowiedniego wykonywania uprawnień było zatem niemal niemożliwe.

Z tych względów ETPC stwierdził, że odpowiednie sekcje ustawy o terroryzmie nie były „ani wystarczająco ograniczone, ani nie podlegały odpowiednim zabezpieczeniom prawnym przeciwko nadużyciom", naruszały zatem art. 8 EKPC.

Aby uzyskać więcej informacji, zob. ETPC, Gillan i Quinton przeciwko Zjednoczonemu Królestwu, nr 4158/05, 12 stycznia 2010 r.

Wymogi prawne dotyczące profilowania określone w zmienionych ramach prawnych UE dotyczących ochrony danych opisano szczegółowo w rozdziale 3.

1.3. Jakie potencjalne negatywne konsekwencje ma niezgodne z prawem profilowanie w przypadku ścigania przestępstw i zarządzania granicami?

Profilowanie tylko na podstawie szerokich kategorii, takich jak rasa, pochodzenie etniczne lub religia, jest nie tylko niezgodne z prawem, lecz może mieć również niekorzystny wpływ na prowadzenie skutecznych działań przez policję i organy zarządzające granicami. W niniejszej sekcji przyjrzano się dwóm potencjalnym negatywnym konsekwencjom:

- Największą trudność stanowią napięcia, które mogą powstać w relacjach ze społecznościami. Profilowanie może wywołać niechęć wśród szczególnie narażonych społeczności i ograniczyć zaufanie do organów policji i organów zarządzania granicami. To z kolei może podważać skuteczność metod opartych na publicznej współpracy.

- Istnieją również wątpliwości co do skuteczności stosowania szerokich kategorii profili w zarządzaniu granicami lub ściganiu przestępstw, np. jeżeli osoba fizyczna zostaje fałszywie objęta podejrzeniem[17].

Ponadto jeżeli profilowanie odbywa się w sposób niezgodny z prawem, organy będą podlegały procedurom zaskarżenia lub postępowaniu prawnemu. Może ono przyjąć formę wewnętrznego nadzoru sprawowanego przez organy ds. skarg na policję, specjalne organy ds. skarg, organy nadzorcze lub w ramach systemu sądownictwa cywilnego i karnego (zob. sekcja 2.3). Poszczególni funkcjonariusze i przełożeni średniego szczebla, w konsekwencji zaangażowania w niezgodne z prawem profilowanie lub przyzwolenie na nie, mogą podlegać sankcjom administracyjnym lub karnym. Sytuacja taka może wyczerpać zasoby policji, obniżyć jej morale i popsuć reputację.

Najważniejsze kwestie

- **Niezgodne z prawem profilowanie podważa zaufanie** do organów ścigania i zarządzania granicami i może skutkować pogorszeniem stosunków z lokalnymi społecznościami.
- Istnieją **wątpliwości dotyczące rzeczywistej skuteczności stosowania szerokiego profilowania** do celów wykrywania przestępstw lub w ramach zarządzania granicami. Nie ma dowodów pozwalających rozstrzygnąć, czy takie profilowanie zwiększa skuteczność działań policji lub zarządzania granicami.

1.3.1. Wpływ na zaufanie do policji i do organów zarządzania granicami oraz dobre stosunki ze społecznością

Zgodnie z badaniami stosowanie szerokich profili może mieć negatywny wpływ na osoby, których one dotyczą, i na społeczności, do których osoby takie należą[18]. W poniższej ramce przedstawiono niektóre odpowiedzi osób po tym, jak zostały zatrzymane i poddane rewizji lub kontroli granicznej.

17 FRA (2017d), s. 51.

18 FRA (2017d).

Przykłady

Wpływ działań zatrzymania i rewizji oraz kontroli granicznej na osoby fizyczne

1. Zatrzymania przez policję – Keskinen, S. i in. (2018)

W latach 2015–2017 szwedzka szkoła nauk społecznych na Uniwersytecie Helsińskim spytała 185 osób o ich doświadczenia z profilowaniem etnicznym. Badanie wykazało, że większość respondentów uznała zatrzymania za nieprzyjemne, irytujące i upokarzające doświadczenie. Poniżej znajdują się fragmenty wypowiedzi respondentów.

„Chwilę później inny policjant znowu mnie zatrzymał […], jak szłam po ulicy z dwójką białych przyjaciółek: jedna była Finką, a druga Holenderką. I zrobił dokładnie to samo […], zadając mi to samo pytanie. Byłam wkurzona, bo nie wiedziałam, dlaczego mnie wybierali. Zapytałam ich o to, to odpowiedzieli tylko, że wykonują swoją pracę". (Kobieta, ok. 30 lat, państwo afrykańskie)

„Moja mama i mój brat byli raz na mieście, gdy zatrzymał ich policjant, mówiąc »Proszę okazać paszporty«. Uważam, że to było profilowanie etniczne. Wtedy mój brat powiedział [po fińsku]: »Nie mamy paszportów, nie nosimy ich cały czas przy sobie«. Jak zobaczyli, że mówi płynnie po fińsku, to stwierdzili: »Dobrze, nieważne«. Byłam zła, bo wiem, że profilowanie etniczne jest niezgodne z prawem, a moja mama i mój brat o tym nie wiedzieli. Więc czułam, jakby, no wie pan, źle ich potraktowano. I byłam przez to bardzo zła. Powiedziałam im, że to, co ich spotkało, było niezgodne z prawem, oni oczywiście wiedzieli, że zostali zatrzymani, bo […] nie wyglądali jak Finowie, wyglądali jak cudzoziemcy". (Kobieta, ok. 20 lat, Somalia-Finlandia)

„Zawsze mają podobny opis. Zastanawiam się w związku z tym, czy jeśli od 11 lat szukają tej samej osoby, która cały czas im się wymyka – to chyba nie idzie im zbyt dobrze, bo posiadany przez nich [straż graniczną] opis jest zawsze podobny i ja zawsze pasuję do tego opisu [śmiech]". (Mężczyzna, ok. 30 lat, państwo afrykańskie – Finlandia)

Aby uzyskać więcej informacji, zob. Keskinen, S. i in. (2018), The Stopped – Ethnic Profiling in Finland.

2. Kontrole graniczne – FRA (2014a i 2014b)

„Rozumiem, dlaczego [funkcjonariusz straży granicznej] mnie zatrzymał, ale nie musiał kierować mnie tutaj [do kontroli drugiej linii/na komisariat policji], czy traktować mnie jak przestępcy. Postępują tak ze wszystkimi z Europy Wschodniej". (Pasażer z Serbii, mężczyzna, przesłuchiwany na lotnisku we Frankfurcie)

Pytanie: *„Jak według pana potraktowano pana podczas kontroli pierwszej linii?"*

Odpowiedź: *„Myślę, że niedobrze. To było poniżające. Potraktowano mnie źle. Strażnik tyko wziął mój paszport, spojrzał na niego i zadzwonił po urzędnika imigracyjnego. Zadawał mi pytania i podnosił głos, ale niczego nie rozumiałem. Wyprowadzili mnie z kolejki, ale nie odnosili się do mnie z szacunkiem i wzbudzali we mnie strach".*

Pytanie: *„Dlaczego czuł się pan przestraszony lub upokorzony?"*

Odpowiedź: *„Ponieważ nie wiedziałem, co się stanie, a oni nie potrafili mi nic wytłumaczyć. Wokół było dużo ludzi, a strażnik rozmawiał z innymi strażnikami, w ogóle się do mnie nie zwracając. Potem musiałem czekać i wciąż nie wiedziałem, dlaczego się tam znalazłem".* (Pasażer z Angoli, mężczyzna, przesłuchiwany w porcie lotniczym Amsterdam-Schiphol)

„Naprawdę rozumiem [...] straż graniczną. Im również jest trudno godzinami pracować w tych budkach! Dlatego od czasu do czasu wykazują negatywne postawy, takie jak krzyczenie na ludzi takich jak my". (Mężczyzna, obywatel Turcji, kierowca samochodu ciężarowego często przekraczający granicę, Kipi)

Suma tych poszczególnych doświadczeń może przekładać się na negatywny efekt grupowy[19]. Może to przyczyniać się do wyraźnego pogorszenia stosunków między policją i organami zarządzania granicami a członkami społeczności mniejszościowych, u których działania zatrzymania i rewizji są prowadzone z dużą częstotliwością lub którzy podlegają większej kontroli na granicach.

19 Organizacja Narodów Zjednoczonych (ONZ) (2007), pkt 57.

Analiza przykładów

Rola zatrzymania i rewizji w przypadku zakłócenia porządku publicznego (Zjednoczone Królestwo 2011 i Francja 2005)

W następstwie zamieszek, które miały miejsce w sierpniu 2011 r. w kilku głównych miastach Zjednoczonego Królestwa, uczelnia London School of Economics wraz z magazynem Guardian przeprowadziła wywiady z 270 uczestnikami zamieszek dotyczące powodu ich udziału. Badanie wykazało, że znaczącymi czynnikami były brak zaufania i antypatia do policji oraz że „najpowszechniejsze skargi związane były z codziennym doświadczeniem ludzi związanym z działaniami policji, przy czym wiele osób wyraziło głęboką frustrację sposobem, w jaki osoby z ich społeczności były poddawane zatrzymaniu i rewizji".

Aby uzyskać więcej informacji, zob. London School of Economics (2011).

Podobną dynamikę zaobserwowano w innych państwach członkowskich UE. We Francji stwierdzono, że zamieszki, które miały tam miejsce w listopadzie 2005 r., wywołało zdarzenie, w którym zginęło przypadkowo dwoje młodych ludzi należących do mniejszości, gdy byli oni rzekomo ścigani przez policję (zob. Jobard, 2008 i Body-Gendrot, 2016).

Aby uzyskać więcej informacji, zob. Hörnqvist (2016).

Wnioskując z powyższego, profilowanie może prowadzić do podwyższonego poziomu wrogości w innych kontaktach obywateli z policją lub innymi organami ścigania. Większa wrogość może wywołać agresję i konflikt w zwykłych kontaktach, co stwarza problemy dotyczące bezpieczeństwa zarówno dla funkcjonariuszów, jak i dla członków społeczności.

Mówiąc szerzej, ostatnie badania wykazały, że osoby zatrzymane, aresztowane, skazane lub poddane karze więzienia mają tendencję do pozostawania z dala od innych usług publicznych poza systemem sądownictwa karnego, takich jak organizacje zdrowia, zatrudnienia i edukacji[20]. Nie podważając uzasadnionych powodów, które doprowadziły do aresztowania skazanych osób, należy mieć na uwadze, że wykluczenie z takich instytucji już marginalizowanych segmentów populacji może osłabiać włączenie społeczne i integrację grup mniejszości.

20 Brayne, S. (2014), s. 367–391.

Koncentracja na ustaleniach FRA i EU-MIDIS II

W latach 2015 i 2016 FRA zgromadziła informacje od ponad 25 500 respondentów z różnych mniejszości etnicznych lub środowisk imigranckich w 28 państwach członkowskich UE.

Jakie informacje gromadzono?

W odniesieniu do profilowania respondentów pytano, czy uważają, że zostali zatrzymani przez policję ze względu na swoje pochodzenie ze środowisk imigranckich lub mniejszości etnicznej, oraz o sposób, w jaki byli traktowani przez policję, w tym o jakiekolwiek doświadczenia napaści fizycznej ze strony policji. W badaniu nie pytano o kontakty z organami zarządzania granicami.

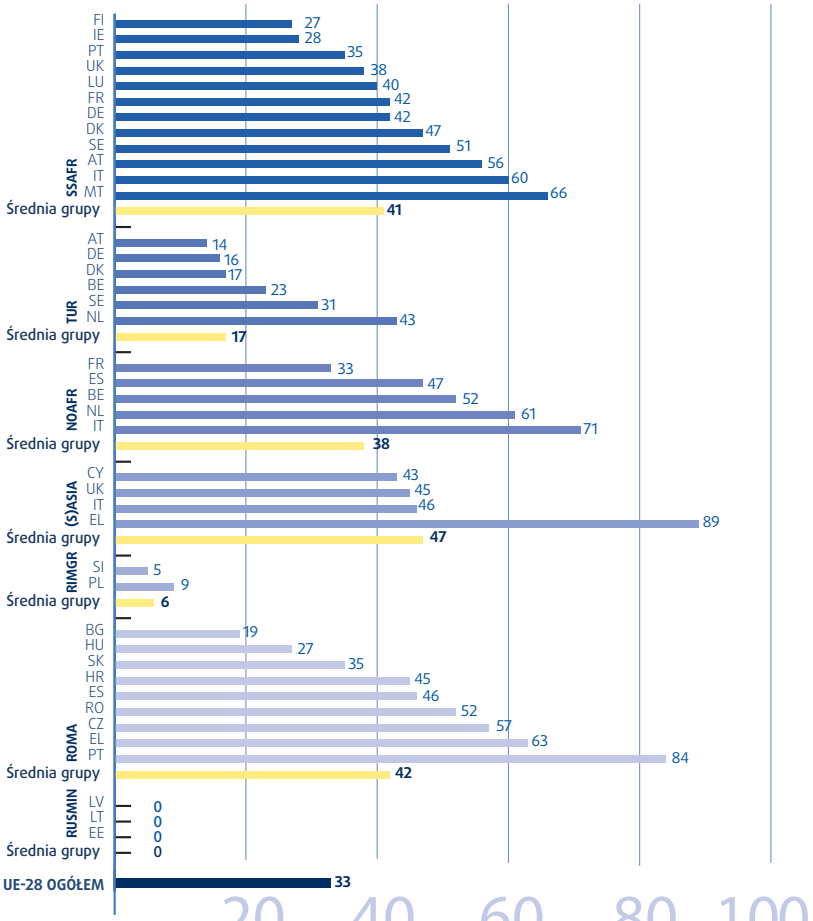
Co pokazują wyniki?

Zatrzymania a pochodzenie etniczne: Wyniki pokazują, że 26 % wszystkich respondentów EU-MIDIS II zostało w ciągu ostatnich pięciu lat przed przeprowadzeniem badania zatrzymanych przez policję. Spośród osób zatrzymanych w ciągu ostatnich pięciu lat przed przeprowadzeniem badania 33 % powiedziało, że powodem było ich pochodzenie etniczne lub pochodzenie ze środowisk imigranckich.

Postrzeganie dyskryminacji: Średnio niemal co drugi respondent pochodzenia azjatyckiego (47 %), subsaharyjskiego (41 %) i północnoafrykańskiego (38 %), który został zatrzymany w przedmiotowym okresie, stwierdził, że powodem zatrzymania było jego pochodzenie ze środowiska imigranckiego lub mniejszości etnicznej. Podobnie wśród zatrzymanych respondentów pochodzenia romskiego niemal co druga osoba (42 %) uważała, że zatrzymanie wynikało z jej pochodzenia etnicznego. Odsetek ten był natomiast znacznie niższy wśród zatrzymanych respondentów pochodzenia tureckiego (17 %) (zob. wykres 3).

Szacunek: Zgodnie z wnioskami z badania większość (59 %) wszystkich respondentów, którzy zostali zatrzymani przez policję w ciągu ostatnich pięciu lat przed przeprowadzeniem badania, czuła, że potraktowano ich z szacunkiem (25 % „z dużym szacunkiem", 34 % „raczej z szacunkiem"). Jeden na czterech respondentów (24 %) stwierdził, że policja „ani nie potraktowała go/jej z szacunkiem, ani nie wykazała braku szacunku".

Wykres 3: Ostatnie zatrzymania przez policję postrzegane jako profilowanie etniczne wśród osób zatrzymanych w ciągu ostatnich pięciu lat przed przeprowadzeniem badania EU-MIDIS II, według państw członkowskich i grup, których dotyczyło badanie (%) [a,b,c,d]



Uwagi: [a] *Spośród respondentów zatrzymanych przez policję w ciągu ostatnich pięciu lat przed przeprowadzeniem badania (n=6787); wyniki ważone.*

[b] *Wyniki oparte na małej liczbie odpowiedzi są statystycznie mniej wiarygodne. W związku z tym wyniki oparte na 20–49 obserwacjach nieważonych w grupie ogółem lub oparte na komórkach o mniej niż 20 obserwacjach nieważonych są podane w nawiasach. Wyniki oparte na mniej niż 20 obserwacjach nieważonych w grupie ogółem nie zostały opublikowane.*

[c] *Pytania: „Czy w ciągu ostatnich pięciu lat w [PAŃSTWO] (lub odkąd jest pan/pani w [PAŃSTWO]) zdarzyło się, aby policja zatrzymała pana/panią, dokonała rewizji lub przesłuchała?"; „Czy uważa pan/pani, że OSTATNIE zatrzymanie było spowodowane pana/pani pochodzeniem etnicznym lub pochodzeniem ze środowisk imigranckich?".*

[d] *Skrótowce dotyczące grup docelowych odnoszą się do imigrantów z [państwa/regionu] i ich potomków: TUR = Turcja, SSAFR = Afryka Subsaharyjska, NOAFR = Afryka Północna, SASIA = Azja Południowa, ASIA = Azja, ROMA = mniejszość romska.*

Źródło: *FRA, 2017b.*

17 % respondentów stwierdziło natomiast, że policja wykazała w stosunku do nich brak szacunku (8 % „raczej brak szacunku" i 9 % „całkowity brak szacunku"). Jak wskazali respondenci pochodzenia romskiego i respondenci pochodzący z Afryki Północnej, którzy zostali zatrzymani, doświadczali oni braku szacunku ze strony policji podczas ostatniego zatrzymania (odpowiednio 25 % i 21 %) częściej niż inne grupy objęte badaniem.

Aby uzyskać więcej informacji, zob. FRA (2017b).

Koncentracja na znaczeniu i przydatności gromadzenia danych na temat zatrzymań przez policję

Zjednoczone Królestwo jest obecnie jedynym państwem spośród 28 państw członkowskich UE, które w gromadzonych danych dotyczących zatrzymań przez policję ujmuje informacje na temat pochodzenia etnicznego zatrzymanych osób (zob. również sekcja 2.2.5 i sekcja 2.3.1).

Na podstawie zgromadzonych danych mierzony jest „wskaźnik zatrzymania i rewizji" w odniesieniu do poszczególnych grup etnicznych w Anglii i Walii. Stosowane kategorie pochodzenia etnicznego odpowiadają kategoriom stosowanym w spisie powszechnym Zjednoczonego Królestwa z 2001 r. W spisie tym określono 16 kategorii, które połączono w pięć szerszych grup:

- rasa biała: pochodzenie angielskie/walijskie/szkockie/północnoirlandzkie/brytyjskie; irlandzkie; każde inne pochodzenie rasy białej,
- pochodzenie mieszane/obejmujące wiele grup etnicznych: rasa biała i czarna pochodzenia karaibskiego; rasa biała i czarna pochodzenia afrykańskiego; rasa biała i azjatycka; każde inne pochodzenie mieszane/obejmujące wiele grup etnicznych,

- Azjaci/Brytyjczycy azjatyckiego pochodzenia: pochodzenie indyjskie; pakistańskie; bangladeskie; każde inne pochodzenie azjatyckie,
- rasa czarna/Afrykanie/Karaibowie/Brytyjczycy rasy czarnej: Afrykanie; Karaibowie; każde inne pochodzenie rasy czarnej/afrykańskie/karaibskie,
- inne grupy etniczne: Chińczycy; inne grupy etniczne.

Wykorzystując zgromadzone dane dotyczące zatrzymania i rewizji, porównano liczbę osób poddanych zatrzymaniu i rewizji pochodzących z konkretnej grupy etnicznej z łączną liczbą osób z tej grupy etnicznej zamieszkujących dany obszar, a następnie obliczono wskaźnik na 1 000 osób.

W odniesieniu do lat 2016–2017 analiza zgromadzonych danych wykazała, że w kategorii osób rasy białej zatrzymano cztery osoby na 1 000, w porównaniu z kategorią osób czarnoskórych, w ramach której zatrzymano 29 osób na 1 000. Dane te wskazują również, że najwyższe wskaźniki dotyczyły trzech grup etnicznych osób czarnoskórych: rasa czarna innego pochodzenia (70 zatrzymań na 1 000 osób), rasa czarna pochodzenia karaibskiego (28 na 1 000 osób) i rasa czarna pochodzenia afrykańskiego (19 na 1 000 osób).

Bez dowodów pochodzących z danych zdezagregowanych trudno jest dowieść istnienia różnic w działaniach policji ukierunkowanych na poszczególne grupy etniczne i – jeżeli takie różnice mają miejsce – tego, że różnice te mogą wynikać ze stosowania praktyk dyskryminacyjnego profilowania. Dane zdezagregowane są dostępne w domenie publicznej w Anglii i Walii w podziale na komendy policji. Umożliwia to identyfikację różnicujących praktyk między organami, które można wyjaśnić jako zgodne z prawem albo wykorzystać do identyfikacji potencjalnej dyskryminacji w praktykach działań policji. Dane wykorzystuje się również na poziomie poszczególnych funkcjonariuszy policji w celu identyfikacji dyskryminacyjnych praktyk w ich pracy.

Aby uzyskać więcej informacji, zob. strona internetowa Gov.uk dotycząca zatrzymania i rewizji, strona internetowa Independent Office for Police Conduct i strona dotycząca otwartych danych na temat przestępstw i działań policji brytyjskiego Home Office. Zob. również Zjednoczone Królestwo (2018). Aby uzyskać wytyczne na temat metod rejestrowania danych, zob. Open Society Justice Initiative (2018b).

Analiza przykładów

Badanie na temat stosunków między policją a społeczeństwem we Francji

W 2016 r. francuski rzecznik praw obywatelskich (*Défenseur des droits*) przeprowadził badanie na temat dostępu do praw. *Défenseur des droits* działa również w roli krajowej komisji ds. skarg na policję. Badanie obejmowało reprezentatywną próbę ponad 5 000 osób.

W pierwszej części sprawozdania przedstawiono wyniki związane z zachowaniem organów ścigania. W ogólnym ujęciu badanie wskazuje na dobre stosunki między społeczeństwem a policją. Przeważająca większość respondentów stwierdziła, że ma zaufanie do policji (82 %).

Konkretnie w kwestii kontroli tożsamości badanie wykazało, że większość osób nie doświadcza takich kontroli: 84 % respondentów twierdziło, że nie skontrolowano ich ani razu w ciągu ostatnich pięciu lat (90 % kobiet i 77 % mężczyzn). Osoby, które potwierdziły, że były kontrolowane, ogólnie zgłosiły niewiele przypadków zachowań naruszających etykę zawodową sił bezpieczeństwa podczas ostatniej kontroli tożsamości, takich jak nieformalny sposób zwracania się (16 %), brutalne zachowanie (8 %), czy stosowanie obraźliwych zwrotów (7 %). 29 % tych osób zgłosiło jednak, że funkcjonariusze nie byli uprzejmi, a ponad połowa kontrolowanych respondentów (59 %) stwierdziła, że nie wyjaśniono im powodów kontroli. Co do zasady kontrole tożsamości postrzega się jako bardziej uzasadnione, gdy siły bezpieczeństwa poświęcają chwilę na wyjaśnienie powodów prowadzenia kontroli.

Z danych wynika również, że konkretne grupy osób zgłaszają bardziej negatywne doświadczenia. W przypadku młodych mężczyzn w przedziale wiekowym 18–24 lata prawdopodobieństwo doświadczania częstych kontroli tożsamości (tj. ponad pięć razy w ciągu ostatnich pięciu lat) jest niemal siedem razy wyższe niż u ogółu społeczeństwa, a w przypadku mężczyzn postrzeganych jako czarnoskórzy lub jako Arabowie częste kontrole tożsamości są od sześciu do 11 razy bardziej prawdopodobne niż w przypadku reszty populacji mężczyzn. Po połączeniu tych dwóch kryteriów okaże się, że 80 % mężczyzn poniżej 25. roku życia i postrzeganych jako Arabowie lub osoby czarnoskóre skontrolowano przynajmniej raz w ciągu ostatnich pięciu lat (w porównaniu z 16 % w przypadku innych respondentów).

W porównaniu z ogółem populacji w grupie tej istnieje dwudziestokrotnie większe prawdopodobieństwo kontroli tożsamości.

Dodatkowo młodzi mężczyźni postrzegani jako osoby czarnoskóre lub Arabowie zgłaszali wyższe poziomy problematycznych zachowań podczas ostatniej kontroli tożsamości, takich jak stosowanie nieformalnego sposobu zwracania się (40 % w porównaniu z 16 % w próbie ogółem), stosowanie obraźliwych zwrotów (21 % w porównaniu z 7 % w próbie ogółem) lub brutalne zachowanie (20 % w porównaniu z 8 % w próbie ogółem). Te negatywne doświadczenia i częstotliwość kontroli wiążą się z niskim poziomem zaufania do policji. Grupa ta istotnie zgłaszała pogarszające się stosunki z policją.

Ponadto wyniki wskazują, że niewielu respondentów (5 %), którzy wskazali naruszenie etyki zawodowej podczas kontroli tożsamości, podejmuje kroki, aby zgłosić taką sytuację. Wskazują oni przede wszystkim, że powodem, dla którego nie zgłaszają swoich doświadczeń, jest fakt, że uznają takie kroki za bezużyteczne.

Aby uzyskać więcej informacji, zob. Défenseur des droits (2017).

Jeżeli w stosunku do mniejszości stosuje się szerokie profile, może to, w połączeniu z innymi działaniami stygmatyzującej polityki, prowadzić do sytuacji, w której grupa ta zacznie postrzegać wewnętrznie samą siebie w sposób negatywny. Dodatkowo szersza społeczność może przyjąć negatywne postrzeganie tej grupy. Mniejszość może stać się „podejrzaną społecznością", którą społeczeństwo będzie kojarzyło z przestępczością[21]. Może to prowadzić do wzrostu uprzedzeń.

Nieproporcjonalna ilość zasobów policji może zostać ukierunkowana na tę mniejszość, co z kolei może prowadzić do wyższej liczby aresztowań lub kontroli na granicy. W rezultacie może dojść do sytuacji, w której stosunek między intensywnymi działaniami policji i wyższym wskaźnikiem aresztowań będzie się sam wypełniał[22].

21 Europejskie Centrum Monitorowania Rasizmu i Ksenofobii (2006), s. 54.

22 Harcourt, B. (2004), s. 1329–1330; House of Commons Home Affairs Committee (2009), pkt 16; i ONZ (2007).

Koncentracja na ryzyku „samospełniającej się przepowiedni”

Jeżeli funkcjonariusze policji nie mają uzasadnionych podstaw do profilowania, lecz opierają się na uprzedzeniach, istnieje prawdopodobieństwo, że będą interpretować informacje w sposób potwierdzający te uprzedzenia. Zjawisko takie nazywa się „efektem potwierdzenia”. Ma ono miejsce, gdy uprzedzenia funkcjonariuszy policji oznaczają, że na podstawie rzeczywistej lub postrzeganej rasy, pochodzenia etnicznego, płci, orientacji seksualnej, religii lub innych cech chronionych danej osoby oczekują oni, że osoba ta będzie postępowała niezgodnie z prawem. Ze względu na tego rodzaju tendencyjność funkcjonariusze posiadający takie uprzedzenia będą z większym prawdopodobieństwem wyróżniać więcej osób pasujących do ich opisu.

