HANDBUCH

Unrechtmäßiges Profiling heute und in Zukunft vermeiden – ein Leitfaden

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Zahlreiche Informationen über die Agentur der Europäischen Union für Grundrechte finden Sie auf der FRA-Website unter fra.europa.eu.

Europe Direct soll Ihnen helfen, Antworten auf Ihre Fragen zur Europäischen Union zu finden

Gebührenfreie Telefonnummer (*):

00 800 6 7 8 9 10 11

(*) Sie erhalten die bereitgestellten Informationen kostenlos, und in den meisten Fällen entstehen auch keine Gesprächsgebühren (außer bei bestimmten Telefonanbietern sowie für Gespräche aus Telefonzellen oder Hotels).

Weitere Informationen über die Europäische Union sind im Internet unter http://europa.eu verfügbar.

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2019

Print:	ISBN 978-92-9474-249-0	doi:10.2811/464197	TK-06-18-031-DE-C
PDF:	ISBN 978-92-9474-247-6	doi:10.2811/853	TK-06-18-031-DE-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Unrechtmäßiges Profiling heute und in Zukunft vermeiden – ein Leitfaden

Inhalt

Abbildungen und Tabellen

Akronyme und Abkürzungen

CCC	Gemeinsamer zentraler Lehrplan
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDSB	Europäischer Datenschutzbeauftragter
EES	Einreise-/Ausreisesystem
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ENISA	Agentur der Europäischen Union für Netz- und Informationssicherheit
ETIAS	Europäisches Reiseinformations- und genehmigungssystem
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EU-MIDIS	Erhebung der Europäischen Union zu Minderheiten und Diskriminierung
FRA	Agentur der Europäischen Union für Grundrechte
Frontex	Europäische Agentur für die Operative Zusammenarbeit an den Aussengrenzen
IT	Informationstechnologie
OHCHR	Amt des Hohen Kommissars der Vereinten Nationen für Menschenrechte
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
SIS II	Schengener