Ponieważ istnieje większe prawdopodobieństwo wykrycia dowodów na popełnienie przestępstwa wśród osób zatrzymanych niż wśród osób, które nie zostały zatrzymane, takie profilowanie oparte na uprzedzeniach dodatkowo wzmacnia istniejące już stereotypy funkcjonariusza. Taki fałszywy „dowód” na to, że decyzja o zatrzymaniu danych osób była

Wykres 4: Cykl samospełniającej się przepowiedni

Źródło: FRA, 2018.

właściwa, nazywany jest „samospełniającą się przepowiednią". Tego rodzaju profilowanie oparte na uprzedzeniach jest dyskryminujące, niezgodne z prawem i utrwala stereotypy.

Na wykresie 4 opisano sposób, w jaki „samospełniająca się przepowiednia" utrwala kryminalizację osób.

1.3.2. Skuteczność profilowania

Istnieją również wątpliwości co do skuteczności wykorzystywania profilowania opartego na szerokich kategoriach do celów wykrywania przestępstw. Nie jest jasne, czy profilowanie rzeczywiście zwiększa skuteczność (lub „wskaźnik trafień") operacji ścigania przestępstw.

Niektóre dowody wskazują na to, że wskaźniki zatrzymywania osób niekoniecznie odpowiadają wskaźnikom występowania naruszeń wśród poszczególnych grup etnicznych lub rasowych (zob. ramka). Należy zauważyć, że dane pochodzące z wymiaru sprawiedliwości w sprawach karnych w większości państw członkowskich UE nie umożliwiają dokonania przeglądu postępów poszczególnych spraw w ramach systemu sądownictwa karnego. W związku z tym nie można określić, czy aresztowanie doprowadziło do postawienia oskarżenia i do wydania wyroku skazującego.

Analiza przykładów

Zmiana wzorca rewizji prowadząca do wyższego „wskaźnika trafień" (1998–2000, USA)

W 1998 r. 43 % rewizji prowadzonych przez władze celne Stanów Zjednoczonych (US Customs) dotyczyło osób czarnoskórych i osób pochodzenia latynoskiego, co stanowi znacznie wyższy wskaźnik niż odsetek tych osób wśród podróżnych. Szczególnie dużą liczbę rewizji, w tym wysoce inwazyjne prześwietlanie promieniowaniem rentgenowskim i rewizje osobiste, przeprowadzono na Latynoskach i czarnoskórych kobietach podejrzanych o bycie tzw. „kurierami narkotykowymi". Działania te prowadzono w oparciu o profil bazujący w znacznym stopniu na narodowości i pochodzeniu etnicznym. Wskaźniki trafień dotyczące tych rewizji były niskie we wszystkich grupach: 5,8 % wśród „osób białych", 5,9 % wśród „osób czarnoskórych" i 1,4 % wśród „Latynosów".

Szczególnie niski wskaźnik dotyczył kobiet pochodzenia latynoskiego, które w rzeczywistości najrzadziej przewoziły narkotyki na ciele lub wewnątrz ciała. W 1999 r. władze celne zmieniły procedury, usuwając rasę spośród czynników, które należy uwzględnić podczas zatrzymań. W zamian wprowadzono techniki obserwacyjne koncentrujące się na takich zachowaniach, jak nerwowość i niespójności w wyjaśnieniach pasażerów, wykorzystanie większej ilości informacji wywiadowczych i ściślejszy nadzór nad decyzjami dotyczącymi zatrzymania i rewizji. Do 2000 r. praktycznie wyeliminowano różnice rasowe podczas rewizji celnych. Liczba przeprowadzonych rewizji zmalała o 75 %, a wskaźnik trafień wzrósł z nieco poniżej 5 % do ponad 13 % i stał się prawie równy dla wszystkich grup etnicznych.

Aby uzyskać więcej informacji, zob. Harris (2002), USA (2000).

Nieskuteczność niegodnego z prawem profilowania (2007–2008, Węgry)

Badanie przeprowadzone na Węgrzech wykazało nieproporcjonalną liczbę kontroli tożsamości ukierunkowanych na osoby pochodzenia romskiego. Około 22 % wszystkich osób kontrolowanych przez policję należało do społeczności romskiej, tymczasem odsetek osób pochodzenia romskiego w ogólnej populacji wynosił ok. 6 %. Nieproporcjonalnie wysoka liczba kontroli tożsamości Romów nie znajdowała odzwierciedlenia w dowodach dotyczących zachowań niezgodnych z prawem: 78 % kontroli tożsamości osób pochodzenia romskiego nie skutkowało podjęciem jakichkolwiek działań przez policję, a 19 % było powiązane z drobnymi wykroczeniami* (w porównaniu z 18 % kontroli w populacji ogółem). Ponadto wskaźniki aresztowań w odniesieniu do społeczności romskiej i do populacji ogółem były podobne.

Aby uzyskać więcej informacji, zob. Tóth, B.M. i Kádár, A. (2011).

* „Drobne wykroczenia to quasi-przestępstwa, których powaga nie ma znamion przestępstwa kryminalnego (tj. nie są one regulowane w kodeksie karnym). Drobne wykroczenia plasują się między wykroczeniami, za które kara wynosi 60 dni kary więzienia, takimi jak prostytucja czy groźby użycia przemocy, a wykroczeniami karalnymi za pomocą łagodniejszych środków (np. grzywny, konfiskaty mienia czy zakazu wejścia na niektóre wydarzenia). Przykładami takich wykroczeń są drobne kradzieże czy wykroczenia naruszające kodeks drogowy". *Zob. Kádár, A., Körner, J., Moldova, Z. i Tóth, B. (2008), s. 23.*

Pojawiają się również pytania dotyczące powodów zatrzymywania niektórych osób. W badaniu przeprowadzonym przez Zjednoczone Królestwo zgłoszono, że „[a]larmujący odsetek 27 % (2 338) zbadanych zapisów zatrzymania i rewizji [...] nie obejmował uzasadnionych podstaw do przeprowadzenia rewizji, mimo że wiele spośród tych zapisów zostało popartych przez przełożonych”[23]. Jak wskazano w badaniu, sugeruje to, że „możliwe, że organy policyjne nie postępują w pełni zgodnie z wymogami dotyczącymi równości w sektorze publicznym, które wymagają od nich należytego uwzględniania konieczności eliminowania niezgodnej z prawem dyskryminacji i promowania równości szans, budowania dobrych relacji; w tym celu organy te muszą zapewniać odpowiednie gromadzenie, analizowanie i publikowanie danych w celu wykazania, że posiadają wystarczające informacje pozwalające na zrozumienie efektów ich pracy”.

23 Zjednoczone Królestwo, Her Majesty’s Inspectorate of Constabulary (HMIC), (2013), s. 6.

2

Zgodne z prawem profilowanie: zasada i praktyka

W niniejszym rozdziale skupiono się na profilowaniu stosowanym przez policję pierwszej linii kontroli, w szczególności na działaniach zatrzymania i rewizji, oraz przez funkcjonariuszy zarządzania granicami, w szczególności na kierowaniu do dalszych kontroli drugiej linii na granicy. Wyjaśniono w nim główne zasady i praktyki, które mogą pomóc w ograniczeniu ryzyka prowadzenia niezgodnego z prawem profilowania. Środki te można podejmować zarówno na szczeblu zarządzania, jak i na szczeblu operacyjnym. W niniejszym rozdziale uwzględniono różne prawne i praktyczne konteksty działań zatrzymania i rewizji i kontroli na granicy.

W kontekście zarządzania granicami w kodeksie granicznym Schengen (rozporządzeniu (UE) 2016/399)[24] ustanowiono jednolite zasady regulujące kontrole na granicach zewnętrznych UE. Oznacza to, że niektóre zasady przedstawione w niniejszym rozdziale – na przykład dotyczące informacji, których należy udzielić obywatelom państw trzecich poddanym kontroli drugiej linii – są przewidziane w prawie i mają charakter wiążący dla państw członkowskich. Ponadto Frontex pełni istotną rolę w promowaniu niezmiennie wysokich standardów kontroli na granicy. W szczególności w rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej z 2016 r. wymaga się od państw członkowskich, aby podczas szkoleń straży granicznej korzystały ze wspólnego podstawowego programu szkoleń opracowanego przez Frontex. Wspólny podstawowy program szkoleń (*Common Cure Curriculum*), który opublikowano w 2012 r., zawiera cześć dotyczącą praw podstawowych, w której ujęto również kwestię profilowania (zob. sekcja 2.2.3 dotycząca ukierunkowanego szkolenia).

24 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen), Dz.U. L 77 z 23.3.2016.

Koncentracja na podstawach skierowania do kontroli drugiej linii na granicy

Regularny charakter kontroli na granicy oznacza, że każdy podróżny poddawany jest podstawowej kontroli pierwszej linii, podczas której sprawdzane są dokumenty podróży i wszelkie inne warunki wjazdu na terytorium. Dodatkowo niektórzy podróżni mogą zostać skierowani do dalszej kontroli drugiej linii. Może się tak stać z wielu powodów: trafienie w bazie danych, podejrzany dokument podróży, dopasowanie do profilu ryzyka, czy podejrzane zachowanie.

Podczas kontroli pierwszej linii funkcjonariusz straży granicznej może opierać się na informacjach uzyskanych dzięki porównaniu danych z dokumentu podróży odczytywanego maszynowo (który zawiera identyfikatory biometryczne) z danymi przechowywanymi w krajowych, unijnych i międzynarodowych bazach danych, takich jak system informacyjny Schengen, wizowy system informacyjny oraz bazy danych Europolu i Interpolu. W praktyce skierowanie do kontroli drugiej linii często jest konsekwencją trafienia w jednej z baz danych.

Osobę można jednak również skierować do kontroli drugiej linii z innych powodów, na przykład gdy pasuje ona do profilu ryzyka lub gdy funkcjonariusz ma inne podejrzenia dotyczące danej osoby. W katalogu schengeńskim UE określono, że oprócz prowadzenia kontroli na granicy zgodnie z kodeksem granicznym Schengen, celem kontroli pierwszej linii powinno być profilowanie pasażerów i wybieranie podejrzanych osób do dokładniejszej kontroli drugiej linii*. Funkcjonariusze straży granicznej muszą zatem dokonać oceny kombinacji innych czynników i kryteriów, aby ustalić, czy dana osoba może usiłować przekroczyć nielegalnie granicę, może stwarzać zagrożenie dla bezpieczeństwa lub, na przykład, może być ofiarą handlu ludźmi. Niezależnie od tego, czy stosują oni konkretny istniejący profil ryzyka, w sytuacjach takich straż graniczna korzysta z profilowania.

Konieczność zapewnienia płynnego przepływu podróżnych oznacza, że funkcjonariusze straży granicznej mają ograniczony czas na dokonanie obiektywnej oceny w kwestii poddania osoby kontroli drugiej linii. Zgodnie z informacjami z Frontexu funkcjonariusze w państwach członkowskich UE mają średnio jedynie 12 sekund na podjęcie decyzji o skierowaniu osoby do dalszej kontroli**. Wywiera to na nich ogromną presję szybkiego podejmowania właściwych decyzji.

* *Rada Unii Europejskiej (2009), zalecenie 43.*
** *Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) (2015).*

Zasady i praktyczne narzędzia ujęte w niniejszym rozdziale stanowią źródło informacji mających zachęcić do dyskusji i do działań, które mogą pomóc funkcjonariuszom i ich większym organizacjom w utrzymaniu działań profilowania w obrębie prawa. Trzy główne omawiane zasady to:

- poszanowanie godności osoby;
- zapewnienie rozsądnych i obiektywnych podstaw profilowania;
- gwarancja odpowiedzialności.

U podstaw każdej z zasad leży zapewnienie, aby stosując profilowanie, funkcjonariusze policji i straży granicznej działali zgodnie z prawem.

2.1. Poszanowanie godności osoby

Najważniejsze kwestie

- Zapewnienie **dobrej jakości kontaktu** nie wyeliminuje samo w sobie dyskryminacyjnego profilowania. Istnieje jednak prawdopodobieństwo, że kontakt taki będzie bardziej udany, a możliwe negatywne skutki zatrzymania i rewizji będą mniejsze. W odniesieniu do zarządzania granicami zachowanie okazujące profesjonalizm i szacunek stanowi obowiązek prawny.
- **Zachowanie okazujące profesjonalizm i szacunek** zwiększa co do zasady zadowolenie osoby związane ze spotkaniem.
- **Wyjaśnienie osobie powodów zatrzymania** pomaga w zwiększeniu zaufania względem operacji prowadzonych przez policję i organy zarządzania granicami oraz ogranicza postrzeganie profilowania jako dyskryminacyjnego.
- Szacunek i uprzejmość **nie mogą nigdy stanowić uzasadnienia dla niezgodnych z prawem kontroli granicznych i działań zatrzymania i rewizji**.

Szacunek dla godności człowieka jest nie tylko sam w sobie prawem podstawowym, lecz stanowi również podstawową zasadę operacji policji i operacji związanych z zarządzaniem granicami. Podczas operacji pierwszego kontaktu policja i funkcjonariusze zarządzający granicami rozmawiają z zatrzymanymi osobami i wchodzą z nimi w relacje, a przedstawiane przez nich informacje są kluczowe.

Należy zawsze pamiętać, że bez względu na to, jak uprzejmie i profesjonalnie zachowują się funkcjonariusze, selekcja osób jest wciąż doświadczeniem o inwazyjnym charakterze i jej podstawy muszą być zawsze zgodne z prawem. Postrzeganie profilowania jako dyskryminującego wiąże się również z częstotliwością i liczbą interakcji z policją i z organami zarządzania granicami. Sprawia to, że zapewnienie, aby zawsze istniały obiektywne i rozsądne podstawy zatrzymania, ma tym większe znaczenie.

Co mówią normy?

„Odprawa graniczna powinna być dokonywana w sposób zapewniający pełne poszanowanie godności osoby ludzkiej. Kontrola graniczna powinna być przeprowadzana profesjonalnie i z zachowaniem szacunku oraz powinna być proporcjonalna do założonych celów".

Motyw 7 kodeksu granicznego Schengen

„Wszyscy podróżni mają prawo do informacji na temat charakteru kontroli oraz do profesjonalnego, życzliwego i uprzejmego traktowania w zgodzie z obowiązującym prawem międzynarodowym, wspólnotowym i krajowym".

Sekcja 1.2 Praktycznego podręcznika dla straży granicznej (podręcznika Schengen)

„Funkcjonariusze policji działają uczciwie i z poszanowaniem społeczeństwa oraz ze szczególnym uwzględnieniem sytuacji jednostek należących do grup szczególnie wymagających ochrony".

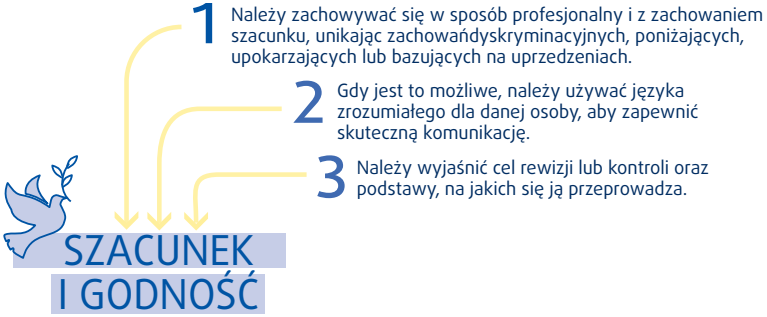
Zalecenie 44 europejskiego kodeksu etyki zawodowej policji

Zapewnienie, aby funkcjonariusze policji i straży granicznej byli uprzejmi i udzielali informacji w napiętych i trudnych sytuacjach, nie zawsze jest łatwym zadaniem. Dowody wskazują jednak, że przyjmowanie tonu wyrażającego szacunek znacznie zwiększa poziom zadowolenia ze spotkania[25]. Na wykresie 5 zilustrowano niektóre elementy spotkania przeprowadzonego z zachowaniem szacunku.

Niektóre elementy kontroli na granicy są uregulowane w kodeksie granicznym Schengen, np. wymogi dotyczące przeprowadzania kontroli w sposób profesjonalny i z zachowaniem szacunku lub udzielenia informacji o celu i procedurze odprawy (motyw 7, art. 7 i art. 8 ust. 5 kodeksu granicznego Schengen). Posługiwanie się

25 FRA (2014b).

Wykres 5: Trzy elementy spotkania przeprowadzonego z zachowaniem szacunku



Źródło: FRA, 2018.

tym samym językiem nie stanowi natomiast bezwzględnego wymogu w kontekście zarządzania granicami z uwagi na zróżnicowany charakter, jaki nieodłącznie wiąże się z ruchem granicznym. W kodeksie granicznym Schengen wymaga się jednak, aby państwa członkowskie zachęcały funkcjonariuszy straży granicznej do nauki języków niezbędnych do wykonywania ich zadań (art. 16 ust. 1). W katalogu schengeńskim, który zawiera zestaw zaleceń i najlepszych praktyk dotyczących kontroli granic zewnętrznych, zaleca się również, aby straż graniczna posiadała umiejętności komunikacji w językach obcych związanych z ich codziennymi obowiązkami. Jako najlepszą praktykę podaje się zadowalający poziom znajomości języków państw sąsiadujących, a także innych języków w zależności od charakteru ruchu granicznego. Najlepiej, gdyby podczas każdej zmiany obecni byli funkcjonariusze posiadający odpowiednie umiejętności językowe[26].

Brak zrozumienia i szacunku podczas zatrzymania przez policję może bezpośrednio wpływać na skuteczność działań policji (zob. sekcja 1.3.2). W opracowanym w Zjednoczonym Królestwie kodeksie dobrych praktyk ustawy o policji i dowodach w sprawach karnych stwierdza się: „Wszystkie zatrzymania i rewizje należy prowadzić w sposób uprzejmy, okazując zatrzymanej osobie zrozumienie i szacunek. Ma to istotny wpływ na zaufanie społeczne do policji. Należy dołożyć wszelkich rozsądnych starań, aby zminimalizować zażenowanie, jakiego może doświadczać przeszukiwana osoba”[27].

26 Rada Unii Europejskiej (2009), zalecenia 27 i 41.

27 Zjednoczone Królestwo, Home Office (2014a), sekcja 3.1.

Niektóre istotne elementy poszanowania godności, takie jak przedstawienie wyjaśnień powodu zatrzymania i zapewnienie, aby osoby miały możliwość wyrażenia swoich poglądów, to podstawowe części procedur policyjnych i z zakresu zarządzania granicami. Formularze zatrzymania i rewizji mogą być pomocne w przedstawianiu tych informacji w sposób zorganizowany (zob. sekcja 2.3.1).

W kontekście zarządzania granicami standaryzowane formularze stanowią przydatne narzędzia informowania podróżnych o celu i procedurze kontroli drugiej linii. Mogą one ułatwić komunikację z podróżnymi, pod warunkiem że w razie potrzeby towarzyszą im lub uzupełniają je ustne wyjaśnienia. W kodeksie granicznym Schengen wymaga się, aby osoby podlegające kontroli drugiej linii otrzymywały pisemne informacje dotyczące celu i procedury kontroli w zrozumiałym dla nich języku lub w języku, co do którego można rozsądnie przypuszczać, że jest dla nich zrozumiały. Informacje te powinny:

- być dostępne we wszystkich językach urzędowych UE oraz w językach państw sąsiadujących z państwem, którego dotyczą;

- wskazywać, że podróżny może zażądać podania nazwiska lub numeru identyfikacyjnego funkcjonariusza dokonującego kontroli, nazwy przejścia granicznego i daty przekroczenia granicy.

Wymienione elementy kontaktu odbywającego się z zachowaniem szacunku, związane z komunikacją i umiejętnościami interpersonalnymi, trudniej jest wprowadzać do procedur operacyjnych i mogą one wymagać większych inwestycji w szkolenia. Trudności w nadawaniu spotkaniu pozytywnego tonu mogą wynikać z:

- ograniczonych umiejętności komunikacyjnych;

- braku umiejętności wyrażenia celu działania; oraz

- braku umiejętności przezwyciężenia własnych lub instytucjonalnych uprzedzeń i negatywnych stereotypów, a także narosłej wrogości w obrębie niektórych części społeczności.

2.2. Rozsądne i obiektywne podstawy

Najważniejsze kwestie

- Gdy ściganie przestępstw i prowadzenie działań związanych z zarządzaniem granicami odbywają się w oparciu o określone i aktualne dane wywiadowcze, mają one większe szanse na bycie obiektywnymi.
- Działania zatrzymania i rewizji i skierowanie do kontroli drugiej linii, aby były zgodne z prawem, muszą **mieć uzasadnione i obiektywne podstawy** do podejrzeń. „Instynktowne przeczucie" nie stanowi rozsądnej ani obiektywnej podstawy, aby zatrzymać osobę i poddać ją rewizji, czy też aby skierować osobę do kontroli drugiej linii na granicy.
- Cechy chronione, takie jak rasa, pochodzenie etniczne, płeć lub religia, mogą znaleźć się wśród czynników uwzględnianych przez organy ścigania i straż graniczną w celu wykonywania swoich uprawnień, **nie mogą one jednak stanowić jedynego lub głównego powodu wyróżnienia osoby**.
- Profilowanie wyłącznie lub głównie na podstawie cechy chronionej lub większej liczby takich cech stanowi bezpośrednią dyskryminację i jest niezgodne z prawem.

Obiektywność to istotna zasada pracy policji i organów zarządzania granicami. W kontekście profilowania zatrzymywanie i rewizja osób lub poddawanie ich kontroli drugiej linii na granicy powinny odbywać się wyłącznie na podstawie rozsądnych i obiektywnych podejrzeń. Obiektywne uzasadnienie może obejmować zachowanie danej osoby, szczegółowe dane wywiadowcze lub okoliczności wiążące osobę lub osoby z podejrzanymi nielegalnymi działaniami.

Aby zapewnić obiektywizm w profilowaniu, należy:

- unikać uprzedzeń, w tym dzięki jasnym wytycznym i ukierunkowanym szkoleniom; oraz
- skutecznie wykorzystywać dane wywiadowcze i posiadane informacje.

2.2.1. Unikanie uprzedzeń

W europejskim kodeksie etyki zawodowej policji przedstawiono wytyczne dotyczące postępowania policji w obszarach obejmujących akcje i interwencje policyjne, odpowiedzialność policji i nadzór policji[28]. Podkreślono w nich ogólną zasadę, zgodnie z którą: „[p]olicja, kierując się w szczególności zasadami niezależności i niedyskryminacji, uczciwie wykonuje obowiązki"[29].

Jeżeli przy wyróżnianiu osób *jako jedyny lub decydujący czynnik* uwzględnia się ich rzeczywistą lub postrzeganą rasę, pochodzenie etniczne, płeć, orientację seksualną, religię, niepełnosprawność lub inne cechy chronione, stanowi to naruszenie praw podstawowych. Może to również mieć istotne negatywne konsekwencje, zarówno dla organów publicznych, jak i dla społeczności (zob. sekcja 1.3).

Dyskryminacyjne profilowanie może odzwierciedlać zarówno indywidualne, jak i instytucjonalne uprzedzenia. Oprócz osobistych uprzedzeń, stereotypy i dyskryminacyjne zachowanie względem osób mogą wynikać z konkretnych praktyk stosowanych przez organy ścigania i organy zarządzania granicami. Zwiększenie przejrzystości procedur i praktyk instytucjonalnych może pomóc w walce z dyskryminacją i z utrwalaniem stereotypów.

Uznanie głęboko zakorzenionych uprzedzeń może być trudne. Funkcjonariusze policji i funkcjonariusze zarządzania granicami mogą uważać, że wyróżniają osoby w oparciu o rozsądne i obiektywne podstawy (takie jak zachowanie), tymczasem decyzje te odzwierciedlają w rzeczywistości ich uprzedzenia.

Zatrzymując osoby, funkcjonariusze często wiążą powód wyróżnienia tej konkretnej osoby z „instynktownym przeczuciem" lub „intuicją". Istnieje prawdopodobieństwo, że podstawą tego przeczucia jest połączenie wiedzy fachowej i przeszłych doświadczeń, mogą one jednak również odzwierciedlać świadome lub podświadome uprzedzenia funkcjonariusza. Aby uniknąć niezgodnego z prawem profilowania, funkcjonariusze powinni zastanowić się nad tym, czy ich decyzja znajduje uzasadnienie w obiektywnych informacjach. „Instynktowne przeczucie" nie stanowi rozsądnej ani obiektywnej podstawy, aby zatrzymać osobę i poddać ją rewizji, czy aby skierować osobę do dokładniejszej kontroli na granicy.

28 Rada Europy, Komitet Ministrów (2001), Zalecenie Rec(2001) 10 Komitetu Ministrów dla państw członkowskich dotyczące europejskiego kodeksu etyki zawodowej policji, 19 września 2001 r.

29 *Ibid.*, pkt 40.

2.2.2. Jasne wytyczne dla funkcjonariuszy

Praktyczne, zrozumiałe i gotowe do zastosowania wytyczne mają szczególne znaczenie, jeżeli chodzi o pomoc funkcjonariuszom organów ścigania i funkcjonariuszom zarządzającym granicami prowadzącym kontrole pierwszej linii w unikaniu niezgodnego z prawem profilowania. Wytyczne mogą przybierać wiele form: mogą być dołączone do aktów prawnych, wydane przez same organy ścigania i organy zarządzania granicami lub dostarczane na co dzień przez starszych funkcjonariuszy. Wykorzystywanie autentycznych przykładów, aby pokazać, co robić w konkretnych sytuacjach, może być skuteczniejsze od wyjaśniania zasad i procedur.

Funkcjonariusze piastujący stanowiska kierownicze muszą informować swój personel, że rzeczywista lub postrzegana rasa, pochodzenie etniczne, płeć, orientacja seksualna, religia lub inne cechy chronione będące podstawą dyskryminacji nie mogą być decydującym czynnikiem pozwalającym na rozpoczęcie działania względem osoby w zakresie ścigania przestępstw lub zarządzania granicami. Wyjaśnienie, kiedy i w jaki sposób można wykorzystywać cechy osobowe, może pomóc w ograniczeniu ryzyka wystąpienia różniących się interpretacji, a także polegania na stereotypach i uprzedzeniach. Wytyczne powinny obejmować również kwestie związane z prywatnością i ochroną danych.

W tabeli 3 przedstawiono niektóre rodzaje wytycznych, które można zastosować, i istotne cechy, które należy wziąć pod uwagę.

Tabela 3: Rodzaje i cechy wytycznych i zaangażowanie zainteresowanych stron

Rodzaje wytycznych	Cechy wytycznych	Zaangażowanie zainteresowanych stron

• obowiązujące procedury działania
• kodeksy postępowania
• regularne wytyczne od starszych funkcjonariuszy
	• szczegółowe i konkretne
	• obejmujące wszystkie działania, w ramach których może pojawić się profilowanie na podstawie uprzedzeń:
	  • zatrzymanie i rewizja
	  • aresztowania
	  • kontrole na granicy
	  • użycie siły itp.
		• opracowanie wytycznych we współpracy z innymi zainteresowanymi stronami
		• udostępnienie wytycznych społecznościom
		• zachęcanie społeczności do przedstawienia informacji zwrotnych na temat wytycznych

Źródło: FRA, 2018.

Analiza przykładów

Kodeks dobrych praktyk i podejście wprowadzające ambasadorów (policja niderlandzka)

Niderlandzka policja opracowała wraz z organizacjami społeczeństwa obywatelskiego, takimi jak Amnesty International, kodeks dobrych praktyk, w którym opisała cztery zasady profesjonalnego zatrzymania:

- ☑ zgodny z prawem i uzasadniony wybór osób;
- ☑ wyjaśnienie powodu zatrzymania i rewizji;
- ☑ stosowanie profesjonalnej komunikacji;
- ☑ funkcjonariusze zastanawiający się nad swoimi praktykami i wymieniający między sobą informacje zwrotne.

Zmiana praktyk, których nie postrzega się jako problematyczne, np. praktyki proaktywnych działań policji mogących prowadzić do profilowania etnicznego, jest trudna. Policja w Amsterdamie opracowała podejście oddolne, zgodnie z którym w zespołach uczestniczą funkcjonariusze terenowi (ambasadorzy) wspierani przez swoich kierowników i szkoleniowców. Pierwszym etapem jest podnoszenie świadomości poprzez pokazanie wpływu proaktywnych zatrzymań na zatrzymywane osoby i omówienie tego wpływu, a także poprzez wprowadzenie alternatywnych sprawiedliwych i skutecznych ram odniesienia. W drugim etapie funkcjonariusze mają przyjąć tę nową praktykę.

Aby uzyskać więcej informacji w języku niderlandzkim, zob. strona internetowa policji.

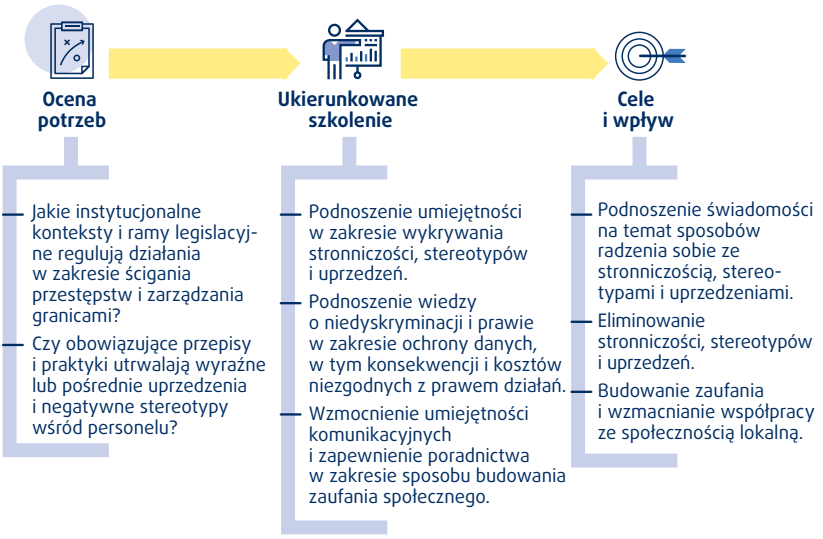
2.2.3. Ukierunkowane szkolenie

Szkolenia dla funkcjonariuszy policji i straży granicznej stanowią kolejne ważne narzędzie służące minimalizowaniu ryzyka niezgodnego z prawem profilowania. Istnieje wiele różnych rodzajów szkoleń, które można prowadzić na różnych etapach kariery funkcjonariusza, w tym: wstępne szkolenie rekrutacyjne, doskonalenie zawodowe i ustawiczny rozwój zawodowy. Niezależnie od rodzaju szkolenia moduły szkoleniowe powinny uwzględniać kulturę organizacyjną i oferować szkolenia, które obejmują strategie zastępowania stereotypów i walki z nimi. Ponadto ocena

wpływu szkolenia jest kluczowa, aby monitorować, jak szkolenie przyczyniło się do zmiany postrzegania przez funkcjonariuszy i poprawy ich praktyk, oraz aby zidentyfikować luki wymagające dalszego szkolenia. Na wykresie 6 uwydatniono niektóre kwestie, które należy rozważyć przy opracowywaniu ukierunkowanego szkolenia.

Niektóre rodzaje szkoleń dla organów ścigania i straży granicznej, np. „szkolenia w zakresie różnorodności" i „szkolenia w zakresie wrażliwości" są już dobrze rozwinięte w niektórych państwach. Szkolenia w zakresie różnorodności mają się odnosić do uczuć związanych z pochodzeniem etnicznym, różnicami i stereotypami oraz do ich wpływu na nasze codzienne życie. Niektóre kursy w zakresie różnorodności nie omawiają jednak zagadnienia dyskryminacji. Niektóre badania wskazują, że szkolenie kulturowe oraz w zakresie różnorodności może w rzeczywistości uwidocznić i wzmocnić różnice, przyczyniając się do powstawania, a nie do zwalczania stereotypów[30]. „Szkolenie w zakresie wrażliwości kulturowej" (w przeciwieństwie do „ogólnego szkolenia w zakresie różnorodności") ma na celu dostarczenie funkcjonariuszom policji i organów ścigania wiedzy na temat kultury szczególnych grup etnicznych, z którymi funkcjonariusze często mają kontakt, ale których nie znają

Wykres 6: Proces i cele opracowywania ukierunkowanego szkolenia



Źródło: FRA, 2018.

30 Wrench, J. (2007).

osobiście. Szkolenie takie obejmuje zalecenia, co należy, a czego nie należy robić, i zawiera wytyczne dotyczące uprzejmości z różnych perspektyw etnicznych, religijnych lub narodowych. Szkolenie w zakresie wrażliwości kulturowej jest najbardziej skuteczne, jeżeli opracowuje się je i prowadzi z pomocą i udziałem osób z odnośnych społeczności.

Analiza przykładów

Szkolenie dotyczące zgodnego z prawem profilowania

Szkolenie dotyczące profilowania dla funkcjonariuszy policji (Włochy)

Od 2014 r. włoskie centrum monitorowania na rzecz ochrony przed aktami dyskryminacji (*Osservatorio per la sicurezza contro gli atti discriminatori*) wdraża moduł szkolenia dotyczący profilowania etnicznego, skierowany do funkcjonariuszy i kadetów policji. Koncentruje się ono głównie na rzekomych uprzedzeniach, które mogą mieć wpływ na profilowanie, na konsekwencjach w zakresie skuteczności działań policji i negatywnym wpływie na stosunki ze społecznościami. Jak dotychczas w przedmiotowym module szkoleniowym wzięło udział 5 000 osób. Od 2017 r. dostępny jest również moduł szkolenia internetowego w ramach podnoszenia kwalifikacji policji.

Aby uzyskać więcej informacji, zob. strona internetowa włoskiej policji państwowej.

Narzędzie dotyczące praw podstawowych w szkoleniu straży granicznej (UE)

We wspólnym podstawowym programie szkoleń (CCC) dla europejskiej straży granicznej określono minimalne normy dotyczące wiedzy i umiejętności, jakie musi posiadać każdy europejski funkcjonariusz straży granicznej. Zawiera on rozdziały dotyczące socjologii i praw podstawowych. Są w nim również specjalne sekcje dotyczące niedyskryminacji (1.5.4) i profilowania etnicznego (1.7.10), z których mogą skorzystać osoby prowadzące szkolenie. W CCC podkreślono mogące występować podczas profilowania ryzyko związane z uprzedzeniami, rasizmem, dyskryminacją rasową, ksenofobią, islamofobią, homofobią i innymi powiązanymi rodzajami nietolerancji. Aktualizacja CCC z 2017 r. zawiera sekcje dotyczące nowych kompetencji, szczególnie w dziedzinie praw podstawowych.

Ponadto Frontex w konsultacji z uczelniami wyższymi i organizacjami międzynarodowymi opracował podręcznik dla osób prowadzących szkolenia (zob. Frontex, 2013). Jest on dla osób prowadzących szkolenia źródłem metodyki służącej podnoszeniu wiedzy i umiejętności straży granicznej w zakresie praw podstawowych i ochrony międzynarodowej. W podręczniku wyraźnie wskazano profilowanie i określono podstawowe zasady unikania dyskryminacji. Szkolenia odbywają się regularnie. Nie funkcjonuje jednak żaden stały mechanizm pozwalający na ocenę realizacji celów szkolenia.

Aby uzyskać więcej informacji, zob. Frontex (2012).

Dni nauki o profilowaniu dla starszych funkcjonariuszy (Belgia)

W 2015 r. centrum działań policji i bezpieczeństwa (*Centre for Policing and Security*, CPS) z siedzibą w Gandawie (Belgia) zorganizowało wraz z belgijskim organem ds. równości (Unia) dzień nauki o profilowaniu etnicznym (*Profilage ethnique: l'égalité sous pression?*). W programie ujęto różne aspekty związane z tą kwestią, w tym: czy i w jaki sposób funkcjonariusze policji pochodzący ze środowisk migranckich mogą przyczynić się do poprawy stosunków ze społecznościami mniejszości etnicznych; jak często funkcjonariusze policji stosują profilowanie etniczne i w jaki sposób dokonano oceny.

W 2016 r. belgijska Unia zorganizowała dwa dni nauki dla starszych funkcjonariuszy z północnej części Brukseli w celu zwiększenia świadomości na temat profilowania etnicznego i zachęcenia do zastanowienia się nad określeniem praktyk profilowania stosowanych przez funkcjonariuszy pierwszej linii. Funkcjonariusze policji z Hiszpanii i Zjednoczonego Królestwa przedstawili słuchaczom, wśród których znaleźli się funkcjonariusze organów ścigania, badacze i NGO, przykłady dobrych praktyk. Pokazali oni w szczególności, że dzięki ograniczeniu profilowania na podstawie pochodzenia etnicznego wzrosła liczba skutecznych aresztowań osób, którymi były zainteresowane organy ścigania. Wskazali oni, że było to możliwe dzięki prowadzeniu poprawnych rejestrów każdego zatrzymania, a także dzięki zapewnieniu przejrzystości w kwestii motywów zatrzymań. Szkolenie miało na celu osiągnięcie wspólnego zrozumienia praktyk profilowania etnicznego, aby wspierać w przyszłości rozwój badań nad praktykami, które policja obecnie realizuje w tym zakresie.

Aby uzyskać więcej informacji, zob. Belgia (2015 i 2017).

Szkolenie powinno obejmować kwestię uprzedzeń i stereotypów, które mogą być zakorzenione w samych instytucjach organów ścigania i instytucjach zarządzania granicami. Przed przeprowadzeniem szkolenia na temat zapobiegania niezgodnemu z prawem profilowaniu należy zbadać szerszy kontekst instytucjonalny i obowiązującą politykę wewnętrzną, np. obowiązujące mechanizmy składania skarg, obecność „zmowy milczenia" między współpracownikami itp. W programach szkoleń należy omówić kwestię uprzedzeń i stereotypów wpisanych w działania policji, takie jak zatrzymanie i rewizja, aresztowania, zatrzymanie (w celu wydalenia) i użycie siły.

Funkcjonariusze wysokiego lub średniego szczebla mają do odegrania kluczową rolę, aby szkolenie było skuteczne, zarówno dla nich jako uczestników, jak i z punktu widzenia znaczenia, jakie przykładają oni do szkolenia[31]. Jako uczestnicy starsi funkcjonariusze mogą nauczyć się nowych praktyk i nabyć nowe umiejętności, które mogą następnie przekazać funkcjonariuszom pierwszej linii. Kultura organizacyjna, którą w znacznym stopniu ustala starsza kadra kierownicza, ma istotny wpływ na codzienne zachowanie funkcjonariuszy policji i straży granicznej, w tym na sposób, w jaki wchodzą oni w interakcje ze społeczeństwem.

Starsi funkcjonariusze mogą również zapewnić pozytywne postrzeganie szkolenia. Na poziom zainteresowania szkoleniem i zaangażowania w nie może mieć wpływ zachowanie kadry kierowniczej, np. sposób zakomunikowania funkcjonariuszom celu szkolenia lub fakt, czy funkcjonariusze myślą, że są wybierani przypadkowo, czy z racji tego, że sprawiają problemy. Zachęcanie funkcjonariuszy do aktywnego uczestnictwa w programach szkoleniowych i do bycia otwartymi na zmiany zachowania w celu poprawy ich codziennej pracy może zwiększyć skuteczność szkolenia[32].

Po zakończeniu szkolenia należy dokonać jego przeglądu i oceny, aby móc ocenić wpływ, jaki miało ono na podnoszenie świadomości i zmiany w zachowaniu.

31 Zob. Komisja Europejska (2017b).

32 Miller, J. i Alexandrou, B. (2016).

Koncentracja na zasadach przewodnich szkoleń

Specjalistyczne szkolenie jest kluczowe dla zapewnienia stosowania profilowania zgodnie z prawem. Komisja Europejska opracowała zbiór kluczowych zasad przewodnich dotyczących sposobu zapewniania skutecznych szkoleń dobrej jakości dotyczących przestępstw z nienawiści. Te same zasady stosuje się w przypadku szkoleń dotyczących zgodnego z prawem profilowania.

Szkolenie dotyczące przestępstw z nienawiści dla organów ścigania i organów wymiaru sprawiedliwości w sprawach karnych: 10 kluczowych zasad przewodnich

Zapewnienie wpływu i zrównoważonego charakteru:

- ☑ Szkolenie powinno być częścią szerszego podejścia do zwalczania dyskryminacji.
- ☑ Należy opracować metodykę odpowiadającą na potrzeby szkolenia.

Określenie celów i budowanie synergii:

- ☑ Należy dostosować programy do potrzeb swoich pracowników.
- ☑ Należy w zorganizowany sposób współpracować ze społeczeństwem obywatelskim.

Wybór odpowiedniej metodyki:

- ☑ Należy łączyć ze sobą różne metodyki.
- ☑ Należy szkolić osoby prowadzące takie szkolenia.

Przekazywanie treści wysokiej jakości:

- ☑ Należy opracować program szkolenia zawierający treści wysokiej jakości.
- ☑ Należy opracować moduły szkolenia dotyczące problemu dyskryminacji.

Wyniki monitorowania i oceny:

☑ Należy powiązać szkolenie z procesem przeglądu realizacji celów.

☑ Należy zapewnić regularne monitorowanie i ocenę metod szkoleniowych.

Aby uzyskać więcej informacji, zob. Komisja Europejska (2017a).

Samo szkolenie nie będzie jednak skuteczne w zwalczaniu ukrytych uprzedzeń funkcjonariuszy. Konieczna jest zmiana instytucjonalnego myślenia. Organy muszą zatem rozważyć zastosowanie wielowymiarowych interwencji mających na celu zwalczenie osobistych i instytucjonalnych uprzedzeń (zob. analiza przykładów).

Analiza przykładów

Zajęcie się kwestią „rasizmu instytucjonalnego" w policji

W następstwie obaw dotyczących roli rasy w źle poprowadzonym przez policję dochodzeniu dotyczącym morderstwa Stephena Lawrence'a dokonanego na tle rasistowskim w Zjednoczonym Królestwie rząd Zjednoczonego Królestwa przeprowadził szeroko zakrojone badanie, aby określić „wnioski, które należy wyciągnąć na potrzeby dochodzenia i postępowania w przypadku przestępstw na tle rasowym".

W sprawozdaniu z badania, które opublikowano w 1999 r., podkreślono kwestię „rasizmu instytucjonalnego" w londyńskiej policji, w tym rozbieżności w danych liczbowych dotyczących zatrzymania i rewizji, jako sprawy o dużym znaczeniu dla społeczności, których ten problem dotyczy. Zaleceniom sformułowanym na podstawie badania, obejmującym kwestie od szkoleń podnoszących świadomość na temat rasizmu po zgłaszanie i rejestrowanie zdarzeń, towarzyszyło ogólne wezwanie do zwiększenia otwartości, odpowiedzialności i odbudowania zaufania do służb policyjnych.

W przeglądach opublikowanych w 2009 r., dziesięć lat po przeprowadzeniu badania podkreślono poprawę w sposobie interakcji policji ze społecznościami mniejszości etnicznych i w prowadzeniu dochodzeń w sprawie przestępstw na tle

rasowym. Odnotowano jednak, że wciąż istnieje większe prawdopodobieństwo zatrzymania osoby czarnoskórej i przeprowadzenia rewizji takiej osoby, niż ma to miejsce w przypadku osób o białym kolorze skóry.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, Home Office (1999), Zjednoczone Królestwo, Equality and Human Rights Commission (2009) i Zjednoczone Królestwo, House of Commons Home Affairs Committee (2009).

2.2.4. Rozsądne podstawy do podejrzeń: wykorzystywanie danych wywiadowczych i uzyskanych informacji

Gdy funkcjonariusze policji i funkcjonariusze zarządzania granicami wyróżniają osobę, zazwyczaj opierają swoją decyzję na kombinacji różnych elementów. Mogą one obejmować „obiektywne" informacje, takie jak szczegółowe dane wywiadowcze, zachowanie, ubiór czy przedmioty, które osoba ma przy sobie, jak również „subiektywną" wiedzę opartą na doświadczeniach.

Wszystkie te elementy mogą stanowić „sygnał" niezgodnego z prawem działania. Informacje należy jednak łączyć i wykorzystywać z ostrożnością. Dowody wskazują na to, że funkcjonariusze mogą mieć w praktyce trudności w rozróżnieniu między obiektywnymi a subiektywnymi elementami, tak jak w przykładzie przedstawionym w ramce.

Przykład

„To bardzo subiektywna kwestia. Są to twoje odczucia wobec osoby i sprawy, ale też kwestie dowodowe dotyczące rozbieżności między tym, co mówią osoby, brak spójności między tym, co mówią osoby, a tym, co mówią członkowie rodziny rozdzielonej, brak spójności między tym, co mówią, a ich dokumentami, między tym, co mówią, a wszystkimi rzeczami, jakie mogą mieć w swoich torbach. Są więc dowody, ale [same te rzeczy

nie mogłyby] całkiem świadczyć przeciwko komuś. Funkcjonariusz musi zbudować całościowy obraz danej osoby". (Urzędnik imigracyjny w dużym porcie lotniczym w Zjednoczonym Królestwie)

Aby uzyskać więcej informacji, zob. FRA (2014a), s. 46.

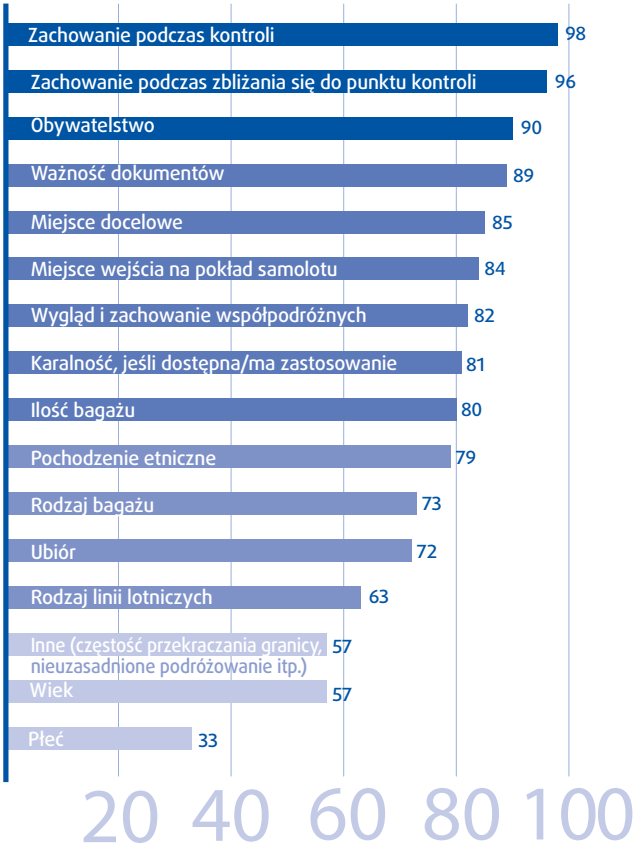
Koncentracja na identyfikacji osób starających się nielegalnie przekroczyć granicę państwa

Badanie FRA przeprowadzone w 2012 r. w głównych portach lotniczych ujawnia, że straż graniczna, podejmując decyzję, czy osoba stara się nielegalnie przekroczyć granicę państwa, bierze pod uwagę szereg czynników. Obejmują one często połączone „obiektywne" kryteria – takie jak zachowanie osoby, gdy zbliża się ona do punktu kontroli i podczas kontroli, rodzaj i ilość bagażu oraz ważność dokumentów podróży – z osobistymi doświadczeniami wcześniejszych kontroli na granicy, jak wskazano na wykresie 7.

Funkcjonariusze straży granicznej określili zachowanie podczas kontroli lub podczas zbliżania się do punktu kontroli jako najbardziej pomocne czynniki w rozpoznawaniu osób starających się nielegalnie przekroczyć granicę państwa. Takie czynniki, jak narodowość i pochodzenie etniczne, które mogłyby wskazywać na dyskryminacyjne profilowanie, również jednak postrzegali jako znaczące.

Ubiór, który także uznali za przydatny wskaźnik, stanowi przykład tego, w jaki sposób pozornie „obiektywna" informacja może być w praktyce wykorzystana w stronniczy sposób. Niektóre rodzaje ubioru mogą być powiązane z konkretnymi profilami ryzyka. Na przykład ofiary handlu ludźmi niektórych narodowości mogą zazwyczaj ubierać się w konkretny sposób. Ubiór może jednak również wskazywać przynależność do konkretnej grupy etnicznej lub religijnej. Nawet jeżeli istnieją wystarczające inne powody uzasadniające skierowanie do kontroli drugiej linii, osoby, które silnie identyfikują się ze swoim pochodzeniem etnicznym lub ze swoją religią, mają negatywne doświadczenia z przeszłości lub nie otrzymały od funkcjonariusza odpowiedniego wyjaśnienia, mogą postrzegać takie traktowanie jako dyskryminacyjne.

Wykres 7: Wskaźniki uznane za pomocne lub bardzo pomocne w skutecznym rozpoznawaniu osób starających się nielegalnie przekroczyć granicę państwa przed przeprowadzeniem rozmowy z funkcjonariuszem (%)



Uwaga: *Ważne odpowiedzi mieszczą się w zakresie od 206 do 216 z 223. Respondenci, którzy nie udzielili odpowiedzi w danej kwestii, zostali wykluczeni podczas podliczania wyników. Przypadki braku odpowiedzi rozciągają się od siedmiu do 17 osób w zależności od kwestii.*

Źródło: *FRA, Badanie dotyczące straży granicznej z 2012 r. (pytanie 17).*

Aby uzyskać więcej informacji, zob. FRA (2014a). W odniesieniu do profili ofiar handlu ludźmi, zob. Frontex (2017).

Dobre dane wywiadowcze dotyczące schematów zachowań lub wydarzeń mogą przyczynić się do większego obiektywizmu profilowania. Mogą się one wiązać z działalnością przestępczą lub, w przypadku zarządzania granicami, nielegalną migracją lub przestępstwami transgranicznymi. Gdy działania z zakresu ścigania przestępstw i zarządzania granicami opierają się na szczegółowych i aktualnych danych wywiadowczych, takich jak informacje o konkretnej osobie i konkretnym kontekście, mają większe szanse być obiektywne i nie opierać się na stereotypach.

Oprócz danych wywiadowczych i obiektywnych elementów, w niektórych okolicznościach można zgodnie z prawem wykorzystać informacje na temat cech chronionych, takich jak rzeczywista lub postrzegana rasa, pochodzenie etniczne, narodowość, płeć lub religia, jako dodatkowy element oceny profilowania. Aby wykorzystanie takich informacji było zgodne z prawem, musi być ono regulowane przepisami, szanować istotę praw i wolności, których dotyczy, być proporcjonalne (tj. zgodne z równowagą interesów) i konieczne (tj. nie mogą być dostępne żadne mniej restrykcyjne środki). Aby funkcjonariusz mógł potraktować osobę w inny sposób niż resztę członków społeczeństwa, musi istnieć uzasadniona przyczyna inna niż cechy chronione. Przyczyna ta musi również odnosić się konkretnie do tej osoby, jak w przykładzie przedstawionym w poniższej ramce.

Przykład

Świadkowie zeznają, że podejrzany w sprawie o rabunek miał na sobie czerwone buty do biegania i czarną czapkę bejsbolówkę, ma 160–170 cm wzrostu i wydawał się być chińskiego pochodzenia. W tych okolicznościach organy ścigania uznają pochodzenie etniczne za istotne dla ustalenia, czy dana osoba jest potencjalnym podejrzanym, gdyż informacji tej używają w połączeniu ze szczegółowymi danymi wywiadowczymi.

Koncentracja na szczegółowych opisach podejrzanego

Dobre opisy podejrzanego mogą ograniczyć ryzyko niezgodnego z prawem profilowania. Opis podejrzanego składa się ze szczegółowych informacji na temat osoby, takich jak kolor skóry, włosów i oczu, wzrost i waga oraz ubiór. Szczegółów tych dostarcza ofiara przestępstwa lub świadkowie, lub gromadzi się je na podstawie innych szczegółowych danych wywiadowczych. Funkcjonariusze mogą wykorzystać dobry opis podejrzanego jako podstawę

do działań zatrzymania i rewizji mających na celu zatrzymanie podejrzanych, lub do skierowania osób do kontroli drugiej linii na granicy.

Gdy funkcjonariusze organów ścigania otrzymają jednak zbyt ogólny opis podejrzanego obejmujący rasę, pochodzenie etniczne lub podobne cechy, nie powinni oni wykorzystywać go jako podstawy prowadzenia swoich operacji. W takich przypadkach prowadzone przez nich operacje mogą skutkować zatrzymaniem wielu niewinnych osób, które charakteryzują się akurat tą samą cechą. Powinni oni raczej szukać dokładniejszych danych wywiadowczych, które posłużą im w prowadzeniu śledztwa.

Aby uzyskać więcej informacji, zob. Komisja Europejska (2017b).

Informacje, które wydają się obiektywne, mogą w rzeczywistości zawierać uprzedzenia. Pozornie obiektywne czynniki, takie jak czas, dzień, miejsce itp., mogą zostać użyte jako zamiennik zakazanych podstaw dyskryminacji, takich jak rzeczywista lub postrzegana rasa, narodowość, płeć, orientacja seksualna lub religia, jak przedstawiono w poniższym przykładzie.

Przykład

Operacja zatrzymania i rewizji odbywa się w piątek koło południa na obszarze X. Czas ten jest jednak najważniejszym momentem modlitwy dla muzułmanów. Ponieważ obszar X znajduje się blisko meczetu, rzekomo obiektywne czynniki czasu, daty i miejsca mogą w rzeczywistości funkcjonować jako zamienniki w odniesieniu do operacji zatrzymania i rewizji opartej na zakazanej dyskryminacyjnej podstawie religii.

Podobnie szukanie konkretnego podejrzanego zachowania może wyglądać jak obiektywna metoda identyfikacji możliwych nadużyć. Funkcjonariusze mogą jednak interpretować zachowanie osoby na różne sposoby w zależności od innych cech osoby, której to dotyczy. Dowody wskazują na to, że wiedza praktyczna i rozumienie danych wywiadowczych może znacznie różnić się między funkcjonariuszami i często nie odpowiada rzeczywistym wzorcom przestępstw[33].

33 Zjednoczone Królestwo, National Policing Improvement Agency (NPIA) (2012).

Dostarczenie funkcjonariuszom aktualnych i szczegółowych danych wywiadowczych, np. na odprawach przed każdą zmianą, powinno ograniczyć działanie według własnego uznania i zapewnić funkcjonariuszom wytyczne co do tego, w jaki sposób powinni ukierunkować swoje uprawnienia na konkretne bieżące wzorce przestępstw i określone kwestie bezpieczeństwa. Postępowanie prowadzi do ograniczenia roli uprzedzeń. Poprawa jakości i wykorzystania danych wywiadowczych w celu skoncentrowania się na czynnikach związanych z zachowaniem lub konkretnych informacjach jest najskuteczniejsza wtedy, gdy połączy się ją ze wzmożonym nadzorem i monitorowaniem sposobu, w jaki funkcjonariusze wykonują swoje uprawnienia.

Analiza przykładów

Zapewnienie obiektywizmu w profilowaniu

Odprawy przed zmianą (UE)

W katalogu schengeńskim zaleca się, aby przed każdą zmianą funkcjonariusz pełniący służbę przedstawiał informacje dotyczące wszelkich wskaźników ryzyka i profili ryzyka. Zapewniając, aby poszczególne zmiany nachodziły na siebie, można zapewnić wystarczającą ilość czasu na wymianę informacji między funkcjonariuszami zmiany przychodzącej i wychodzącej oraz na odpowiednią odprawę.

Aby uzyskać więcej informacji, zob. Rada Unii Europejskiej (2009).

Program szkoleniowy SDR (Niderlandy)

Program szkoleniowy Szukaj, wykrywaj i reaguj (ang. *Search, Detect and React*, SDR) ma na celu zapobieganie przestępstwom i aktom terroryzmu dzięki poprawie zdolności personelu odpowiedzialnego za bezpieczeństwo w odniesieniu do profilowania zachowań. Oznacza to, że przy dokonywaniu wyborów dotyczących działań policji należy oderwać uwagę od niezmiennych cech, takich jak kolor skóry, i skupić się zamiast tego na zachowaniu osoby. Ponieważ wskaźniki podejrzanego zachowania są szczególne dla każdego kontekstu, szczegóły szkolenia są dostosowywane do środowiska. W szkoleniu odrzucono pogląd, że istnieje jedno uniwersalne rozwiązanie pasujące do każdej sytuacji. Po wykryciu istotnych wzorców postępowania

funkcjonariusze są zobowiązani do postępowania z zachowaniem pewnego stopnia „wrażliwości". W większości przypadków przeprowadzą oni z podejrzanym nieformalną rozmowę zamiast korzystać z jakichkolwiek formalnych uprawnień policyjnych. Oprócz szkolenia zorientowanego na praktykę i zdobywanie kwalifikacji w trakcie pracy program obejmuje również kształcenie teoretyczne.

Aby uzyskać więcej informacji, zob. strona internetowa SDR Academy.

Narzędzie dozwolonej praktyki zawodowej (ang. *Authorised Professional Practice*, APP) w zakresie zatrzymania i rewizji (Zjednoczone Królestwo)

Instytucja wspierająca policję w Zjednoczonym Królestwie, College of Policing, opracowała wytyczne dotyczące dozwolonej praktyki zawodowej (APP) obejmujące różne aspekty pracy policji. W APP na temat zatrzymania i rewizji wyjaśniono, czym jest zatrzymanie i rewizja, dlaczego właściwe wykonywanie uprawnień jest ważne oraz jakie są cechy zgodnego z prawem zatrzymania i rewizji. Wyjaśniono, że wsparcie legalności i skuteczności kontaktów obejmujących zatrzymanie i rewizję będą zapewnione dzięki:

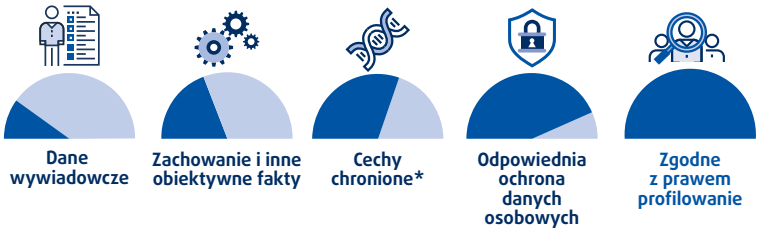
- **sprawiedliwości**: decyzja funkcjonariusza dotycząca zatrzymania i rewizji musi opierać się wyłącznie na odpowiednich, obiektywnych czynnikach. Nie można nigdy zatrzymać osoby wyłącznie lub głównie na podstawie cech chronionych lub takich czynników, jak wcześniejsze wyroki skazujące;
- **zgodności z prawem**: zatrzymanie i rewizja muszą mieć podstawy prawne, które stosuje się zgodnie z prawem;
- **profesjonalnemu podejściu**: podczas spotkań obejmujących zatrzymanie lub rewizję funkcjonariusze muszą zachować zgodność z normami postępowania zawodowego, szczególnie z kodeksem etyki zawodowej, stosować skuteczną komunikację z ludźmi traktować ich z godnością i szacunkiem;
- **przejrzystości**: poszczególne spotkania należy dokładnie rejestrować. Należy zapewnić skuteczny nadzór i skuteczne monitorowanie zatrzymań i rewizji, a także kontrolę publiczną.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, College of Policing (2016).

Na wykresie 8 przedstawiono różne elementy, które można zastosować podczas zgodnego z prawem profilowania; sposób ich łączenia będzie zależał od charakteru danej sprawy.

Na wykresie 9 wskazano, w jaki sposób można łączyć te elementy w celu zapewnienia, aby profilowanie nie było dyskryminacyjne.

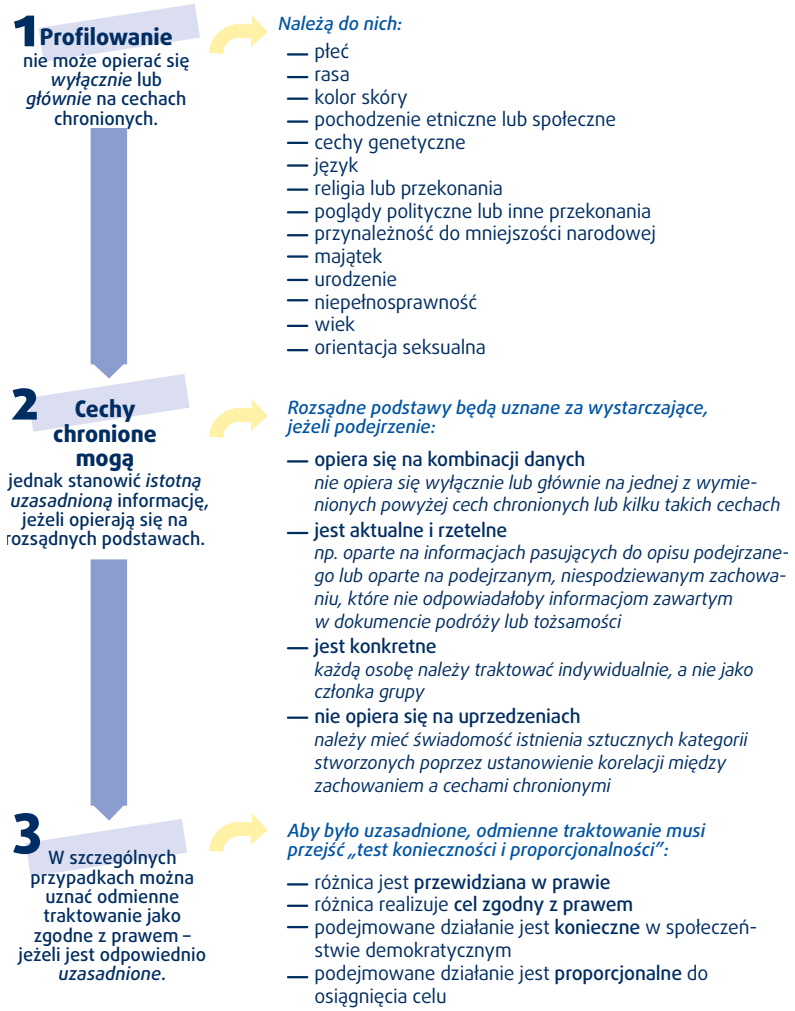
Wykres 8: Łączenie elementów



* *Zob. wykres 9, aby uzyskać wykaz cech chronionych na podstawie prawa Unii. Profilowanie nigdy nie powinno opierać się wyłącznie lub głównie na cechach chronionych.*

Źródło: FRA, 2018.

Wykres 9: Elementy niedyskryminacyjnego profilowania



Uwagi: *Wykaz cech chronionych różni się w zależności od państwa członkowskiego. Aby uzyskać przegląd podstaw dyskryminacji, które występują w kodeksach karnych każdego z państw członkowskich, zob. FRA (2018d). Zob. również strona internetowa Equinet, europejskiej sieci organów ds. równości, na której znajduje się wykaz podstaw dyskryminacji, którymi zajmują się krajowe organy ds. równości.*

Źródło: *FRA, 2018.*

2.2.5. Formularze zatrzymania i rewizji w odniesieniu do profilowania przez organy ścigania

Formularze zatrzymania i rewizji mogą pomóc funkcjonariuszom zastanowić się, czy prowadzone przez nich zatrzymania mają rozsądne podstawy, i umożliwiają starszym funkcjonariuszom monitorowanie potencjalnych praktyk dyskryminacyjnych podczas stosowania zatrzymania i rewizji przez poszczególnych funkcjonariuszy. Chociaż czasami uznaje się je za uciążliwe, dzięki nim powstaje również rejestr zatrzymań, który po zestawieniu dostarcza danych wskazujących na to, czy zatrzymania przeprowadzono w sposób zgodny z prawem[34]. Może to pomóc w promowaniu otwartości i odpowiedzialności. Poza wypełnianiem papierowych formularzy do rejestrowania takich informacji można wykorzystywać również nowe technologie, takie jak aplikacje mobilne.

W ramce poniżej przedstawiono niektóre ważne informacje, które należy uwzględnić przy opracowywaniu formularzy zatrzymania i rewizji.

Koncentracja na informacjach składających się na dobre formularze zatrzymania i rewizji

Aby formularze zatrzymania i rewizji były przydatne, muszą być odpowiednio opracowane. Po pierwsze, wypełnianie formularzy dodatkowo obciąża pracą funkcjonariuszy. Jeżeli nie są one opracowane w jasny sposób i nie są rozsądnej długości, istnieje ryzyko, że funkcjonariusze mogą nie wypełniać formularza w całości lub że będą go wypełniać w pobieżny sposób. Po drugie, dobre formularze umożliwiają łatwe wyodrębnienie i zestawienie danych mające na celu wspieranie monitorowania i oceny działań zatrzymania i rewizji.

W miarę możliwości formularze zatrzymania i rewizji powinny:

- zawierać pola wielokrotnego wyboru, które wypełnia się szybciej i które są prostsze do statystycznego przetworzenia;
- określać wyczerpującą listę wariantów w odniesieniu do każdej pozycji;
- unikać niejednoznacznych pozycji;

34 Zjednoczone Królestwo, Stop Watch (2011).

- być łatwe do zrozumienia, zarówno dla funkcjonariusza, jak i dla zatrzymanej osoby;
- zawierać:
  - podstawę prawną rewizji; preferowane jest raczej proste wyjaśnienie niż wykaz przepisów;
  - dzień, godzinę i miejsce, w którym dokonano rewizji osoby lub pojazdu;
  - obiekt rewizji, tj. przedmiot lub przedmioty poszukiwane przez funkcjonariuszy;
  - wynik zatrzymania;
  - nazwisko funkcjonariusza lub funkcjonariuszy prowadzących rewizję i ich komisariat policji;
  - dane osobowe osoby lub osób, które podlegają rewizji, takie jak imię i nazwisko, adres i narodowość, mogą być rejestrowane. Osoba może jednak odmówić podania tych informacji.

Aby formularze były skuteczne, należy je wypełniać w momencie przeprowadzania zatrzymania.

Osoba zatrzymana lub osoba odpowiedzialna za przeszukiwany pojazd powinna otrzymać kopię formularza. W Zjednoczonym Królestwie zatrzymane osoby mają prawo do zażądania kopii rejestru w ciągu trzech miesięcy od momentu zatrzymania. W ten sposób formularz stanowi nie tylko dowód zatrzymania dla policji, lecz również dla zatrzymanych osób.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, West Midlands Police (2012), s. 7 i Zjednoczone Królestwo, Home Office (2014a).

Analiza przykładów

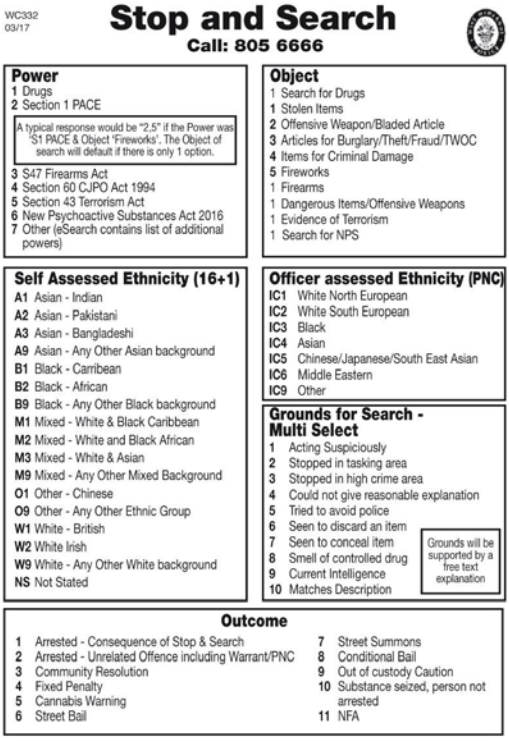
Formularz zatrzymania i rewizji (Zjednoczone Królestwo)

Poniżej powielono formularz zatrzymania i rewizji stosowany przez West Midlands Police w Zjednoczonym Królestwie.

Widać na nim, że zatrzymana osoba jest proszona o określenie, do której kategorii etnicznej należy, przy czym dostępne warianty obejmują „inna" lub

„nie określono". Funkcjonariusz prowadzący zatrzymanie może dodać swoje postrzeganie pochodzenia etnicznego, jeżeli nie zgadza się z wariantem określonym przez zatrzymaną osobę.

W kodeksie dobrych praktyk dotyczących uprawnień w zakresie zatrzymania i rewizji w Zjednoczonym Królestwie określono, że funkcjonariusze powinni wyjaśnić zatrzymanym osobom, że informacje dotyczące pochodzenia etnicznego „są potrzebne, aby uzyskać prawdziwy obraz działań zatrzymania i rewizji oraz aby pomóc w usprawnieniu monitorowania mniejszości etnicznych, zwalczać praktyki dyskryminacyjne i promować skuteczne wykonywanie uprawnień".



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

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, West Midlands Police (2017a) i Zjednoczone Królestwo, Home Office (2014a), s. 19.

Wiele sił odchodzi aktualnie od gromadzenia danych dotyczących zatrzymania i rewizji na formularzach i stosuje zamiast tego takie technologie, jak aplikacje na telefony komórkowe, systemy łączności radiowej, mobilne terminale danych lub laptopy. Technologie te mogą przyspieszyć proces rejestracji i ograniczyć biurokrację, mogą jednak również stworzyć nowe zagrożenia, szczególnie w związku z wykorzystaniem algorytmu przy przetwarzaniu danych osobowych (zob. rozdział 3).

Analiza przykładów

Rejestrowanie na żywo działań zatrzymania i rewizji

„eSearch" (West Midlands Police, Zjednoczone Królestwo)

Przyjęty w kwietniu 2014 r. system opiera się na połączeniu między funkcjonariuszem w terenie i członkiem personelu z punktem kontaktowym (punktem dyspozytorskim). Szczegółowe dane na temat zatrzymania i rewizji są natychmiast rejestrowane w punkcie kontaktowym i włączane do bazy danych. Następnie można uzyskać dostęp do tych informacji i wykorzystać je do analizy skuteczności działań zatrzymania i rewizji, zarówno do celów wewnętrznych, jak i zewnętrznych. System eSearch zmienił rejestrowanie działań zatrzymania i rewizji. Można o wiele szybciej zobaczyć treści rejestrów w policyjnych systemach, co jest korzystne w kontekście wywiadu i integracji tych danych na potrzeby działań operacyjnych policji.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, West Midlands Police (2014) i Zjednoczone Królestwo, West Midlands Police (2016).

Aplikacja mobilna dla funkcjonariuszy pierwszej linii kontroli (West Midlands Police, Zjednoczone Królestwo)

W październiku 2017 r. uruchomiono nową aplikację mobilną, która ma na celu przyspieszenie i podniesienie skuteczności zatrzymania i rewizji. Aplikacja eSearch umożliwia funkcjonariuszom rejestrowanie szczegółowych informacji na temat ulicznych kontaktów bezpośrednio w aplikacji za pośrednictwem smartfonów bez konieczności dzwonienia do personelu punktu kontaktowego. Każde zatrzymanie otrzymuje niepowtarzalny numer referencyjny, a GPS automatycznie rejestruje lokalizację zatrzymania.

Oczekuje się, że dzięki aplikacji liczba połączeń z punktem kontaktowym zmaleje o niemal 1 000 połączeń miesięcznie.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, West Midlands Police (2017b).

Starsi funkcjonariusze odgrywają ważną rolę w zapewnianiu, aby operacje zatrzymania i rewizji odbywały się zgodnie z prawem. Poniższy przykład przedstawia sposób, w jaki starsi funkcjonariusze mogą sprawować nadzór. Powinni oni również zapewnić, aby działania zatrzymania i rewizji nie były wykorzystywane jako narzędzie pomiaru efektywności w oparciu o liczbę przeprowadzonych zatrzymań.

Analiza przykładów

Podpisywanie rejestrów zatrzymania i rewizji (Zjednoczone Królestwo)

Od sierpnia 2014 r. każdy rejestr zatrzymania i rewizji w Zjednoczonym Królestwie musi zostać podpisany przez przełożonego funkcjonariusza, który prowadził tę rewizję. Zatwierdza on rejestr jako spełniający odpowiednie normy lub nie. W tym drugim przypadku funkcjonariusz zgłaszający musi w rejestrze zatrzymania i rewizji podać przyczynę takiej niezgodności.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, Home Office (2014a).

2.3. Odpowiedzialność

Najważniejsze kwestie

- Organy ścigania i funkcjonariusze zajmujący się zarządzaniem granicami są **odpowiedzialni** za to, aby profilowanie odbywało się zgodnie z prawem.
- **Gromadzenie rzetelnych, dokładnych i aktualnych danych** dotyczących działań profilowania jest kluczowe dla zapewnienia takiej odpowiedzialności.
- **Skuteczne mechanizmy wnoszenia skarg** mogą zarówno zwalczać nadużycia, jak i zabezpieczać oraz odbudowywać zaufanie względem operacji prowadzonych przez policję i organy zarządzania granicami.

- **Spotkania z członkami społeczeństwa mające na celu uzyskanie informacji zwrotnych** – słuchanie ich opinii, omawianie kwestii profilowania i gromadzenie informacji zwrotnych na temat operacji daje sposobność wyciągnięcia istotnych wniosków i poprawy działań związanych z profilowaniem.

Odpowiedzialność jest kluczową zasadą demokratycznych rządów. W bardzo ogólnym ujęciu obejmuje ona udzielanie odpowiedzi osobom, które są uprawnione do żądania takiej odpowiedzi[35]. Odpowiedzialność skupia się nie tylko na podejmowaniu decyzji przez poszczególne osoby, lecz także przez instytucje (tzw. „odpowiedzialność instytucjonalna"). Jako funkcjonariusze publiczni i podmioty publiczne, funkcjonariusze organów ścigania i zarządzający granicami, a także ich organizacje, odpowiadają przed społeczeństwem za podejmowane decyzje i prowadzone działania. Zasada ta obejmuje również odpowiedzialność za zapewnianie, aby profilowanie było zgodne z prawem.

Gromadzenie rzetelnych, dokładnych i aktualnych danych jest kluczowe dla zapewnienia takiej odpowiedzialności. Ponieważ wiele danych zawiera wrażliwe dane osobowe, należy postępować z nimi w sposób zgodny z przepisami i procedurami w zakresie ochrony danych osobowych (zob. rozdział 3).

Lista kontrolna dotycząca odpowiedzialności

Przedstawiona poniżej lista kontrolna zawiera podstawowy przegląd kroków, które mogą podjąć organy ścigania i organy zarządzania granicami, aby zapewnić odpowiedzialność za decyzje i działania dotyczące profilowania. Lista ta może wskazywać funkcjonariuszom, w jaki sposób mogą poprawić swoją odpowiedzialność, nie należy jej jednak traktować jako listy obowiązkowych kroków zarówno dla funkcjonariuszy organów ścigania, jak i dla funkcjonariuszy zarządzania granicami. W zależności od kontekstu niektóre zalecenia mogą nie mieć zastosowania do szczególnego charakteru zarządzania granicami.

1. Rozpoznanie

☑ Rozpoznanie i **uznanie** problemu niezgodnego z prawem profilowania. Uprzedzenia i stereotypy istnieją i mogą stanowić zagrożenie dla zaangażowanych osób, w tym funkcjonariuszy i lokalnych społeczności.

35 Bovens, M., Schillermans, T. i Goodlin, R.E. (2014), s. 1–11.

- ☑ **Gromadzenie i wykorzystanie danych zdezagregowanych**: jest to istotne narzędzie oceny skuteczności i efektywności.
- ☑ Uczestnictwo w zewnętrznych panelach organizowanych przez społeczność lub społeczeństwo obywatelskie w celu uzyskania **informacji zwrotnych** na temat swoich praktyk i w celu podniesienia zaufania do swoich operacji.

2. Gromadzenie informacji

- ☑ Gwarancja odpowiedzialności poprzez **prowadzenie rejestrów** działań profilowania.
- ☑ Pod warunkiem stosowania odpowiednich zabezpieczeń, **monitoring wizyjny** lub **kamery nasobne** mogą zwiększyć odpowiedzialność i dostarczyć dowodów wspierających działania zmierzające do zmiany wzorców stronniczych zachowań.
- ☑ Tworzenie **formularzy zatrzymania i rewizji**, które funkcjonariusze policji mają wypełniać po każdym zatrzymaniu.

3. Działanie i zapobieganie

- ☑ Prowadzenie **oceny** w celu weryfikacji, czy istnieją jakiekolwiek zasady lub praktyki, które bezpośrednio lub pośrednio utrwalają uprzedzenia i negatywne stereotypy.
- ☑ Wprowadzenie specjalnych szkoleń lub **sesji szkoleniowych** koncentrujących się na rozwiązywaniu problemów osobistych i instytucjonalnych uprzedzeń i stereotypów.
- ☑ **Przedstawianie informacji** zatrzymanym osobom, aby zwiększyć postrzeganie sprawiedliwego zatrzymania, i dostarczenie osobom wystarczających informacji, aby mogły zdecydować, czy chcą wnieść skargę. W odniesieniu do skierowania do kontroli drugiej linii na przejściach granicznych informowanie stanowi obowiązek prawny.
- ☑ Okazywanie **zerowej tolerancji** względem zdarzeń opartych na uprzedzeniach w obrębie organizacji.

- ☑ Ustanowienie **wewnętrznych mechanizmów** nadzoru i kontroli, takich jak wewnętrzne panele służące omawianiu, czy zatrzymania odbywają się w oparciu o rozsądne podstawy.
- ☑ Upewnianie się, czy **wskaźniki efektywności** są powiązane z unikaniem uprzedzeń i stereotypów.
- ☑ Ustanowienie **mechanizmów zaskarżania** w celu odstraszenia od nadużyć uprawnień i zapewnienia odpowiedzialności.

Źródło: FRA, 2018.

2.3.1. Monitorowanie wewnętrzne

Przywództwo i kierownictwo policji i organów zarządzania granicami odgrywa znaczącą rolę w budowaniu etosu ochrony praw jednostki i zasady niedyskryminacji, zarówno w obrębie organizacji, jak i w kontaktach ze społeczeństwem. Przyczyniają się one również do tworzenia klimatu odpowiedzialności i przejrzystości. Otwarta komunikacja między personelem (w ujęciu poziomym i pionowym) i ustanawianie jasnych norm zachowania, takich jak zawodowe kodeksy postępowania, to dwa elementy polityki wewnętrznej, które powinny funkcjonować, aby zwiększyć odpowiedzialność. Istotną rolę odgrywają również rekrutacja i szkolenie (zob. sekcja 2.2.3).

Zgodnie z prawem Unii każdy organ lub podmiot publiczny musi wyznaczyć **inspektora ochrony danych**. Inspektor doradza policji i siłom zarządzającym granicami w kwestiach obowiązków ochrony danych, w tym prowadzenia rejestrów czynności przetwarzania lub dokonywania oceny skutków dla ochrony danych. W kontekście profilowania inspektor ochrony danych będzie na przykład doradzał i nadzorował, aby dane osobowe zgromadzone na potrzeby profilowania lub podczas profilowania były przetwarzane i przechowywane w sposób zgodny z prawem.

Koncentracja na roli inspektora ochrony danych

Zgodnie z **dyrektywą dotyczącą policji** od państw członkowskich wymaga się, aby wyznaczyły inspektora ochrony danych, którego zadania obejmują:

- monitorowanie przestrzegania mających zastosowanie przepisów dotyczących ochrony danych osobowych, w tym:
  - przydziału obowiązków;

- działań podnoszących świadomość i szkoleń personelu;
- audytów;

- przedstawianie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
- pełnienie funkcji punktu kontaktowego wobec organu nadzorczego.

Należy w pełni i niezwłoczne włączyć inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych.

Zob. art. 32–34 dyrektywy dotyczącej policji.

Prowadzenie wewnętrznego monitorowania w ramach sił policyjnych może odbywać się jako część szerokiego zakresu innych środków służących prowadzeniu rejestrów kontaktów między organami a ogółem społeczeństwa (zob. wykres 10). Obejmują one wykorzystywanie:

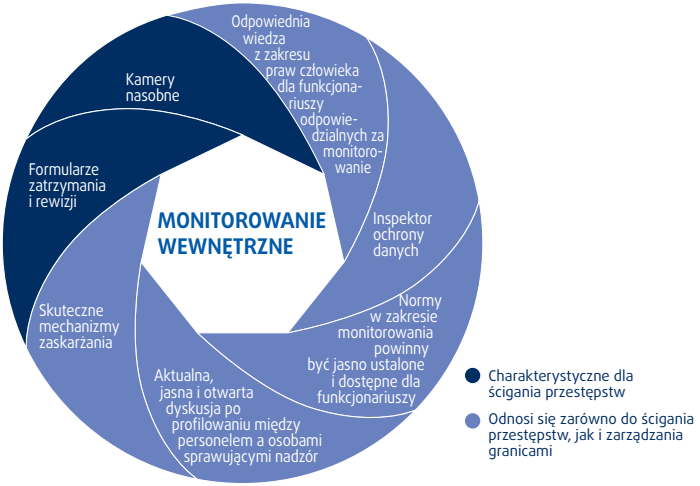
- **formularzy zatrzymania i rewizji**: są one przydatnym praktycznym narzędziem mającym zachęcić funkcjonariuszy do prowadzenia odpowiednio uzasadnionych zatrzymań i promować otwartość i odpowiedzialność względem społeczeństwa (zob. sekcja 2.2.5);

- **kamer nasobnych**: pod warunkiem zastosowania odpowiednich zabezpieczeń mogą one podnieść zaufanie między społecznościami a policją oraz służyć jako środek odstraszający od nadużywania siły i od dyskryminacji (zob. sekcja 2.3.2).

Środki te mogą być również wykorzystywane do działań wewnętrznego monitorowania w organizacjach zarządzania granicami. Na przykład w katalogu schengeńskim zaleca się rejestrowanie liczby przypadków skierowania do kontroli drugiej linii i powody takiego skierowania. Ponadto różne konteksty kontroli na granicy, infrastruktura przejść granicznych i obecność przełożonych na miejscu stwarzają możliwości do prowadzenia wewnętrznego monitorowania. Na przykład może być dostępny dodatkowy sprzęt technologiczny, taki jak monitoring wizyjny.

Przy zastosowaniu odpowiednich zabezpieczeń nagranie wideo może stanowić źródło dowodów do celów oceny sposobu prowadzenia profilowania, a także w przypadku konkretnych skarg. Na przykład mogłoby służyć potwierdzeniu,

Wykres 10: Elementy monitorowania wewnętrznego



Źródło: FRA, 2018.

czy zachowanie osoby podczas oczekiwania na kontrolę pierwszej linii stworzyło wystarczające powody do skierowania tej osoby do kontroli drugiej linii.

W odróżnieniu od działań zatrzymania i rewizji pasażerowie na przejściach granicznych w znacznej mierze spodziewają się obecności monitoringu wizyjnego z uwagi na publiczny charakter tych miejsc i ze względów bezpieczeństwa. Stosowanie takich narzędzi musi być jednak zgodne z prawem do prywatności i z mającymi zastosowanie przepisami w zakresie ochrony danych.

Prowadzenie rejestrów może przynosić zarówno krótkotrwałe, jak i długotrwałe korzyści. Na przykładach formularzy zatrzymania i rewizji pokazano, w jaki sposób:

- W perspektywie **krótkoterminowej** formularze zatrzymania i rewizji mogą zapewnić odpowiedzialność na miejscu. W Zjednoczonym Królestwie każda zatrzymana osoba otrzymuje zapis formularza zatrzymania lub pokwitowanie z informacją, jak może uzyskać dostęp do kopii. Zawiera on szczegółowe informacje na temat powodów zatrzymania, a także informacje na temat miejsca i sposobu składania skarg. Umożliwia to zatrzymanej osobie poznanie powodów zatrzymania i zaskarżenie decyzji, jeżeli uzna ją za niesłuszną.

- W perspektywie **długoterminowej** analiza rejestrów umożliwia siłom policyjnym określenie, czy uprawnienia do zatrzymania i rewizji są w nieproporcjonalny sposób ukierunkowane na członków grup mniejszości, oraz odpowiednie dostosowanie wytycznych dla funkcjonariuszy. Rejestry te można upublicznić w celu zwiększenia przejrzystości i promowania zaufania publicznego w odniesieniu do wykonywania uprawnień zatrzymania i rewizji.

Prowadzenie rejestrów: co mówią przepisy?

Aby zapewnić zgodność z prawem przy przetwarzaniu danych, w dyrektywie dotyczącej policji zawarto wymóg, aby organy ścigania prowadziły wykaz wszystkich kategorii czynności przetwarzania, za które odpowiadają. Ponadto w zautomatyzowanych systemach przetwarzania muszą one prowadzić ewidencje czynności, aby wiedzieć, kto przeglądał lub ujawnił dane osobowe, kiedy miało to miejsce, kto otrzymał te dane, i aby ustalić zasadność przetwarzania danych (zob. sekcja 3.1.3).

Artykuł 24 i 25 dyrektywy dotyczącej policji

Analiza przykładów

Wykorzystywanie rejestrów do wykrywania nieproporcjonalności w działaniach zatrzymania i rewizji (Zjednoczone Królestwo)

W opracowanym w Anglii i Walii (Zjednoczone Królestwo) kodeksie dobrych praktyk ustawy o policji i dowodach w sprawach karnych nałożono na siły policyjne statutowy obowiązek monitorowania wykonywania uprawnień w zakresie zatrzymania i rewizji, aby wykrywać, czy są one „wykonywane na podstawie stereotypowych wizerunków lub niepoprawnych uogólnień". Należy zidentyfikować i zbadać każde pozornie nieproporcjonalne wykorzystanie uprawnień przez poszczególnych funkcjonariuszy lub przez grupy funkcjonariuszy lub w związku z konkretnymi częściami społeczności i podjąć odpowiednie działania zmierzające do zaradzenia tej sytuacji. Ponadto policja musi zorganizować analizę rejestrów przez przedstawicieli społeczności oraz wyjaśnić kwestię wykonywania uprawnień w zakresie zatrzymania i rewizji na szczeblu lokalnym.

Aby uzyskać więcej informacji, zob. Zjednoczone Królestwo, Home Office (2014a).

Policja w Zjednoczonym Królestwie opracowała kilka narzędzi służących zwiększaniu przejrzystości poprzez ułatwienie dostępu do danych na temat zatrzymania i rewizji. Strona internetowa www.police.uk umożliwia użytkownikom wprowadzenie swojego kodu pocztowego w celu uzyskania szczegółowych informacji na temat liczby i charakteru zatrzymań przeprowadzonych w ich okolicy. Publikowane informacje opierają się na wypełnionych formularzach zatrzymania i rewizji. Ponadto na tablicy wskaźników na temat zatrzymania i rewizji służb londyńskiej policji przedstawiono dane dotyczące wszystkich zatrzymań i rewizji w Londynie, w tym odsetek zatrzymanych osób o mniejszościowym pochodzeniu etnicznym w stosunku do ogółu populacji. Użytkownicy mogą uzyskać dostęp do szczegółowych danych online na różne sposoby, obejmujące:

- mapę przedstawiającą dokładne lokalizacje zatrzymań i rewizji przeprowadzonych na konkretnym obszarze w każdym miesiącu. Narzędzie to dostarcza również szczegółowych informacji na temat zatrzymania i rewizji (przedmiot, rodzaj, wynik, czy zatrzymanie i rewizja były częścią operacji policyjnej), osoby (płeć, przedział wiekowy, podane pochodzenie etniczne, pochodzenie etniczne określone przez funkcjonariusza) i przepisów, na podstawie których przeprowadzono zatrzymanie i rewizję (zob. wykres 11); oraz

- przegląd statystyk i wykresów przedstawiających przeprowadzone przez policję działania zatrzymania i rewizji. Umożliwiają one zagregowanie i pobranie informacji.

Chociaż praktyka ta sprzyja przejrzystości i zaufaniu, może mieć wpływ na prawa do prywatności i do ochrony danych osobowych osób, których informacje te dotyczą. Istnieje możliwość wywnioskowania tożsamości osoby z połączenia danych dostępnych za sprawą tego narzędzia lub innych narzędzi online. Należy dokonać oceny takiego zagrożenia i w razie konieczności podjąć środki zaradcze.

2.3.2. Kamery nasobne

Siły policyjne coraz częściej używają kamer nasobnych. Mogą one odgrywać pewną rolę w zapewnianiu odpowiedzialności, poprawie jakości poszczególnych spotkań i zmianie wzorców stronniczych zachowań. Mogą być również pomocne w łagodzeniu niebezpiecznych sytuacji. Oprócz nagrań gromadzonych przez policję coraz częściej członkowie społeczeństwa filmują zatrzymania i inne interakcje z policją. Nagrania takie można również wykorzystać do przeglądu praktyk policji.

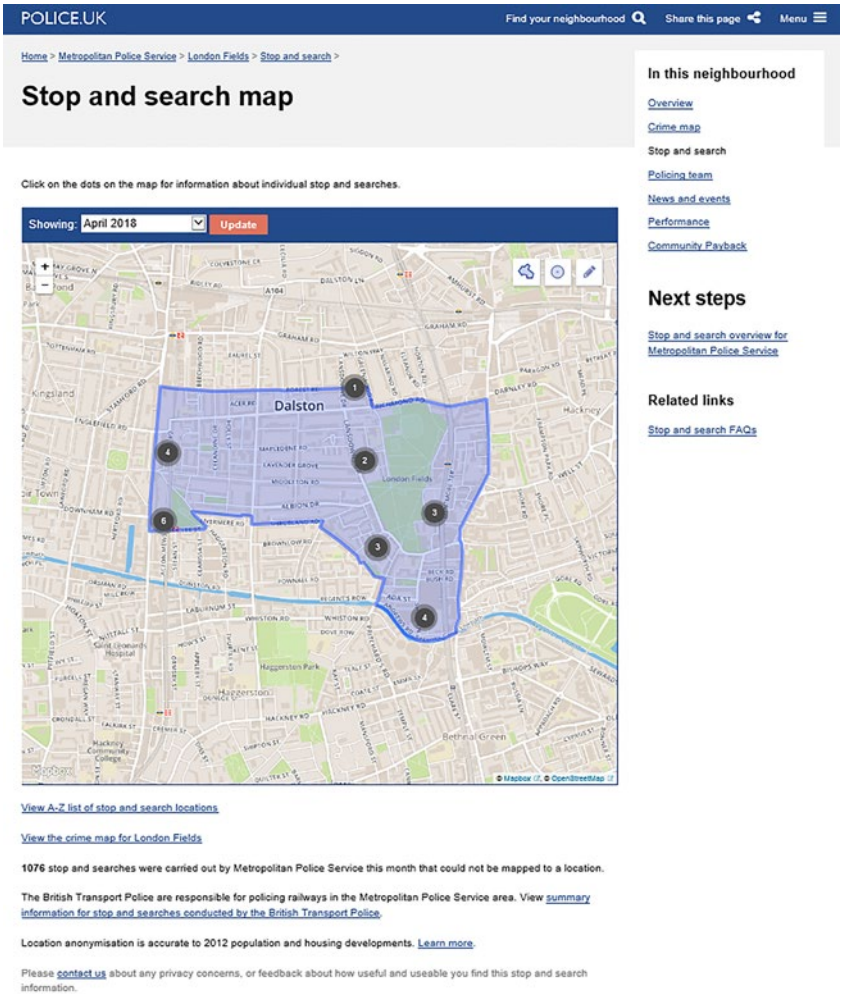
Analiza przykładów

Skuteczność kamer nasobnych

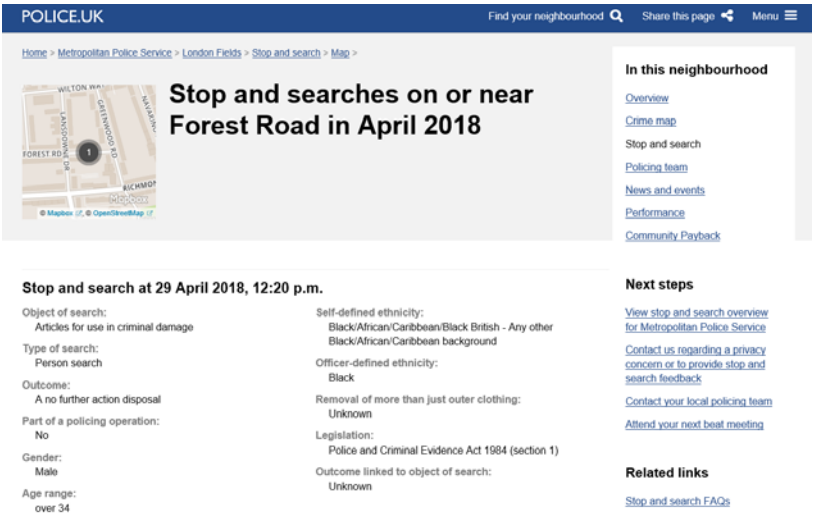
Badanie przeprowadzone w Zjednoczonym Królestwie w 2015 r. dotyczące użycia 500 kamer przez 814 funkcjonariuszy londyńskiej policji wykazało „brak ogólnego wpływu na liczbę lub rodzaj przeprowadzonych zatrzymań i rewizji; brak wpływu na odsetek aresztowanych za przestępstwa z użyciem przemocy; oraz brak dowodów na to, że kamery wpłynęły na zmianę sposobu postępowania funkcjonariuszy względem poszkodowanych albo podejrzanych". W sprawozdaniach oceniających wpływ podobnych prób przeprowadzanych przez inne siły policyjne wykazano nieliczne dowody lub brak dowodów na to, aby miały one jakikolwiek pozytywny wpływ na ograniczenie przestępstw, skarg na działania funkcjonariuszy czy użycie siły.

Aby uzyskać więcej informacji, zob. Big Brother Watch (2017).

Wykres 11: Narzędzie online przedstawiające szczegółowe informacje na temat działań zatrzymania i rewizji prowadzonych w Londynie



Źródło: *Zjednoczone Królestwo, Home Office, strona internetowa przedstawiająca mapę zatrzymań i rewizji.*



Źródło: Zjednoczone Królestwo, Home Office, strona internetowa służąca wyszukiwaniu szczegółowych informacji.

We Francji rozmieszczono kamery nasobne w 300 lokalizacjach na dwuletni okres pilotażowy. W czerwcu 2018 r. ministerstwo spraw wewnętrznych przeprowadziło przegląd, w którym podkreśliło pozytywny wpływ i pozytywne wyniki tej próby. W sprawozdaniu podkreślono w szczególności efekt odstraszający, jaki noszenie kamer nasobnych miało względem osób zatrzymanych w kontekście nadużyć i wyzywania policji. W sprawozdaniach sporządzonych w gminach wskazano, że wykorzystanie poszczególnych kamer ograniczyło agresję i obraźliwe zachowania względem funkcjonariuszy policji. Niektóre gminy wskazały, że korzystanie z kamer nasobnych wydaje się łagodzić sytuacje, które w innym przypadku mogłyby skończyć się obrazą funkcjonariuszy policji. Chociaż w sprawozdaniach tych sugeruje się, że kamery nasobne są przydatne głównie ze względu na swój skutek odstraszający wynikający z samego noszenia, niektóre nagrania wykorzystano jako dowody w postępowaniach sądowych do celów identyfikacji przestępców. Ponadto kilka gmin podkreśliło przydatność narzędzia pod kątem edukacyjnym, gdyż szkolenie niektórych funkcjonariuszy policji w zakresie procedur i technik interwencyjnych opierało

się na oglądaniu nagrań powstałych podczas interwencji. W następstwie okresu pilotażowego przedłożono w parlamencie francuskim projekt ustawy mający na celu harmonizację stosowania kamer nasobnych we wszystkich siłach policyjnych i rozszerzenie ich stosowania na strażaków i służbę więzienną.

Aby uzyskać więcej informacji, zob. Francja, ministerstwo spraw wewnętrznych (2018).

W latach 2012–2013 w Rialto w Stanach Zjednoczonych przeprowadzono duży dwunastomiesięczny test, w którym przyjrzano się, czy kamery nasobne będą prowadzić do pożądanych społecznie zachowań wśród noszących je funkcjonariuszy. Wyniki wykazały, że w porównaniu z 2011 r. podczas dwunastomiesięcznego okresu testu użycie siły spadło z 60 do 25 przypadków, a liczba skarg na policję zmniejszyła się z 28 do 3.

Aby uzyskać więcej informacji, zob. Farrar, T. (2018).

Stosowanie kamer nasobnych przez policję budzi jednak pewne istotne obawy związane z prawami podstawowymi i obawy operacyjne. Konieczne jest stosowanie jasnych zabezpieczeń i polityk dotyczących ich użycia, aby odpowiedzieć na te obawy.

- **Rola kamer nasobnych w wykrywaniu niezgodnego z prawem profilowania i zniechęcaniu do niego** nie jest jasna. Kamery nagrywają poszczególne zdarzenia i nie umożliwiają gromadzenia danych statystycznych, które można by było wykorzystać do ustalenia, czy operacje zatrzymania i rewizji mają charakter dyskryminacyjny. Można je raczej wykorzystać do przeglądu i omówienia poszczególnych spotkań, co może być pomocne w podniesieniu jakości.

- Stosowanie kamer nasobnych może mieć **negatywny wpływ na stosunki ze społecznościami mniejszościowymi**, jeżeli mają one poczucie, że jest ono ukierunkowane szczególnie na nie. Opracowanie zabezpieczeń i polityk w konsultacji z lokalnymi społecznościami może pomóc w promowaniu kamer nasobnych jako narzędzia służącego podniesieniu odpowiedzialności, a nie stygmatyzacji grup mniejszości.

- Stosowanie kamer nasobnych wiąże się z **konsekwencjami w odniesieniu do praw do prywatności i do ochrony danych**, a także innymi podstawowymi

prawami człowieka. Mogą one na przykład wpływać na wolność pokojowych zgromadzeń, jeżeli stosuje się je w celu monitorowania publicznych demonstracji. Często nie jest jasne, kiedy należy włączyć lub wyłączyć kamerę, i co się dzieje, gdy funkcjonariusz zapomni włączyć kamerę lub zdecyduje o niewłączaniu kamery: konieczne jest sformułowanie jasnych wytycznych w tym obszarze. Prywatne przedsiębiorstwa świadczące takie usługi muszą mieć jasność, że nie mogą przetwarzać nagrań do własnych celów. Stosowanie kamer nasobnych powinno być prawnie uregulowane, aby zapewnić zgodność z prawami podstawowymi.

Koncentracja na skutecznym stosowaniu kamer nasobnych

W zapewnieniu skutecznego stosowania kamer nasobnych może pomóc przestrzeganie trzech istotnych zasad:

- **autentyczność**: obrazy muszą być jasno związane ze zdarzeniem. Należy rejestrować dzień i godzinę (np. za pomocą znacznika czasu) i dokładną lokalizację zdarzenia;
- **rzetelność**: wysyłanie obrazów do systemu centralnego powinno się odbywać w rygorystyczny, bezpieczny i poufny sposób. Obrazy te powinny być zgodne z zasadami ochrony danych i poszanowaniem życia prywatnego, nie należy ich zatem przechowywać dłużej niż przez okres przewidziany w prawie;
- **dopuszczalność**: aby nagranie mogło być przydatne w postępowaniu karnym, musi być dopuszczalne w sądach. Może ona obejmować:
  - unikanie ciągłego nagrywania, które stanowi nieakceptowalną ingerencję w prawo do prywatności zarówno funkcjonariuszy policji, jak i filmowanych osób;
  - informowanie osób, które mogą być nagrywane, i uzyskanie ich zgody (w razie konieczności);
  - przechowywanie obrazów z zachowaniem odpowiedniego poziomu bezpieczeństwa i śledzenie dostępu do obrazów ze strony zarówno funkcjonariuszy policji, jak i obywateli.

Aby uzyskać więcej informacji, zob. Coudert i in. (2015), s. 8.

Dalszy rozwój technologiczny będzie wymagał opracowania nowych zabezpieczeń, aby zapewnić stosowanie kamer nasobnych zgodnie z prawem. Na przykład kamery, które mogą automatycznie rozpoznać twarz osoby, porównując i dopasowując ją z wcześniejszymi zapisami w istniejącej bazie danych, stawiają nowe wyzwania w odniesieniu do praw do prywatności i do ochrony danych.

Analiza przykładów

Kamery nasobne w policji: tabela wyników w zakresie polityki (USA)

Aby zwiększyć przejrzystość i odpowiedzialność w zakresie stosowania kamer nasobnych, organizacje Leadership Conference on Civil and Human Rights i Upturn w Stanach Zjednoczonych opracowały narzędzie służące ocenie i zorganizowaniu informacji, które można pozyskać z nagrania z kamery nasobnej.

W ramach narzędzia proponuje się osiem kryteriów oceny takiego nagrania:

1. Czy policja upubliczniła nagranie i czy jest ono łatwo dostępne?
2. Czy gestia funkcjonariuszy co do tego, kiedy należy rejestrować, jest wyraźnie ujawniana?
3. Czy rozwiązano kwestię prywatności?
4. Czy funkcjonariusze muszą przejrzeć nagranie przed sporządzeniem wstępnego pisemnego raportu?
5. Czy nieoznakowane nagranie powinno zostać usunięte w określonym terminie?
6. Czy nagranie jest chronione przed manipulowaniem i nadużyciem?
7. Czy nagranie jest udostępniane osobom wnoszącym skargi?
8. Czy ograniczono stosowanie technologii biometrycznych do identyfikacji osób znajdujących się na nagraniu?

Inicjatywy takie mogą być pomocne w umacnianiu odpowiedzialności poprzez ustanawianie norm i zachęcanie do wdrażania mechanizmów oceny odpowiedniego gromadzenia i wykorzystywania nagrań.

Aby uzyskać więcej informacji, zob. strona internetowa z tabelą wyników w zakresie polityki organizacji Leadership Conference on Civil and Human Rights i Upturn.

2.3.3. Mechanizmy wnoszenia skarg

Skuteczne mechanizmy wnoszenia skarg mogą zarówno zwalczać nadużycia, jak i pomagać w zabezpieczaniu i odbudowywaniu zaufania względem operacji prowadzonych przez policję i organy zarządzania granicami. Zazwyczaj istnieją wraz z formalnymi kanałami prawnymi umożliwiającymi osobom fizycznym zaskarżenie działania lub decyzji organu publicznego przed niezależnym i bezstronnym sądem.

Aby były one skuteczne, istotne jest, aby:

- **osoby fizyczne miały łatwy dostęp do mechanizmów wnoszenia skarg**: dowody niezmiennie pokazują, że ludzie niechętnie wnoszą skargi, np. z uwagi na zbyt długi czas rozpatrywania lub zbyt wysokie koszty, lub z powodu strachu przed negatywnymi reperkusjami. Zapewnienie łatwego dostępu do mechanizmów wnoszenia skarg za pośrednictwem internetowych platform, takich jak strony internetowe lub aplikacje, może zachęcić ludzi do korzystania z nich. Ponadto organizacje mogą wspierać osoby we wnoszeniu skarg, wnosząc skargi w ich imieniu albo za pomocą mechanizmów dochodzenia roszczeń zbiorowych, jak przewidziano w art. 80 ust. 2 RODO;

- **rozpatrywanie skarg odbywało się w sposób przejrzysty**: pomoże to w podniesieniu zaufania względem mechanizmów wnoszenia skarg;

- **organy zajmujące się rozpatrywaniem skarg były niezależne** od organizacji lub od części organizacji, której skarga dotyczy.

Istnieje szeroki zakres różnych mechanizmów, które zajmują się różnego rodzaju skargami. Na wykresie 12 przedstawiono niektóre mechanizmy wnoszenia skarg dostępne w państwach członkowskich UE i na szczeblu unijnym.

Wykres 12: Przegląd mechanizmów wnoszenia skarg w państwach członkowskich UE

Źródło: *FRA, 2018.*

Dzięki mechanizmom, w ramach których funkcjonariusze policji spotykają się z członkami społeczeństwa, aby wysłuchać ich skarg, omówić kwestię profilowania i uzyskać informacje zwrotne na temat swoich operacji, możliwe jest wyciągnięcie ważnych wniosków, aby usprawnić procesy regulujące profilowanie. Mechanizmy te stwarzają również sposobność do zaangażowania społeczeństwa w działania ścigania przestępstw (zob. analiza przykładów).

Analiza przykładów

Publiczne mechanizmy wnoszenia skarg w sektorze ścigania przestępstw

Publiczne panele kontroli (West Midlands Police – Zjednoczone Królestwo)

Każdy z ośmiu policyjnych okręgów miejskich podlegających pod West Midlands Police (WMP) prowadzi odbywające się co dwa miesiące spotkanie panelu kontroli w zakresie zatrzymania i rewizji, któremu przewodzą członkowie społeczeństwa. Panele te oceniają rejestry zatrzymań i rewizji, zapewniają, aby WMP przestrzegała prawa, i udostępniają społecznościom kanał, którym mogą oni przekazać skargi i podnieść kwestie, które ich niepokoją. Harmonogramy i protokoły spotkań są publikowane online. WMP przyjęła szereg dodatkowych praktyk związanych z zaangażowaniem społeczności, starając się zwiększyć sprawiedliwość i ukierunkowanie ulicznych zatrzymań, jak również odpowiedzialność funkcjonariuszy.

Aby uzyskać więcej informacji, zob. West Midlands Police, strona internetowa na temat zatrzymania i rewizji i Her Majesty's Inspectorate of Constabulary (2016).

Panele dotyczące rozsądnych podstaw (Northamptonshire Police – Zjednoczone Królestwo)

Northamptonshire Police ustanowiła panele dotyczące rozsądnych podstaw, aby zaangażować członków społeczeństwa w poprawę operacji zatrzymania i rewizji. Panele te stanowią kanał dyskusji na temat wykonywania uprawnień w zakresie zatrzymania i rewizji oraz ich wpływu na społeczności. Przewodniczy im główny inspektor, a składają się one z funkcjonariuszy pierwszej linii i dwóch członków społeczności, przy czym mogą to być przestępcy lub byli przestępcy. Oprócz poprawy komunikacji między policją a społeczeństwem, panel może pozbawić funkcjonariuszy ich uprawnień

i skierować ich na dodatkowe szkolenie w celu poprawy prowadzenia przez nich operacji zatrzymania i rewizji.

Aby uzyskać więcej informacji, zob. stronę internetową Northamptonshire Police dotyczącą panelu i Open Society Justice Initiative (2018a).

Nieformalna sieć mechanizmów wnoszenia skarg przeciwko policji

Sieć niezależnych organów rozpatrujących skargi na policję (IPCAN) jest nieformalną siecią służącą wymianie informacji i współpracy między niezależnymi strukturami odpowiedzialnymi za zewnętrzną kontrolę sił bezpieczeństwa. Utworzona w 2013 r. sieć skupia organy zajmujące się rozpatrywaniem skarg z ok. 20 państw. Podmioty te, głównie z państw członkowskich UE, otrzymują i przetwarzają skargi przeciwko siłom bezpieczeństwa publicznego i czasami przeciwko podmiotom prywatnym.

Aby uzyskać więcej informacji, zob. strona internetowa IPCAN.

W zarządzaniu granicami mechanizmy wnoszenia skarg można wdrożyć, umożliwiając wnoszenie skarg na miejscu, lub *ex post*. Możliwość dostępu do takich mechanizmów zwiększa przejrzystość i odpowiedzialność, a także buduje wzajemny szacunek i dobre stosunki między strażą graniczną a społeczeństwem. Dzięki wariantowi wniesienia skargi *ex post* do podmiotu wyższego szczebla, a nie tylko możliwości wniesienia jej bezpośrednio na przejściu granicznym, istnieje pewien poziom nadzoru i może to pozytywnie wpłynąć na chęć podróżnych do zgłaszania ewentualnych zdarzeń[36].

Analiza przykładów

Publiczne mechanizmy wnoszenia skarg w zarządzaniu granicami

Wewnętrzny mechanizm wnoszenia skarg w porcie lotniczym Manchester (Zjednoczone Królestwo)

W porcie lotniczym Manchester działa centralna platforma wnoszenia skarg stanowiąca pojedynczy punkt kontaktowy dla wszystkich pasażerów pragnących wnieść skargę. Skargi można wnosić za pośrednictwem

36 FRA (2014b).

poczty elektronicznej, listownie, telefonicznie, faksem lub osobiście, w języku angielskim lub walijskim. W wytycznych dla sił straży granicznej Zjednoczonego Królestwa określono możliwe sposoby rozpatrywania skarg. Niewielkie przewinienia, takie jak nieuprzejmość, gwałtowność czy nieodpowiednia postawa, można zazwyczaj rozpatrzeć lokalnie. Dostępne warianty obejmują wyjaśnienie kwestii z klientem, wyjaśnienie procedur operacyjnych, uzgodnienie dalszych działań i w stosownych przypadkach zaoferowanie przeprosin. Skargi na temat poważnych przewinień przypisuje się zazwyczaj jednostce ds. norm zawodowych. W wytycznych dla sił straży granicznej zawarto test na określenie znaków możliwej dyskryminacji, która stanowiłaby poważne przewinienie. Jeżeli istnieją mocne wstępne dowody na to, że potraktowanie pasażera w dany sposób można wyjaśnić czynnikami innymi niż rasa, sprawę zazwyczaj kieruje się do lokalnego rozpatrzenia.

Aby uzyskać więcej informacji, zob. FRA (2014a), s. 74.

Mechanizm wnoszenia skarg indywidualnych Frontexu (UE)

W następstwie przyjęcia w 2016 r. nowego rozporządzenia w sprawie Europejskiej Straży Granicznej i Przybrzeżnej (Frontex) Frontex ustanowił mechanizm wnoszenia skarg indywidualnych w celu monitorowania przestrzegania praw podstawowych w działaniach Agencji. Działania te obejmują projekty pilotażowe, operacje powrotowe, wspólne operacje, szybkie interwencje na granicy, rozmieszczenie zespołu wspierającego zarządzanie migracjami oraz interwencje powrotowe. Każda osoba, której prawa zostały bezpośrednio naruszone w konsekwencji działań personelu, w tym personelu krajowych organów publicznych, zaangażowanego w takie działania Frontexu, może wnieść skargę do urzędnika ds. praw podstawowych Frontexu. Urzędnik ten podejmuje decyzję na temat dopuszczalności skargi i przesyła ją do dyrektora wykonawczego Frontexu, a także do organów państwa członkowskiego, którego sprawa dotyczy, jeżeli w rzekome naruszenie był zaangażowany personel krajowy. Skargi można wnosić w dowolnym języku, za pośrednictwem wiadomości e-mail, listownie lub za pośrednictwem internetowego formularza skargi dostępnego na stronie internetowej Frontexu: http://frontex.europa.eu/complaints/.

Koncentracja na prawach funkcjonariuszy organów ścigania

Funkcjonariuszom policji przysługują te same prawa i wolności co innym osobom, i podczas wykonywania swojej pracy podlegają oni ochronie zgodnie z normami w zakresie praw człowieka. Mogą oni odnosić się do swoich praw określonych w różnych międzynarodowych dokumentach dotyczących praw człowieka, takich jak: Europejska konwencja praw człowieka (EKPC) lub Międzynarodowy pakt praw obywatelskich i politycznych (MPPOiP). W europejskim kodeksie etyki zawodowej policji wyjaśniono, że „[f]unkcjonariusze policji, co do zasady, korzystają z tych samych praw obywatelskich i politycznych co ogół obywateli. Ograniczenia w tym zakresie mogą być wprowadzone w zgodzie z prawem i Europejską konwencją praw człowieka i tylko, gdy są niezbędne dla wykonywania funkcji policyjnych w demokratycznym społeczeństwie". Jeden wyjątek można znaleźć w art. 11 EKPC, który odnosi się do wolności zgromadzeń i stowarzyszania się.

Pełniąc funkcje policyjne, szczególnie wykonując uprawnienia policji, funkcjonariusz nie działa jako osoba prywatna, lecz jako organ państwowy. Obowiązek państwa dotyczący poszanowania i ochrony praw człowieka wpływa zatem bezpośrednio na możliwości, jakie posiada funkcjonariusz policji, gdy reaguje na agresję. Prawa funkcjonariuszy policji, którzy mogą ryzykować zranienie lub własne życie, aby wypełnić swoje obowiązki, muszą również być szanowane i chronione, np. poprzez dostarczanie im sprzętu ochronnego, staranne planowanie operacji policyjnych lub podejmowanie środków zapobiegawczych. Ograniczenia ich praw mogą być konieczne do pełnienia funkcji policyjnych, ale każde takie ograniczenie musi odzwierciedlać zasadę proporcjonalności. Z uwagi na jej szczególną rolę jako organu państwowego policja może doświadczać większych ograniczeń jej praw niż „przeciętny obywatel". Jeżeli na przykład na demonstracji pojawi się przemoc, „przeciętny obywatel" może uciec lub zwrócić się o pomoc, funkcjonariusz policji natomiast jest zobowiązany do ochrony praw człowieka innych osób i do przywrócenia porządku publicznego.

Aby uzyskać więcej informacji, zob. FRA (2013).

3

Profilowanie z wykorzystaniem algorytmu

Profilowanie z wykorzystaniem algorytmu obejmuje wszelkie techniki komputerowe stopniowo analizujące dane w celu określenia tendencji, wzorców lub korelacji[37]. W procesie profilowania wybór osób „opiera się na powiązaniach z innymi osobami, określonych za pomocą algorytmu, nie zaś rzeczywistego zachowania", a „wybory dokonywane przez osoby są organizowane zgodnie z informacjami na temat grupy", nie zaś zgodnie z osobistymi wyborami osoby[38].

Profilowanie z wykorzystaniem algorytmu może być skutecznym sposobem wykorzystywania danych przez organizacje zarządzania granicami i egzekwowania prawa do zapobiegania przestępstwom, ich wykrywania i prowadzenia dochodzeń w ich sprawie. Gromadzenie i przetwarzanie dużych zbiorów danych budzi jednak szereg obaw związanych z prawami podstawowymi. Oprócz znaczenia, jakie ma unikanie dyskryminacji, profilowanie z wykorzystaniem algorytmu pociąga za sobą nowe zagrożenia, szczególnie związane z prawami do prywatności i ochrony danych. W niniejszej sekcji skupiono się najpierw na tych nowych zagrożeniach. Następnie zilustrowano wyzwania w odniesieniu do praw podstawowych związane ze stosowaniem profilowania z wykorzystaniem algorytmu w wielkoskalowych bazach danych do celów zarządzania granicami i do celów bezpieczeństwa, i zaproponowano pewne sposoby minimalizacji tych zagrożeń.

37 Aby uzyskać więcej informacji na temat tego, czym są algorytmy, zob. FRA (2018b), s. 4.

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

Koncentracja na działaniach policji opartych na prognozowaniu

Organy ścigania korzystają z kilku aplikacji służących prognozowaniu czasu i miejsca popełnienia przestępstwa. Niektóre przykłady takich aplikacji to: PredPol w Zjednoczonym Królestwie i USA, Criminality Awareness System (CAS) w Niderlandach i Precobs w Niemczech i Szwajcarii. Skuteczność tych metod prognozowana do celów zapobiegania przestępstwom nie została jednak jeszcze poddana odpowiedniej ocenie. Dotychczas z dowodów wynikają sprzeczne wnioski, jak wskazano w następujących przykładach.

Badania terenowe w zakresie działań policji opartych na prognozowaniu w Kencie (Zjednoczone Królestwo) i Los Angeles (USA)

Policja w Zjednoczonym Królestwie i w USA przeprowadziła eksperyment w celu porównania bardziej tradycyjnego podejścia z w pełni zautomatyzowanym algorytmem służącym identyfikacji obszarów o szczególnej koncentracji przestępstw i zapewnieniu rozplanowania patroli policyjnych.

Wnioski z eksperymentu wykazały, że zautomatyzowany algorytm lepiej określał przyszłe przestępstwa. Przewidywał 1,4–2,2 razy więcej działań przestępczych niż funkcjonariusz analizujący przestępstwa przy użyciu tradycyjnych danych wywiadowczych na temat przestępstw i praktyk mapowania przestępstw. Ponadto działania związane z patrolowaniem opierające się na narzędziach służących prognozowaniu są skuteczniejsze i prowadzą średnio do ograniczenia liczby przestępstw o 7,4 %.

Aby uzyskać więcej informacji, zob. Mohler, G.O., i in. (2016).

Program PILOT (ang. *Predictive Intelligence Led Operational Targeting*) w Shreveport (USA)

W programie tym wykorzystuje się model prognozowania do identyfikacji niewielkich obszarów o zwiększonym zagrożeniu wystąpienia przestępczości przeciwko mieniu i wdraża się w nich model interwencyjny w celu zapobiegania przestępczości przeciwko mieniu. Wyniki z trzech dzielnic, w których korzystano z programu PILOT, porównano z wynikami z trzech dzielnic, w których prowadzono tradycyjne działania policji. Żadne dane statystyczne nie wskazywały na to, aby w trzech badanych dzielnicach,

w których korzystano z programu PILOT, wystąpił większy spadek przestępczości przeciwko mieniu.

Aby uzyskać więcej informacji, zob. Hunt, P. i in. (2014).

Oprogramowanie „Beware" (USA)

Dzięki oprogramowaniu „Beware" u funkcjonariuszy odbierających połączenia alarmowe wyświetlają się wyniki zakodowane według kolorów (na czerwono, żółto i zielono), wskazując poziom zagrożenia w odniesieniu do osoby lub miejsca. Oprogramowanie przeszukuje bazy danych, w tym rejestry aresztowań, rejestry własności, komercyjne bazy danych, pogłębione wyszukiwania internetowe, posty w mediach społecznościowych i inne publicznie dostępne bazy danych.

Nie dokonano oceny słabych i mocnych stron tego systemu. Brak nadzoru nad procesem decyzyjnym i tajny charakter algorytmu, który jest chroniony tajemnicą handlową, budzą jednak obawy co do odpowiedzialności. Ponadto potencjalna niedokładność zgromadzonych danych lub informacje wnioskowane na podstawie analizy mogą ograniczać ogólną skuteczność tego narzędzia.

Aby uzyskać więcej informacji, zob. American Civil Liberties Union (2016).

Analiza przykładów

Ocena wpływu i zagrożenia działań policji opartych na prognozowaniu – narzędzie oceniające ALGO-CARE

Należy uwzględnić potencjalne negatywne skutki stosowania działań policji opartych na prognozowaniu, aby zapewnić zrównoważony i przejrzysty przegląd jego wpływu na społeczeństwo. Zgodnie z wnioskami z analizy przeprowadzonej przez grupę obejmującą pracowników akademickich i funkcjonariuszy policji, ponieważ działania policji oparte na prognozowaniu są wciąż w Zjednoczonym Królestwie w fazie eksperymentalnej, należy prowadzić szczegółową ocenę ich wpływu na społeczeństwo i na poszczególne osoby. W badaniu wysunięto argumenty, że istnieją decyzje, które mogą mieć zbyt poważne konsekwencje dla społeczeństwa i dla jednostki, aby mogły

podlegać wpływom nowo powstałej technologii; w przypadkach tych nie należy więc podejmować decyzji z wykorzystaniem algorytmu.

Grupa opracowała ramy decyzyjne o nazwie ALGO-CARE służące rozmieszczaniu narzędzi oceny z wykorzystaniem algorytmu w kontekście działań policji. Ramy te mają służyć jako wytyczne dla funkcjonariuszy policji, gdy oceniają oni potencjalne zagrożenie, stosując działania policji oparte na prognozowaniu. Starają się również przełożyć kluczowe zasady prawa publicznego i praw człowieka na praktyczne rozważania i wskazówki, które mogą wziąć pod uwagę podmioty sektora publicznego.

W ramach narzędzia oceniającego zachęca się funkcjonariuszy policji do stosowania działań policji opartych na prognozowaniu za pośrednictwem ośmiu kroków uzupełniających:

- **doradczy charakter**: ocena zakresu ludzkiej interwencji;
- **legalność**: ocena prawnego uzasadnienia zastosowania algorytmu;
- **stopień szczegółowości**: ocena, czy algorytm może osiągnąć wystarczający stopień szczegółowości w konkretnej sprawie;
- **własność**: zapewnienie, aby siły policyjne były prawnym właścicielem i aby posiadały zdolność techniczną do regularnego dostępu, utrzymania, regularnej aktualizacji i poprawy kodu źródłowego;
- **zaskarżalność**: zapewnienie, aby funkcjonowały mechanizmy nadzoru i kontroli;
- **dokładność**: ocena tego, czy algorytm pasuje do celu działań policyjnych, czy może podlegać okresowej weryfikacji oraz czy prawdopodobieństwo wystąpienia niedokładności i jej wpływ stanowią ryzyko możliwe do zaakceptowania;
- **odpowiedzialność**: ocena sprawiedliwości, rozliczalności i przejrzystości algorytmu;
- **możliwość wyjaśnienia**: ocena dostępności informacji w odniesieniu zarówno do zasad podejmowania decyzji, jak i wpływu każdego z czynników na wynik końcowy.

Aby uzyskać więcej informacji, zob. Oswald, M., i in. (2017).

3.1. Ramy ochrony danych regulujące profilowanie z wykorzystaniem algorytmu

Rozwój i coraz większe wykorzystanie nowych technologii – w tym rosnące wykorzystywanie dużych zbiorów danych w celu wspierania podejmowania decyzji – skłoniły UE w 2016 r. do szeroko zakrojonej rewizji przepisów regulujących przetwarzanie danych osobowych. Dwa nowe instrumenty, ogólne rozporządzenie o ochronie danych (RODO) i dyrektywa dotycząca policji, ustanowiły ważne zasady i normy obejmujące wszelkie decyzje podejmowane w oparciu o komputerowe procesy podejmowania decyzji, w tym profilowanie z wykorzystaniem algorytmu.

RODO i dyrektywa dotycząca policji weszły w życie w maju 2018 r., co oznacza, że w momencie pisania niniejszego przewodnika istnieje niewiele praktycznych przykładów ich wdrażania. W sekcji 1.2.2 opisano normy prawne regulujące prawa do prywatności i do ochrony danych oraz wyjaśniono niektóre główne różnice między RODO a dyrektywą dotyczącą policji (zob. tabela 2). Niniejszy rozdział opiera się na tych informacjach w celu opisania i wyjaśnienia wymogów prawnych dotyczących profilowania z wykorzystaniem algorytmu, które wprowadzono RODO i dyrektywą dotyczącą policji. Oto niektóre z nich:

- przetwarzanie danych musi odbywać się w określonym celu i w oparciu o konkretną podstawę prawną;
- należy poinformować osoby fizyczne o przetwarzaniu ich danych;
- dane muszą być przechowywane w sposób bezpieczny;
- należy wykrywać niezgodne z prawem przetwarzanie danych i zapobiegać mu.

Funkcjonariusze policji i straży granicznej, którzy chcieliby uzyskać dodatkowe informacje na temat wymogów prawnych opisanych w niniejszym rozdziale, powinni zwrócić się do inspektorów ochrony danych w swoich organizacjach. Ponadto w publikacji *Handbook on European Data Protection Law* (Podręcznik europejskiego prawa ochrony danych) opracowanej przez FRA, EIOD i Radę Europy, przedstawiono dodatkowe wytyczne dotyczące stosowania dyrektywy dotyczącej policji i RODO[39].

39 FRA, EIOD i Rada Europy (2018).

Najważniejsze kwestie

- Profilowanie z wykorzystaniem algorytmu musi być **zgodne z prawem**, **konieczne** i **proporcjonalne**.
- Przetwarzanie danych nie może odbywać się bez **określonego celu opartego na konkretnej podstawie prawnej**.
- Osobom fizycznym przysługują konkretne prawa opisane szczegółowo w przepisach RODO i dyrektywy dotyczącej policji, w tym:
  - **prawo do bycia poinformowanym**, w tym do otrzymywania istotnych informacji o zasadach stosowania algorytmu;
  - prawo **dostępu do swoich danych osobowych**;
  - prawo **do wniesienia skargi** do organu nadzorczego; oraz
  - prawo do **skutecznego środka ochrony prawnej przed sądem**.
- Dane należy gromadzić, przetwarzać i przechowywać **w bezpieczny sposób**.
- Należy **zapobiegać** niezgodnemu z prawem przetwarzaniu danych i **wykrywać je**.

3.1.1. Przetwarzanie danych musi się odbywać w określonym celu

Wszelkie przetwarzanie danych osobowych musi mieć podstawę prawną. Oznacza to, że należy je wykonywać, aby osiągnąć **określony cel** przewidziany w prawie.

Zanim dojdzie do jakiegokolwiek przetwarzania, funkcjonariusz musi znać jego cel. Należy stwierdzić, między innymi:

- Czy przetwarzanie danych służy wykrywaniu przestępstw?
- Czy przetwarzanie ma na celu utrzymanie bezpieczeństwa publicznego?
- Czy przetwarzanie ma na celu zwalczanie terroryzmu?

Po poprawnym określeniu celu funkcjonariusze będą wiedzieli, które ramy prawne powinni zastosować i jakie są ich obowiązki prawne. W tabeli 4 przedstawiono, w jaki sposób określić, które ramy prawne należy zastosować.

Tabela 4: Określenie odpowiednich ram prawnych w zależności od celu przetwarzania

1. Jaki jest cel przetwarzania danych?	
• **zapobieganie przestępstwom, badanie, wykrywanie przestępstw i prowadzenie postępowań przygotowawczych;** • **egzekwowanie sankcji karnych;** • **zabezpieczanie bezpieczeństwa publicznego.**	• każdy inny cel
⬇	⬇
2. Zastosowanie ma dyrektywa dotycząca policji	**2. Zastosowanie ma ogólne rozporządzenie o ochronie danych**
⬇	⬇
3. Prawo Unii lub prawo krajowe definiuje*	**3. Zezwala się na przetwarzanie wyłącznie gdy:**
• **które dane osobowe można przetwarzać;** • **określone cele przetwarzania danych.**	• osoba, której dane dotyczą, **wyraziła na to zgodę**; • jest ono niezbędne do wykonania **umowy**; • jest ono niezbędne do wypełnienia **obowiązku prawnego**; • jest ono niezbędne do ochrony **żywotnych interesów** osoby; albo • jest ono niezbędne do wykonania zadania realizowanego **w interesie publicznym**.
⬇	⬇

4. Czy cel profilowania jest wyłączony z przepisów dyrektywy dotyczącej policji?	4. Czy cel profilowania jest wyłączony z przepisów RODO?
Prawa do bycia poinformowanym, do dostępu do danych osobowych i do żądania zmiany lub usunięcia danych mogą zostać ograniczone (w całości lub w części) w następujących przypadkach: • aby uniknąć utrudniania oficjalnych lub prawnych **badań**, dochodzeń lub procedur; • aby uniknąć szkody w zapobieganiu przestępstwom, wykrywaniu i badaniu przestępstw lub prowadzeniu postępowań przygotowawczych, lub egzekwowaniu sankcji karnych; • aby chronić bezpieczeństwo publiczne; • aby chronić bezpieczeństwo narodowe; • aby chronić prawa i wolności innych osób.	Obowiązki (przejrzystości, informowania i zgłaszania naruszeń) i prawa (dostępu, sprostowania, usunięcia, sprzeciwu lub do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu) ustanowione w RODO **mogą zostać ograniczone** prawem krajowym lub prawem Unii w celu zabezpieczenia: • bezpieczeństwa narodowego, obrony narodowej lub bezpieczeństwa publicznego; • zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw lub egzekwowania sankcji karnych, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; • innych ważnych celów realizowanych w interesie publicznym Unii lub państwa członkowskiego, w szczególności w ważnym interesie gospodarczym lub finansowym Unii lub państwa członkowskiego, w tym w sprawach pieniężnych, budżetowych i podatkowych, związanych ze zdrowiem publicznym i zabezpieczeniem społecznym; • ochrony niezależności sądu i postępowania sądowego; • zapobiegania naruszeniom etyki zawodów regulowanych, prowadzenia postępowań przygotowawczych, wykrywania i ścigania takich naruszeń; • monitorowania, kontroli lub funkcji regulacyjnej związanych, nawet okazjonalnie, z wykonywaniem władzy publicznej w szczególnych przypadkach; • ochrony osoby, której dane dotyczą, oraz praw i wolności innych osób; • egzekwowania roszczeń cywilnoprawnych.

Uwaga: ** Akty prawa krajowego transponujące dyrektywę dotyczącą policji są dostępne na stronie internetowej portalu EUR-Lex.*

Źródło: *FRA, 2018.*

Tabela 5: Obowiązek przekazania osobie fizycznej informacji na temat profilowania: rodzaj danych, środki komunikacji i wyjątki

	Obowiązek powiadomienia – lista kontrolna
Komu?	Osobie, której dane są przetwarzane
Jak?	• jasny i prosty język • łatwo dostępna forma • w takiej samej formie, w jakiej przekazała wniosek – *preferowane środki elektroniczne*
Co?	**Informacje na temat przetwarzania**: • nazwa organu i dane kontaktowe • dane kontaktowe inspektora ochrony danych • cele przetwarzania • podstawa prawna przetwarzania • maksymalny okres przechowywania danych • rodzaje osób/organizacji, które otrzymają dane **Informacje na temat praw osoby fizycznej:** • prawo do **wniesienia skargi** do organu nadzorczego i dane kontaktowe organu nadzorczego • prawo żądania **dostępu** do swoich danych • **sprostowanie** lub **usunięcie** danych osobowych • prawo żądania **ograniczenia** przetwarzania
Wyjątki	• W odniesieniu do nadmiernych (tj. powtarzalnych) lub wyraźnie nieuzasadnionych żądań • Gdy nie można wyraźnie potwierdzić tożsamości wnioskodawcy • Gdy przekazanie informacji utrudniłoby dochodzenie • Gdy przekazanie informacji byłoby ze szkodą dla zapobiegania przestępstwom/prowadzenia postępowań przygotowawczych • Aby chronić bezpieczeństwo publiczne i narodowe • Aby chronić prawa innych osób

Źródło: *FRA, 2018.*

3.1.2. Należy informować osoby fizyczne

W art. 13 dyrektywy dotyczącej policji i w art. 13 i 14 RODO wymaga się, aby osoby fizyczne były informowane o przetwarzaniu ich danych. W tabeli 5 opisano, w jaki sposób i kiedy należy przekazać informacje osobie, której dane podlegają przetwarzaniu.

Koncentracja na „prawie do wyjaśnienia"

W przypadkach profilowania przy podejmowaniu decyzji w RODO wymaga się, aby przekazać osobie „istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania" danych. Informacje należy przekazać zarówno w momencie gromadzenia danych (powiadomienie), jak i w przypadku, gdy osoba żąda dalszych informacji (prawo dostępu). Prawa tego nie wymieniono wyraźnie w dyrektywie dotyczącej policji. W motywie 38 określono jednak, że „[przetwarzanie automatyczne] powinno zawsze podlegać odpowiednim zabezpieczeniom, wraz z konkretną informacją dla osoby, której dane dotyczą, [...], a zwłaszcza [...] uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji".

Takie „prawo do wyjaśnienia" może w praktyce okazać się trudne do realizacji. Niektóre osoby mogą posiadać umiejętności cyfrowe pozwalające na zrozumienie kodu algorytmu, dla innych zaś wystarczające są uproszczone informacje dotyczące celu przetwarzania i powiązań wykorzystywanych danych. Kluczem do oceny istoty przedstawionego wyjaśnienia jest jego cel. Osoba powinna otrzymać wystarczające informacje, aby zrozumieć cel, logikę i kryteria, które doprowadziły do podjęcia decyzji.

Prawo do wyjaśnienia nie jest prawem bezwzględnym (zob. krok 4 w tabeli 4). Państwa członkowskie mogą ograniczyć to prawo w przepisach w kilku przypadkach, w tym ze względów: bezpieczeństwa narodowego, obrony, bezpieczeństwa publicznego, zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw, egzekwowania sankcji karnych, ochrony osób, których dane dotyczą, lub ochronę praw i wolności innych osób, egzekwowania roszczeń cywilnoprawnych.

Przedstawianie rozsądnych informacji na temat celu i przewidywanych konsekwencji przetwarzania jest jednak zalecaną dobrą praktyką. Opracowywanie prostych sposobów wyjaśniania logiki takiego przetwarzania i kryteriów stosowanych do podjęcia decyzji zwiększy ostatecznie przejrzystość i odpowiedzialność.

Aby uzyskać więcej informacji, zob. RODO, art. 13–15 (prawo do informacji i prawo dostępu), art. 22 (zautomatyzowane podejmowanie decyzji

w indywidualnych przypadkach, w tym profilowanie) i art. 23 (ograniczenia); oraz dyrektywa dotycząca policji, art. 11 (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach) i art. 13–15 (prawo do informacji i prawo dostępu).

Zob. również Grupa Robocza Art. 29 (2018a).

3.1.3. Bezpieczne przechowywanie danych: rejestry, ewidencje i zasady przechowywania

Organy gromadzące i przetwarzające dane osobowe do celów profilowania muszą nie tylko przetwarzać dane w sposób zgodny z prawem, lecz również zapewnić, aby:

- nieuprawnione osoby nie miały dostępu do danych;
- dane nie były wykorzystywane do innych celów niż cel pierwotny; lub
- dane nie były przechowywane dłużej, niż jest to konieczne.

W tym celu organy i funkcjonariusze organów ścigania i funkcjonariusze zarządzający granicami muszą zapewnić wdrożenie odpowiednich środków mających na celu ochronę integralności i bezpieczeństwa danych. Muszą śledzić każdy przypadek dostępu do danych i każde ich wykorzystanie poprzez tworzenie i prowadzenie rejestrów wszystkich czynności przetwarzania lub kategorii czynności przetwarzania (art. 30 RODO i art. 24 dyrektywy dotyczącej policji). Rejestry muszą zawierać:

- **imię i nazwisko lub nazwę** oraz **dane kontaktowe** organów i administratora danych;
- **cel** przetwarzania;
- **kategorie odbiorców**, którym dane osobowe zostały lub zostaną ujawnione;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- informacje o **stosowaniu profilowania**;

- wskazanie **podstawy prawnej** operacji przetwarzania;
- jeżeli jest to możliwe, planowane **terminy** usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO lub w art. 29 ust. 1 dyrektywy dotyczącej policji.

Ponadto jeżeli profilowanie z wykorzystaniem komputerów jest wdrażane do celów ujętych w dyrektywie dotyczącej policji (zob. sekcja 3.2), organy muszą prowadzić ewidencję obejmującą: zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie danych.

Wspomniane rejestry i ewidencje posłużą do wspierania funkcjonariuszy w wykazywaniu zgodności z wymogami prawnymi podczas monitorowania wewnętrznego i zewnętrznego. Jeżeli np. osoba wniesie skargę, organy ścigania i organy zarządzania granicami będą zobowiązane do udostępnienia krajowym organom ochrony danych rejestrów i ewidencji.

Nie należy przechowywać danych osobowych przez okres dłuższy, niż jest to konieczne do osiągnięcia założonego zgodnego z prawem celu. Przechowywanie przez dłuższy okres musi być odpowiednio uzasadnione. W takich przypadkach organy powinny zapewnić, aby przechowywanie podlegało regularnym przeglądom w celu zapewnienia integralności i bezpieczeństwa.

3.1.4. Należy wykrywać niezgodne z prawem przetwarzanie i zapobiegać mu

Wykrywanie niezgodnego z prawem przetwarzania danych osobowych i zapobieganie mu stanowi wyzwanie. Ze względu na specjalistyczne umiejętności konieczne do zrozumienia złożonych algorytmów i dużych baz danych zapewnienie odpowiednich kontroli jest trudne.

Aby poradzić sobie z tym problemem, w RODO i w dyrektywie dotyczącej policji ujęto zabezpieczenia mające pokierować funkcjonariuszy organów ścigania

i organów zarządzania granicami przed przetwarzaniem danych, w trakcie przetwarzania i po takim przetwarzaniu. Odnoszą się one do:

- oceny skutków dla ochrony danych; oraz
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

Ocena skutków

Ramy prawne UE wymagają od policji i od organów zarządzania granicami dokonania oceny skutków przed przeprowadzeniem przetwarzania danych, które z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw osób fizycznych (art. 35 RODO i art. 27 dyrektywy dotyczącej policji). Oznacza to, że oceny skutków należy dokonać nie tylko, gdy wynik przetwarzania może stanowić naruszenie norm ochrony danych i prywatności, lecz również w każdej sytuacji, która może prowadzić do naruszenia *jakiegokolwiek prawa podstawowego*. Mogą one obejmować: prawo do równości i niedyskryminacji, wolność wypowiedzi i informacji; wolność myśli, sumienia i religii; prawo do nauki; ochronę zdrowia; prawo do azylu; oraz ochronę w przypadku usunięcia z terytorium państwa, wydalenia lub ekstradycji. Ocena skutków jest szczególnie istotna w przypadku, gdy profilowanie może mieć konsekwencje prawne dla jednostek. W takich przypadkach RODO i dyrektywa dotycząca policji wymagają dokonania oceny skutków.

Oceny skutków należy dokonać przed samym zautomatyzowanym przetwarzaniem. Cele takiej oceny skutków są jednak dwojakie:

- *a priori*: przed przetwarzaniem danych dokonanie oceny skutków co do jakości danych lub algorytmu przetwarzania pomoże w wykryciu potencjalnych naruszeń praw podstawowych i, w stosownych przypadkach, zaradzeniu im;
- *a posteriori*: po przetworzeniu danych można wymagać od funkcjonariusza wykazania, że działał on zgodnie z prawem. Ocena skutków może pomóc mu w wykazaniu, że wdrożył wszystkie niezbędne środki w celu zapewnienia zgodności z prawem.

Ocena skutków pomoże również funkcjonariuszom w wykryciu ukrytych uprzedzeń, które mogą naruszać prawa do ochrony danych i do niedyskryminacji, i mieć wpływ na jakość profilowania (zob. sekcja 1.3.2).

Koncentracja na zagrożeniach stosowania „algorytmów dynamicznych"

„Algorytmy dynamiczne" to algorytmy, które są stale definiowane na nowo i „usprawniane" w oparciu o „informacje zwrotne". Informacje te tworzą same systemy algorytmiczne i nie jest możliwe ich właściwe zrozumienie ani nawet wyrażenie w prostym języku (zob. art. 35 RODO i art. 27 dyrektywy dotyczącej policji). W przeciwieństwie do „algorytmów statycznych", które opierają się na określonych wcześniej kryteriach, „algorytmy dynamiczne" tworzą **nowe korelacje** poprzez ciągłe ponowne definiowanie samych siebie.

Algorytmy dynamiczne tworzą zagrożenie polegające na tym, że eksperci w dziedzinie programowania w pewnym momencie przestaną rozumieć logikę algorytmu. Sytuacja taka tworzy znaczne **ryzyko mimowolnego powielania istniejących uprzedzeń** oraz utrwalania nierówności społecznych i stygmatyzowania niektórych grup. W takich przypadkach zapewnienie odpowiedzialności i możliwości zaskarżenia dla jednostek, których dotyczy przetwarzanie, jest bardzo trudne.

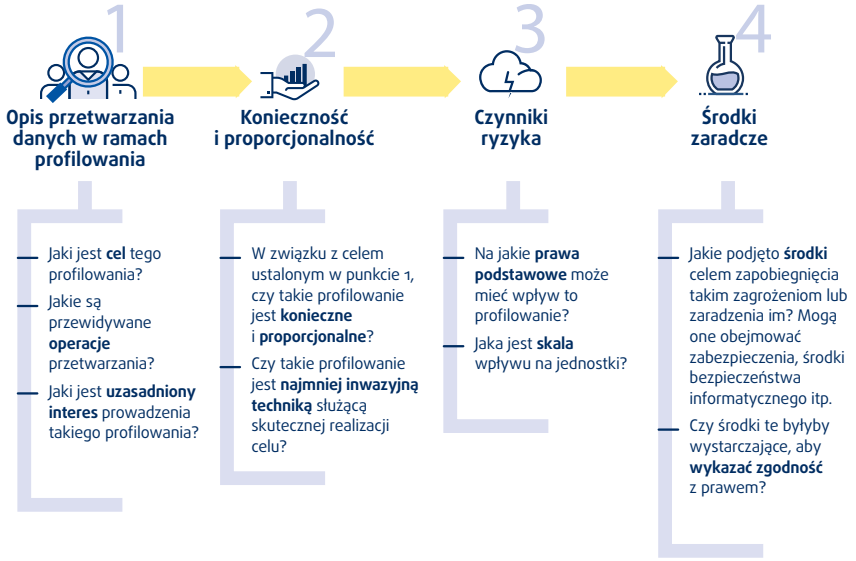
Należy zatem **unikać** stosowania „algorytmów dynamicznych" **lub ograniczyć** takie stosowanie, aby zminimalizować ryzyko utraty możliwości śledzenia kryteriów oceny. Umożliwia to audytorom wewnętrznym i zewnętrznym ocenę algorytmów i ich modyfikacje, gdy okaże się, że są niezgodne z prawem. Jeżeli stosowanie algorytmów dynamicznych jest uzasadnione, należy dokonywać przeglądu czynników ryzyka i badać je w celu zapewnienia, aby nie prowadziły do niezgodnego z prawem profilowania.

Aby uzyskać więcej informacji, zob. Gandy, O. (2010) i Korff, D. (2015).

Ocena skutków może znacznie się różnić w zależności od rodzaju i wolumenu przetwarzanych danych osobowych, a także od rodzaju i celu przetwarzania. Może ona obejmować sprawdzenie jakości danych, kontrole techniczne algorytmu lub algorytmów przetwarzających dane lub pełen przegląd celów przetwarzania itp. Na wykresie 13 przedstawiono minimalne kryteria, które powinny podlegać ocenie.

Grupa Robocza Art. 29 (zastąpiona obecnie przez Europejską Radę Ochrony Danych), która skupia krajowe organy ochrony danych w państwach członkowskich UE, opracowała wytyczne, w których znajduje się więcej informacji na temat oceny skutków

Wykres 13: Minimalne wymogi oceny skutków



Źródło: *FRA, 2018.*

dla ochrony danych. Wytyczne te zawierają szczegółowe mapowanie kryteriów, które należy stosować podczas prowadzenia oceny skutków[40].

Osadzenie zgodności z prawem „w fazie projektowania" oraz „domyślnie"

Niezależnie od tego, czy w ramach oceny skutków wykryto możliwość naruszenia praw podstawowych, można wdrożyć środki służące dalszemu zapobieganiu jakiemukolwiek zagrożeniu niezgodnością z prawem. Nazywa się je „ochroną danych w fazie projektowania" oraz „domyślną ochroną danych" (art. 25 RODO i art. 20 dyrektywy dotyczącej policji).

Ochrona danych w fazie projektowania ma na celu zapewnienie, aby *przed* przetwarzaniem danych i *po* takim przetwarzaniu zostały wdrożone środki techniczne

40 Grupa Robocza Art. 29 (2017a).

i organizacyjne mające zagwarantować przestrzeganie zasad ochrony danych. Na przykład dane osobowe można by było w miarę możliwości poddać pseudonimizacji. Pseudonimizacja jest środkiem, za pomocą którego dane osobowe nie mogą być przypisane osobie bez dodatkowych informacji, które są przechowywane osobno. Klucz umożliwiający ponowną identyfikację osób musi być przechowywany oddzielnie i zabezpieczony[41]. W przeciwieństwie do danych zanonimizowanych dane spseudonimizowane nadal są danymi osobowymi i w związku z tym muszą podlegać przepisom i zasadom dotyczącym ochrony danych.

Domyślna ochrona danych służy zapewnieniu, aby „przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania"[42]. Ma ona wpływ na:

- ilość gromadzonych i przechowywanych danych osobowych;
- rodzaje przetwarzania, które mogą obejmować dane osobowe;
- maksymalny okres przechowywania;
- liczbę osób uprawnionych do dostępu do takich danych osobowych.

Koncentracja na odpowiedzialności

Najważniejszym celem ochrony danych w fazie projektowania i domyślnej ochrony danych jest wspieranie organów ścigania i organów zarządzania granicami i ich funkcjonariuszy w opracowywaniu programów służących profilowaniu z wykorzystaniem algorytmu, które będą zgodne z wymogami w zakresie praw podstawowych, w szczególności z zasadami **zgodności z prawem**, **przejrzystości** i **bezpieczeństwa**.

Środki takie mogą jednak również służyć wykazaniu, w jaki sposób organy zachowują zgodność z wymogami prawa w zakresie **odpowiedzialności**. Zgodnie z prawem od organów przetwarzających dane oczekuje się wdrożenia „odpowiednich środków technicznych i organizacyjnych" służących wykazaniu zachowania zgodności z prawem Unii. Na przykład jeżeli

41 FRA, EIOD i Rada Europy (2018), s. 83.

42 Artykuł 25 ogólnego rozporządzenia o ochronie danych.

osoba wniesie skargę, krajowe organy sądownicze i ochrony danych mogą zwrócić się do organu o przedstawienie każdego z poniższych punktów:

- zasadności, konieczności i proporcjonalności profilowania z wykorzystaniem komputerów;
- zgodności celu z prawem;
- informacji przekazanych osobom;
- integralności i bezpieczeństwa danych;
- środków w zakresie jakości i kontroli przeprowadzonych przed operacjami profilowania i w trakcie takich operacji.

3.2. Wielkoskalowe bazy danych do celów zarządzania granicami i bezpieczeństwa

Unia Europejska opracowała kilka wielkoskalowych systemów lub mechanizmów informatycznych służących gromadzeniu i przetwarzaniu danych, które można wykorzystywać do celów zarządzania granicami i migracją oraz, w pewnym stopniu, do celów ścigania przestępstw. Służą one jako przykłady ilustrujące niektóre powszechne wyzwania związane ze stosowaniem profilowania z wykorzystaniem algorytmu, a także jako możliwe zabezpieczenia.

W tabeli 6 przedstawiono pokrótce unijne systemy i mechanizmy informatyczne. W załączniku przedstawiono szczegółowy przegląd istniejących i planowanych wielkoskalowych unijnych systemów informatycznych (stan na marzec 2018 r.).

Wielkoskalowe unijne systemy informatyczne są wykorzystywane w szeregu procesów związanych z migracją, w tym do procesu oceny ryzyka przed przybyciem, procesu azylowego, procesu ubiegania się o przyznanie wizy, podczas kontroli na granicy, przy wydawaniu dokumentów pobytowych, przy zatrzymywaniu migrantów w nielegalnej sytuacji, podczas procedury powrotowej i do celów wydawania zakazów wjazdu. Ustanowione przez UE systemy informatyczne, w tym systemy początkowo stworzone do celów azylowych i zarządzania migracją, są coraz częściej wykorzystywane w kontekście bezpieczeństwa wewnętrznego, np. podczas rewizji policyjnych i w zwalczaniu poważnych przestępstw i terroryzmu.

Tabela 6: Wybrane instrumenty UE wymagające przetwarzania dużych ilości danych do celów zarządzania granicami i ścigania przestępstw

Baza danych	Skrót	Główny cel
System informacyjny Schengen	*SIS II*	Wprowadzanie i przetwarzanie wpisów dotyczących poszukiwanych lub zaginionych osób do celów utrzymania bezpieczeństwa, wprowadzanie i przetwarzanie wpisów dotyczących obywateli państw trzecich do celów odmowy przekroczenia granicy lub pozostania w państwie oraz wprowadzanie i przetwarzanie wpisów dotyczących obywateli państw trzecich podlegających decyzji nakazującej powrót.
Wizowy system informacyjny	*VIS*	Ułatwianie wymiany danych dotyczących wniosków wizowych między państwami członkowskimi należącymi do strefy Schengen.
Europejski zautomatyzowany system identyfikacji odcisków palców	*EURODAC*	Określenie państwa członkowskiego odpowiedzialnego za zbadanie wniosku o przyznanie ochrony międzynarodowej i pomoc w kontroli nielegalnej imigracji i wtórnych przepływów.
System wjazdu/wyjazdu	*EES*	Obliczanie i monitorowanie okresu uprawnionego pobytu obywateli państw trzecich i identyfikacja osób przekraczających dozwolony okres pobytu.
Dane dotyczące przelotu pasażera	*PNR*	Gromadzenie, przetwarzanie i wymiana danych dotyczących pasażerów lotów pozaunijnych w przypadku lotów z państw trzecich („loty pozaunijne")*. Ściśle mówiąc, wykorzystywane wyłącznie do celów ścigania przestępstw.
Dane pasażera przekazywane przed podróżą	*API*	Gromadzenie i przetwarzanie danych pasażerów lotów z państw trzecich („lotów pozaunijnych") do celów zarządzania granicami i ścigania przestępstw.
Europejski system informacji o podróży oraz zezwoleń na podróż	*ETIAS*	Ocena, czy obywatele państw trzecich zwolnieni z obowiązku wizowego stwarzają ryzyko dla bezpieczeństwa, ryzyko nielegalnej imigracji lub ryzyko dla zdrowia publicznego.
Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich	*ECRIS-TCN*	Wymiana informacji na temat wcześniejszych wyroków skazujących w odniesieniu do obywateli państw trzecich.

*Uwaga: * Dodatkowo art. 2 dyrektywy (UE) 2016/681 daje państwom członkowskim możliwość przetwarzania danych z lotów wewnątrzunijnych.*

Źródło: FRA, 2018.

Większość systemów ustanowionych przepisami UE skupia się na identyfikacji konkretnych osób poprzez łączenie danych alfanumerycznych i biometrycznych (obecnie odcisków palców) z informacjami znajdującymi się już w systemie. Poza kilkoma wyraźnymi wyjątkami (zob. „Koncentracja na profilowaniu z wykorzystaniem algorytmu w instrumentach UE"), nie zawierają one algorytmu, który umożliwiłby połączenie osoby z profilem. Mogą jednak być wykorzystywane do tworzenia zanonimizowanych statystyk, w tym dotyczących cech uznanych za cechy chronione, takich jak płeć czy wiek (zob. sekcja 1.2.1).

Statystyki takie mogłyby być wykorzystane do utworzenia profili ryzyka stosowanych w przyszłości do celów zarządzania granicami lub podejmowania decyzji odnośnie do działań policji. Jako część większego systemu na rzecz interoperacyjności unijnych systemów informatycznych Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) będzie odpowiedzialna za zarządzanie centralnym repozytorium sprawozdawczo-statystycznym. Repozytorium to będzie bazowało na danych z istniejących baz danych UE (systemu wjazdu/wyjazdu, ETIAS, systemu informacyjnego Schengen i wizowego systemu informacyjnego) w celu tworzenia statystyk i raportów analitycznych dla unijnych i krajowych podmiotów[43].

43 Komisja Europejska (2017), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniającego decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226, COM(2017) 793 final, Strasburg, dnia 12 grudnia 2017 r.; Komisja Europejska (2017), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja), COM(2017) 794 final, Bruksela, dnia 12 grudnia 2017 r.

Koncentracja na profilowaniu z wykorzystaniem algorytmu w instrumentach UE

Niektóre istniejące instrumenty UE przewidują wykorzystywanie statystyk utworzonych na podstawie ich danych do celów tworzenia profili ryzyka. Poza umożliwianiem zatrzymania konkretnych „znanych" podejrzanych zawierają one funkcję profilowania z wykorzystaniem algorytmu, która pozwala na identyfikację „nieznanych" osób, które mogą być przedmiotem zainteresowania organów ścigania i organów zarządzania granicami.

Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) [44], przyjęty we wrześniu 2018 r., ale w momencie ukończenia niniejszego przewodnika jeszcze niedziałający, będzie umożliwiał ocenę, czy obywatele państw trzecich zwolnieni z obowiązku wizowego stwarzają ryzyko nielegalnej imigracji, ryzyko dla bezpieczeństwa lub ryzyko dla zdrowia publicznego, przed przyznaniem zezwolenia na podróż. Informacje przedstawione przez podróżnych podczas procesu składania wniosku będą automatycznie porównywane ze stosownymi unijnymi i międzynarodowymi bazami danych oraz z zestawem wskaźników ryzyka („regułami kontroli przesiewowej") zawartymi w samym systemie ETIAS. Algorytm opracowany przez Frontex porówna dany profil podróżnego (w oparciu o takie wskaźniki, jak wiek, płeć, narodowość, miejsce pobytu, poziom wykształcenia i zawód) ze wskaźnikami ryzyka, aby określić, czy wniosek należy skierować do ręcznego przeglądu.

Przewoźnicy lotniczy gromadzą **dane dotyczące przelotu pasażera (PNR)** z informacji dostarczanych przez pasażerów w systemach rezerwacji lotów, takich jak daty podróży i trasa, szczegółowe dane kontaktowe i dotyczące płatności, informacja o bagażu i inne „uwagi ogólne", takie jak preferencje żywieniowe. Nie istnieje żadna centralna baza danych UE gromadząca takie dane, w dyrektywie UE w sprawie danych PNR[45] wymaga się jednak, aby przewoźnicy lotniczy przekazywali dane do krajowej jednostki do spraw

44 Komisja Europejska (2018), art. 33 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniającego rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, COM(2016) 731 final, Bruksela, dnia 16 listopada 2016 r.

45 Artykuł 6 ust. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119.

informacji o pasażerach (JIP), która następnie dokona analizy informacji do celów zwalczania terroryzmu i poważnej przestępczości. Poza wykrywaniem transgranicznego przemieszczania się znanych osób, dane te można wykorzystać do identyfikacji nieznanych jeszcze zagrożeń, przetwarzając dane pasażerów względem określonych wskaźników ryzyka („określonych wcześniej kryteriów"). Kryteria te są określane przez JIP i aktualizowane na podstawie nowych danych i dostępnych w systemie wzorców.

3.2.1. Minimalizowanie zagrożenia dla praw podstawowych podczas przetwarzania danych w wielkoskalowych bazach danych

Kompleksowe dane na temat podróżnych, takie jak narodowość, płeć i wiek, będą wykorzystywane do profilowania, w tym profilowania z wykorzystaniem algorytmu, na dużą skalę, co w przeszłości nie było możliwe. Nawet w przypadku anonimizacji tych danych ich przetwarzanie stwarza pewne ryzyko. Świadome lub nieświadome uprzedzenia w wyborze wskaźników ryzyka, opracowywanie algorytmów lub interpretacja wyników mogą prowadzić do działań operacyjnych, które będą dyskryminacyjne względem niektórych kategorii osób[46].

W niniejszej sekcji przyjrzano się niektórym z tych zagrożeń i zaproponowano pewne sposoby na ich zminimalizowanie. Opiera się ona na *dwunastu czynnikach operacyjnych w dziedzinie poszanowania praw podstawowych na potrzeby ścigania w kontekście przetwarzania danych PNR* sformułowanych przez FRA (zob. analiza przykładów). Chociaż czynniki te opracowano w określonym kontekście przetwarzania danych PNR, niektóre z nich można zastosować w bardziej ogólnym kontekście i można je uznać za zabezpieczenia ograniczające zagrożenia wynikające z profilowania z wykorzystaniem algorytmu.

Analiza przykładów

Wytyczne operacyjne FRA dotyczące ustanawiania krajowych systemów danych PNR

W 2014 r., z uwagi na brak przepisów unijnych regulujących kwestię danych PNR, Komisja Europejska zwróciła się do FRA o opracowanie praktycznych wytycznych dotyczących przetwarzania danych PNR do celów ścigania przestępstw dla

46 Aby uzyskać więcej informacji, zob. FRA (2017e) i FRA (2018a).

państw członkowskich, które planują ustanowić własne krajowe systemy danych PNR. W wytycznych skupiono się na prawie do poszanowania życia prywatnego (art. 7 Karty), ochronie danych osobowych (art. 8 Karty) i niedyskryminacji (art. 21 Karty). Niektóre z zaproponowanych zabezpieczeń wprowadzono następnie w dyrektywie UE w sprawie danych PNR.

Dwanaście czynników w dziedzinie poszanowania praw podstawowych na potrzeby ścigania w kontekście przetwarzania danych PNR brzmi następująco:

- dane PNR należy wykorzystywać wyłącznie do zwalczania terroryzmu i poważnych przestępstw transgranicznych;
- należy ograniczyć dostęp do bazy danych PNR do wyspecjalizowanych jednostek;
- nie należy żądać bezpośredniego dostępu do baz danych linii lotniczych;
- należy usuwać wrażliwe dane PNR;
- należy ustanowić ścisłe zabezpieczenia przeciwko nadużyciom, zapewniające bezpieczeństwo i identyfikowalność;
- należy ograniczyć prawdopodobieństwo oznaczania wyników fałszywie dodatnich;
- należy zachować przejrzystość względem pasażerów;
- należy umożliwić osobom dostęp do ich danych PNR i ich sprostowanie;
- nie należy zezwalać na identyfikację osób, których dane dotyczą, lub przechowywanie danych przez dłuższy okres, niż jest to konieczne;
- należy przekazywać dane z systemu danych PNR wyłącznie uprawnionym do tego krajowym organom publicznym;
- przekazywanie danych z systemu danych PNR do państw trzecich możliwe jest wyłącznie na restrykcyjnych warunkach;
- należy prowadzić obiektywną i przejrzystą ocenę systemu danych PNR.

Aby uzyskać więcej informacji, zob. FRA (2014c).

Przetwarzanie danych ujawniających cechy chronione powinno być konieczne i proporcjonalne

Ze względu na charakter profilowania z wykorzystaniem algorytmu wykorzystywanie cech osobowych związanych z cechami chronionymi pociąga za sobą szczególnie duże ryzyko dyskryminacji[47]. W kontekście UE zarówno przepisy w sprawie ETIAS, jak i w sprawie danych PNR zabraniają, aby wskaźniki ryzyka opierały się na kryteriach pociągających za sobą duże ryzyko dyskryminacji, w tym na rasie, pochodzeniu etnicznym czy przekonaniach religijnych. Nawet w przypadku braku takich danych inne rodzaje danych mogą być jednak silnie skorelowane z tymi cechami i działać w rezultacie jako zamienniki takich cech chronionych. Na przykład kategoria „uwagi ogólne" w danych PNR mogąca zawierać preferencje żywieniowe podróżnych, może ujawnić niektóre przekonania religijne.

Konkretna kombinacja danych wykorzystywanych w algorytmie może również sprawić, że pewna kategoria osób będzie postawiona w niekorzystnej sytuacji. Może na przykład postawić w niekorzystnej sytuacji osoby ze względu na ich pochodzenie etniczne lub społeczne lub bycie członkiem mniejszości narodowej, które to cechy są cechami chronionymi na podstawie art. 21 Karty. Na przykład jeżeli profil ryzyka w ETIAS dotyczący ryzyka nielegalnej migracji opiera się na połączeniu pewnej narodowości z pewną grupą zawodową, może prowadzić do ukierunkowania profilu na grupę etniczną lub narodowość, która w danym państwie pracuje zazwyczaj w konkretnym sektorze gospodarczym, np. w budownictwie lub w rolnictwie[48].

- Przetwarzanie danych ujawniających cechy chronione art. 21 Karty powinno ograniczać się do tego, co absolutnie konieczne i proporcjonalne, i nigdy nie powinno skutkować dyskryminacją. Przed jakimkolwiek przetwarzaniem właściwy organ powinien ocenić dane w celu określenia jakichkolwiek chronionych cech i usunięcia wszelkich danych, których przetwarzanie byłoby niezgodne z prawem. W ramach dobrej praktyki należałoby uzupełnić tę czynność, stosując program służący łączeniu i usuwaniu danych zaopatrzony w regularnie aktualizowany glosariusz „terminów wrażliwych".

47 Europejski Inspektor Ochrony Danych (2018).

48 Zob. również FRA (2017a).

Kryteria profilowania powinny być konkretne i ukierunkowane

Kolejne zagrożenie wynika z wykorzystywania **szerokich kryteriów profilowania**. Istniejące instrumenty UE umożliwiają znaczny stopień uznania w odniesieniu do opracowywania algorytmów na potrzeby profilowania. Aby ocenić ryzyko nielegalnej migracji, w systemie ETIAS przewiduje się korzystanie z unijnych i krajowych statystyk na temat wskaźnika przypadków przekroczenia dozwolonego okresu pobytu i odmowy wjazdu. W odniesieniu do ryzyka związanego z bezpieczeństwem informacji odnosi się to wyłącznie ogólnie do informacji dotyczących konkretnych wskaźników bezpieczeństwa i zagrożeń. W dyrektywie w sprawie danych PNR znajdują się wyłącznie ogólne odniesienia do opracowywania algorytmów, nie określono jednak, jakie kryteria można zastosować w celu identyfikacji osób potencjalnie zaangażowanych w przestępstwa o charakterze terrorystycznym lub poważne przestępstwa, ani jaką wagę należy przypisać poszczególnym kryteriom.

Zbyt szerokie kryteria skutkują znaczną liczbą wyników „fałszywie dodatnich", co oznacza błędne dopasowanie osób do określonego profilu ryzyka. Niektóre z tych „fałszywie dodatnich" wyników mogą nieć również charakter dyskryminacyjny. Na przykład szeroka definicja kryterium „wcześniejsze wyroki skazujące" oznacza, że osoby LGBT byłyby zobowiązane do zgłoszenia uprzedniej karalności związanej z niektórymi zachowaniami seksualnymi podlegającymi penalizacji w niektórych państwach spoza UE.

- Kryteria oceny powinny być wcześniej zdefiniowane, ukierunkowane, konkretne, proporcjonalne i oparte na faktach. Kryteria oceny należy poddać testom na zanonimizowanych próbach. Powinny one podlegać regularnym przeglądom prowadzonym przez audytorów wewnętrznych w celu ustalenia, czy wciąż są uzasadnione określonymi celami.

- Przed przekazaniem na potrzeby dalszych działań wpisu opartego na zautomatyzowanym przetwarzaniu właściwy organ powinien dokonać ręcznego przeglądu danych w połączeniu z innymi informacjami, aby ustalić, czy osoba pasuje do profilu ryzyka i wyeliminować wynik fałszywie dodatni. Podmioty otrzymujące dane powinny przedstawić informacje zwrotne dotyczące działań podjętych na podstawie wpisu.

Przetwarzane dane powinny być dokładne i rzetelne

Zgodnie z badaniem FRA istniejące wielkoskalowe systemy informatyczne zawierają znaczne ilości niedokładnych danych[49]. **Niedokładne lub nierzetelne dane** mogą wywrzeć liczne negatywne skutki w kontekście profilowania z wykorzystaniem algorytmu do celów zarządzania granicami i ścigania przestępstw. Niedokładne dane mogą mieć niekorzystny wpływ na jednostki, mogą jednak również skutkować powstaniem nieprawidłowych korelacji i zaburzonego obrazu, narażając skuteczność pracy policji i organów zarządzających granicami.

Jest to szczególnie istotne w przypadkach, gdy dane wprowadzane są przez członków społeczeństwa, np. danych PNR i danych w aplikacjach ETIAS, które mogą być bardziej podatne na błędy niż oficjalne rejestry. Podobnie, kontrola kont w mediach społecznościowych przewidziana w niektórych systemach autoryzacji podróży poza UE niesie ze sobą duże ryzyko wprowadzenia do procesu profilowania nierzetelnych informacji. Ponadto wiąże się z nią szczególne ryzyko gromadzenia informacji ujawniających wrażliwe dane osobowe chronione na podstawie Karty, takie jak poglądy polityczne lub informacje związane z życiem seksualnym.

- Należy dostarczać osobom dokładnych informacji na temat gromadzenia, przechowywania i przetwarzania ich danych oraz na temat stosowania zasad ochrony danych. Należy uświadamiać osobom ich prawa, w tym dostępność mechanizmów zaskarżania.

- Należy umożliwić osobom sprostowanie ich danych, gdy są one niedokładne, i informować je co do tego, czy dane zostały sprostowane lub usunięte.

- Należy zapewnić skuteczne administracyjne i sądowe środki zaskarżania na wypadek naruszenia jakichkolwiek praw w zakresie ochrony danych, w tym na wypadek odmowy dostępu do danych lub braku sprostowania lub usunięcia niedokładnych danych.

49 Zob. FRA (2018c), s. 81–98.

Wniosek

Przedstawiciele organów ścigania i straż graniczna korzystają z profilowania zgodnie z prawem w celu zapobiegania przestępstwom, badania i ścigania działalności przestępczej oraz w celu zapobiegania nielegalnej imigracji.

Aby profilowanie było legalne, sprawiedliwe i skuteczne, musi być stosowane w granicach prawa. W szczególności przy profilowaniu należy przestrzegać wymogów równego traktowania i ochrony danych osobowych.

Można to osiągnąć poprzez połączenie pewnych elementów. Stosując jakiekolwiek profilowanie, należy:

- traktować osoby równo, z szacunkiem i godnością;
- unikać profilowania osób na podstawie uprzedzeń;
- postępować rozsądnie, obiektywnie i w oparciu o dane wywiadowcze; oraz
- zapewnić odpowiednią ochronę danych osobowych i życia prywatnego jednostek.

Funkcjonariusze policji i straż graniczna mają dostęp do różnych narzędzi służących zapewnieniu, aby zasady te były im znane, zrozumiałe i przestrzegane w praktyce:

- przed przystąpieniem do profilowania funkcjonariusze powinni otrzymać wytyczne i odbyć szkolenie;
- podczas profilowania należy rejestrować i przechowywać szczegółowe dane dotyczące działania;
- po zakończeniu profilowania funkcjonariusze powinni być poddani monitorowaniu i ocenie, aby zidentyfikować obszary wymagające poprawy.

Zapobieganie niezgodnemu z prawem profilowaniu nie tylko utrzyma działania funkcjonariuszy organów ścigania i straży granicznej w granicach prawa, lecz również zapewni ich rozumienie i akceptowanie przez ogół społeczeństwa. Budowanie zaufania do organów ścigania i organów zarządzania granicami przyczynia się do poprawy skuteczności działań policji i zarządzania granicami, a zatem również do większego poziomu bezpieczeństwa i ochrony w społeczeństwie jako całości.

Załącznik

Tabela 7: Istniejące lub planowane wielkoskalowe unijne systemy informatyczne

System informatyczny	Główny cel	Osoby objęte systemem	Stosowanie	Instrument prawny/wniosek	Identyfikatory biometryczne
System Eurodac	Ustalenie państwa członkowskiego odpowiedzialnego za zbadanie wniosku o udzielenie ochrony międzynarodowej *Pomoc w kontroli nielegalnej imigracji i wtórnych przepływów*	Wnioskodawcy ubiegający się o przyznanie ochrony międzynarodowej i beneficjenci takiej ochrony, *Nielegalni migranci*	28 PCUE+ SAC	Rozporządzenie (UE) nr 603/2013 (rozporządzenie w sprawie Eurodac) *COM(2016) 272 final (wniosek w sprawie Eurodac)*	
Wizowy system informacyjny (VIS)	Ułatwianie wymiany danych dotyczących wniosków wizowych między państwami członkowskimi należącymi do strefy Schengen	Osoby ubiegające się o wizę i członkowie rodziny rozdzielonej	24 PCUE (oprócz CY, HR, IE, UK)[1] + SAC	Rozporządzenie (WE) nr 767/2008 (rozporządzenie w sprawie systemu VIS)	
System informacyjny Schengen (SIS II) – policja	Ochrona bezpieczeństwa w UE i w państwach członkowskich należących do strefy Schengen	Osoby zaginione lub poszukiwane	26 PCUE (oprócz CY, IE)[2] + SAC	Decyzja Rady 2007/533/WSiSW (decyzja w sprawie SIS II) *COM(2016) 883 final (wniosek w sprawie SIS II policja)*	
System informacyjny Schengen (SIS II) – granice	Wprowadzanie i przetwarzanie wpisów do celów odmowy wjazdu do państwa członkowskiego należącego do strefy Schengen lub pozostania w takim państwie	Nielegalni migranci	25 PCUE (oprócz CY, IE, UK)[2] + SAC	Rozporządzenie (WE) nr 1987/2006 (rozporządzenie w sprawie SIS II) *COM(2016) 882 final (wniosek w sprawie SIS II granice)*	
System informacyjny Schengen (SIS II) – powroty	*Wprowadzanie i przetwarzanie wpisów dotyczących obywateli państw trzecich podlegających decyzji nakazującej powrót*	*Nielegalni migranci*	*25 PCUE (oprócz CY, IE, UK)[2] + SAC*	*COM(2016) 881 final (wniosek w sprawie SIS II powroty)*	

System wjazdu-wyjazdu (EES)	*Obliczanie i monitorowanie okresu uprawnionego pobytu obywateli państw trzecich i identyfikacja osób przekraczających dozwolony okres pobytu*	*Podróżni przybywający na pobyt krótkoterminowy*	*22 PCUE (oprócz BG, CY, HR, IE, RO, UK)[3] + SAC*	*Rozporządzenie (UE) 2017/2226 (rozporządzenie w sprawie EES)*	
Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)	*Ocena, czy obywatele państw trzecich zwolnieni z obowiązku wizowego stwarzają ryzyko dla bezpieczeństwa, ryzyko nielegalnej imigracji lub ryzyko dla zdrowia publicznego*	*Podróżni zwolnieni z obowiązku wizowego*	*26 PCUE (oprócz IE, UK)3 + SAC*	*COM(2016) 731 final (wniosek w sprawie ETIAS)*	*Brak*
Europejski system przekazywania informacji z rejestrów karnych na temat obywateli państw trzecich (ECRIS-TCN)	*Wymiana informacji na temat wcześniejszych wyroków skazujących w odniesieniu do obywateli państw trzecich*	*Obywatele państw trzecich z wcześniejszymi wyrokami skazującymi*	*27 PCUE (oprócz DK)4*	*COM(2017) 344 final (wniosek w sprawie ECRIS- ETIAS)*	
Interoperacyjność – Wspólne repozytorium danych umożliwiających identyfikację	*Ustanowienie ram interoperacyjności między EES, VIS, ETIAS, Eurodac, SIS II i ECRIS-TCN*	*Obywatele państw trzecich podlegający Eurodac, VIS, SIS II, EES, ETIAS i ECRIS-TCN*	*28 PCUE5 + SAC*	*COM(2017) 793 final (wniosek w sprawie granic i interoperacyjności)* *COM(2017) 794 final (wniosek w sprawie współpracy policyjnej, azylu i migracji)*	

Uwaga: *Planowane systemy i planowane zmiany w systemach zaznaczono kursywą.*
Odciski palców; *Odciski dłoni;* *Wizerunki twarzy;* *Profil DNA.*
PCUE: państwa członkowskie UE.SAC: państwa stowarzyszone w ramach Schengen, tj. Islandia, Liechtenstein, Norwegia i Szwajcaria.

1 *Irlandia i Zjednoczone Królestwo nie uczestniczą w systemie VIS. Dania nie podlega rozporządzeniu, ale uczestniczy w systemie VIS. VIS nie stosuje się jeszcze w Chorwacji i na Cyprze, a w Bułgarii i Rumunii jest on stosowany tylko częściowo zgodnie z decyzją Rady (UE) 2017/1908 z dnia 12 października 2017 r.*

2 *Cypr i Irlandia nie są jeszcze podłączone do SIS. Dania nie podlega rozporządzeniu ani decyzji Rady, ale uczestniczy w SIS II i musi podjąć decyzję co do ponownego uczestnictwa przed przyjęciem wniosku w sprawie SIS II. Zjednoczone Królestwo uczestniczy w SIS II, nie może jednak korzystać z wpisów ani uzyskać do nich dostępu w celu odmowy wstępu na obszar strefy Schengen lub pozostania w tym obszarze. Bułgaria, Rumunia i Chorwacja nie mogą wydawać wpisów dotyczących całej strefy Schengen w sprawie odmowy wjazdu na obszar strefy lub pozostania w tym obszarze, gdyż nie należą jeszcze do strefy Schengen.*

3 *Dania może podjąć decyzję co do uczestnictwa w EES i ETIAS.*

4 *ECRIS-TCN nie ma zastosowania do Danii. Zjednoczone Królestwo i Irlandia mogą podjąć decyzję co do uczestnictwa.*

5 *Dania, Irlandia i Zjednoczone Królestwo będą brały udział, gdyż uczestniczą w nadawaniu interoperacyjności systemom IT.*

Źródło: *FRA, na podstawie istniejących i proponowanych instrumentów prawnych, 2018.*

Źródła

Akhgar, B., Saathoff, G.B., Arabnia, H.R., Hill, R., Staniforth, A. i 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 stycznia 2016 r.

Belgia, Unia, *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Bruksela, 2015.

Belgia, Unia, *Sprawozdanie roczne 2016*, Bruksela, wrzesień 2017.

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

Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka (OHCHR) (2014), *Recommended Principles and Guidelines on Human Rights at International Borders*, 23 lipca 2014 r.

Body-Gendrot, S. (2016), „Making sense of French urban disorders in 2005", *European Journal of Criminology*, t. 13, nr 5, s. 556–572.

Bovens i in. (2014), „Public accountability" w: Bovens, M., Schillermans, T. i Goodlin, R.E. (red.), *The Oxford handbook of public accountability*, Oksford, Oxford University Press, 2014.

Brayne, S. (2014), „Surveillance and system avoidance: criminal justice contact and institutional attachment", *American Sociological Review*, t. 79, nr 3, s. 367–391.

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

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

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

Coudert, F., Butin, D. i Le Metayer, D. (2015), „Body-worn cameras for police accountability: opportunities and risks", *Computer Law and Security Review*, t. 31, s. 749–762.

De Hert, P. i Lammerant, H. (2016), „Predictive profiling and its legal limits: effectiveness gone forever?" w: van der Sloot, B., Broeders, D. i Schrijvers, E. (red.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, s. 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. i 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, s. 3.

Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) (2012), *Common core curriculum, EU border guard basic training*, marzec 2012 r.

Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) (2015), *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Europejska Komisja przeciwko Rasizmowi i Nietolerancji (ECRI) (2007), *Zalecenie nr 11 dotyczące polityki ogólnej ECRI: zwalczanie rasizmu i dyskryminacji rasowej w działalności policji* przyjęte 29 czerwca 2007 r., Strasburg, 4 października 2007 r.

Europejska sieć ekspertów prawnych w dziedzinie równouprawnienia płci i niedyskryminacji (2016), *Links between migration and discrimination - A legal analysis of the situation in EU Member States*, lipiec 2016 r.

Europejski Inspektor Ochrony Danych (EIOD) (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, Opinia 5/2015, Bruksela, 24 września 2015 r.

Europejski Inspektor Ochrony Danych (EIOD) (2018), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Bruksela, 18 kwietnia 2018 r.

Europejskie Centrum Monitorowania Rasizmu i Ksenofobii (2016), *Perceptions of discrimination and islamophobia – Voices from members of Muslim communities in the European Union*, 2006.

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 (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Luksemburg, Urząd Publikacji, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luksemburg, Urząd Publikacji, 2014.

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

FRA (2016), *Fundamental Rights Report 2016*, Luksemburg, Urząd Publikacji, 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)*, Opinia FRA – 2/2017 [ETIAS], czerwiec 2017 r.

FRA (2017b), *Second European Union Minorities and Discrimination Survey — Main results*, Luksemburg, Urząd Publikacji, grudzień 2017 r.

FRA (2017c), *Fundamental Rights Report 2017*, Luksemburg, Urząd Publikacji, maj 2017 r.

FRA (2017d), *Second European Union Minorities and Discrimination Survey Muslims – Selected findings*, Luksemburg, Urząd Publikacji, 2017.

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luksemburg, Urząd Publikacji, maj 2017 r.

FRA (2018a), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, Opinia FRA – 1/2018 [Interoperacyjność], kwiecień 2018 r.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, FRA Focus Paper, maj 2018 r.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luksemburg, Urząd Publikacji, luty 2018 r.

FRA (2018d), *Hate crime recording and data collection practice across the EU,* Luksemburg, Urząd Publikacji, czerwiec 2018 r.

FRA (2018e), *Fundamental Rights Report 2018*, Luksemburg, Urząd Publikacji, czerwiec 2018 r.

FRA (Agencja Praw Podstawowych Unii Europejskiej) (2013), *Szkolenie policji z zakresu praw podstawowych – Podręcznik dla osób prowadzących szkolenia dla policji*, Luksemburg, Urząd Publikacji, grudzień 2013 r.

FRA (Agencja Praw Podstawowych Unii Europejskiej), Europejski Inspektor Ochrony Danych (EIOD) i Rada Europy (2018), *Handbook on European data protection law – Edition 2018*, Luksemburg, Urząd Publikacji, maj 2018 r.

FRA i Rada Europy (2018), *Handbook on European non-discrimination law – 2018 edition*, Luksemburg, Urząd Publikacji, luty 2018 r.

Francja, Ministerstwo spraw wewnętrznych (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 czerwca 2018 r.

Gandy, O. (2010), „Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems', *J Ethics Inf Technol*, t. 12, nr 1, s. 29–42, 2010.

Gross, S.R. (2002), „Racial Profiling under Attack", D. Livingston, współautor. *Colum.* L Rev. 102, nr 5, s. 1413–1438.

Grupa Robocza Art. 29 (2014), *Opinia 01/2014 w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa*, 536/14/PL, WP 211, Bruksela, 27 lutego 2014 r.

Grupa Robocza Art. 29 (2017a), *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, WP 248 rev.01, 4 października 2017 r.

Grupa Robocza Art. 29 (2017b), *Opinia dotycząca niektórych głównych zagadnień dyrektywy (UE) 2016/680 dotyczącej policji [(UE) 2016/680)]*, 7 grudnia 2017 r.

Grupa Robocza Art. 29 (2018a), *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia (UE) 2016/679/UE*, WP251rev.01, 6 lutego 2018 r.

Grupa Robocza Art. 29 (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Bruksela, 23 kwietnia 2018 r.

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*, t. 71, 2004.

Harris, D. (2002), „Flying While Arab: Lessons from the Racial Profiling Controversy", *Civil Rights Journal*, t. 6, nr 1, zima 2002 r.

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

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

Hildebrandt, M. i Gutwirth, S. (red.) (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*, t. 13, nr 5, s. 573–589.

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

Jobard, F. (2008), „The 2005 French urban unrests: data-based interpretations", *Sociology Compass*, t 2, nr 4, s. 1287–1302.

Kádár, A., Körner, J., Moldova, Z., i Tóth, B. (2008), *ProjectControl(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS)*, Budapeszt, s. 23.

Keskinen, S. i in. (2018), *The Stopped – Ethnic Profiling in Finland*, Swedish School of Social Science, Uniwersytet Helsiński, Helsinki, 3 kwietnia 2018 r.

Komisja Europejska (2017a), *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, luty 2017 r.

Komisja Europejska (2017b), *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, grudzień 2017 r.

Komisja Europejska, podgrupa ds. metod rejestrowania i gromadzenia danych o przestępstwach z nienawiści (2017), *Improving the recording of hate crime by law enforcement authorities - Key guiding principles*, Bruksela, grudzień 2017 r.

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

Miller, J. i 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. i Floridi, L. (2016), „The ethics of algorithms: Mapping the debate", *Big Data & Society*, 1 grudnia 2016 r.

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

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

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

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

Organizacja Narodów Zjednoczonych (ONZ) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29 stycznia 2007 r.

Oswald, M., Grace, J., Urwin, S. i Barnes, G., „Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality", *Information & Communications Technology Law*, 31 sierpnia 2017 r.

Rada Europy, Komitet Ministrów (2001), Zalecenie Rec(2001) 10 Komitetu Ministrów dla państw członkowskich dotyczące Europejskiego Kodeksu Etyki Zawodowej Policji przyjęte przez Komitet Ministrów, 19 września 2001 r.

Rada Unii Europejskiej (2009), *Zaktualizowany Schengeński schengeński katalog UE „Kontrola na granicach zewnętrznych powroty i readmisja"*, 19 marca 2009 r.

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

Scheinin, M. (2007), Specjalny sprawozdawca ONZ ds. praw człowieka i walki z terroryzmem, *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/26, 29 stycznia 2007 r.

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

Tóth, B.M. i Kádár, A. (2011), „Ethnic profiling in ID checks by the Hungarian police", *Policing and Society*, t. 21, nr 4, s. 383–394.

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, marzec 2000 r.

Van Brakel, R. (2016), „Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing" w: van der Sloot, B., Broeders, D. i Schrijvers, E. (red.), The Netherlands Scientific Council for Government Policy

(*Wetenschappelijke Raad voor het Regeringsbeleid*), *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, s. 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*, t. 11, nr 2, s. 285–330.

Zjednoczone Królestwo, Camden and London Prepared (2006), *Major Incident Procedures, What businesses and the voluntary sector need to know*, kwiecień 2006 r.

Zjednoczone Królestwo, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29 września 2016 r.

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

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

Zjednoczone Królestwo, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, luty 2016 r.

Zjednoczone Królestwo, Home Office (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, luty 1999 r.

Zjednoczone Królestwo, 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.

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

Zjednoczone Królestwo, House of Commons Home Affairs Committee (2009), *The Macpherson Report – Ten Years On,* Twelfth Report of Session 2008–09, 22 lipca 2009 r.

Zjednoczone Królestwo, Izba Lordów (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents)*, [2006] UKHL 12, 8 marca 2006 r.

Zjednoczone Królestwo, London School of Economics (2011), *Reading the Riots*, grudzień 2011 r.

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

Zjednoczone Królestwo, Northamptonshire Police (2018), *Get Involved – Reasonable Grounds Panel*, dostęp: kwiecień 2018 r.

Zjednoczone Królestwo, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), *An Independent Report into Stop & Search Encounters by Staffordshire Police,* styczeń 2015 r.

Zjednoczone Królestwo, Stop Watch (2011), *„Carry on Recording" Why police stops should still be recorded*, maj 2011 r.

Zjednoczone Królestwo, West Midlands Police (2012), *Stop and Search Policy*, listopad 2012 r.

Zjednoczone Królestwo, West Midlands Police (2016), *Stop and Search Recommendations,* lipiec 2015 r. (ostatnia aktualizacja: czerwiec 2016 r.).

Zjednoczone Królestwo, West Midlands Police (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, kwiecień 2017 r.

Zjednoczone Królestwo, West Midlands Police (2017b), *New "app" set to speed up Stop & Search process*, sierpień 2017 r.

Zjednoczone Królestwo, West Midlands Police (2018), *Stop and Search Scrutiny Panels*, dostęp: kwiecień 2018 r.

Zjednoczone Królestwo, West Midlands Police and Crime Commissioner (2014), *Stop and Search Action Plan – Outcome of consultation*, styczeń 2014 r.

Prawodawstwo UE

Prawa podstawowe

Karta praw podstawowych Unii Europejskiej, 2012/C 326/02, Dz.U. C 326 z 2012, s. 1.

Wyjaśnienia dotyczące Karty praw podstawowych, 2007/C 303/02, Dz.U. C 303 z 2007, s. 17.

Niedyskryminacja

Dyrektywa Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzająca w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne.

Dyrektywa Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy.

Ochrona danych

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Zarządzanie granicami

Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 205 z 2007, s. 63.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119 z 2017, s. 132.

Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 381 z 2006, s. 4.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz.U. L 2018 z 2008, s. 60.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.U. L 180 z 2013, s. 1.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE, Dz.U. L 251 z 2016, s. 1.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiające europejski system nadzorowania granic (EUROSUR), Dz.U. L 295 z 2013, s. 11.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen), Dz.U. L 77 z 2016, s. 1.

Orzecznictwo

Francja, *Cour de Cassation*, *Décision 1245*, 9 listopada 2016 r.

Zjednoczone Królestwo, Izba Lordów, *R (on the application of Gillan et al.) przeciwko Commissioner of Police for the Metropolis et al.* [2006] UKHL 12, 8 marca 2006 r.

TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland*, 16 grudnia 2008 r.

ETPC, *B.S. przeciwko Hiszpanii*, nr 47159/08, 24 lipca 2012 r.

ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu,* nr 30562/04 i 30566/04, 4 grudnia 2008 r.

ETPC, *Gillan i Quinton przeciwko Zjednoczonemu Królestwu*, nr 4158/05 2010, 12 stycznia 2010 r.

UNHRC, *Rosalind Williams Lecraft przeciwko Hiszpanii*, Comm. nr 1493/2006, 30 lipca 2009 r.

Jak skontaktować się z UE

Osobiście

W całej Unii Europejskiej istnieje kilkaset centrów informacyjnych Europe Direct. Adres najbliższego centrum można znaleźć na stronie: https://europa.eu/european-union/contact_pl.

Telefonicznie lub drogą mailową

Europe Direct to serwis informacyjny, który udziela odpowiedzi na pytania na temat Unii Europejskiej. Można się z nim skontaktować:

— dzwoniąc pod bezpłatny numer telefonu: 00 800 6 7 8 9 10 11 (niektórzy operatorzy mogą naliczać opłaty za te połączenia),
— dzwoniąc pod standardowy numer telefonu: +32 22999696,
— drogą mailową: https://europa.eu/european-union/contact_pl.

Wyszukiwanie informacji o UE

Internet

Informacje o Unii Europejskiej są dostępne we wszystkich językach urzędowych UE w portalu Europa: https://europa.eu/european-union/index_pl.

Publikacje UE

Bezpłatne i odpłatne publikacje UE można pobrać lub zamówić na stronie: https://publications.europa.eu/pl/publications. Większą liczbę egzemplarzy bezpłatnych publikacji można otrzymać, kontaktując się z serwisem Europe Direct lub z lokalnym centrum informacyjnym (zob. https://europa.eu/european-union/contact_pl).

Prawo UE i powiązane dokumenty

Informacje prawne dotyczące UE, w tym wszystkie unijne akty prawne od 1952 r., są dostępne we wszystkich językach urzędowych UE w portalu EUR-Lex: http://eur-lex.europa.eu.

Portal Otwartych Danych UE

Unijny portal otwartych danych (http://data.europa.eu/euodp/pl) umożliwia dostęp do zbiorów danych pochodzących z instytucji i innych organów UE. Dane można pobierać i wykorzystywać bezpłatnie, zarówno do celów komercyjnych, jak i niekomercyjnych.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Rozwój technologiczny przyczynił się do zwiększenia korzystania z profilowania w szerokim zakresie kontekstów, a wykorzystywanie narzędzi profilowania w celu wspierania pracy funkcjonariuszy organów ścigania i organów zarządzania granicami zyskuje coraz większą uwagę państw członkowskich UE. Profilowanie wykorzystuje się zgodnie z prawem w celu zapobiegania przestępstwom, badania i ścigania przestępstw oraz w celu zapobiegania nielegalnej imigracji. Niezgodne z prawem profilowanie może jednak podważać zaufanie do organów i stygmatyzować niektóre społeczności.

W niniejszym przewodniku wyjaśniono, czym jest profilowanie, które ramy prawne je regulują oraz dlaczego prowadzenie profilowania w sposób zgodny z prawem jest zarówno konieczne, aby przestrzegać praw podstawowych, jak i kluczowe do prowadzenia skutecznych działań policji i skutecznego zarządzania granicami. W przewodniku zawarto również praktyczne wytyczne dotyczące sposobu unikania niezgodnego z prawem profilowania podczas operacji policyjnych i zarządzania granicami.

FRA – AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ
Schwarzenbergplatz 11 – 1040 Wiedeń – Austria
Tel. +43 158030-0 – faks +43 158030-699
fra.europa.eu – @EURightsAgency

Urząd Publikacji
Unii Europejskiej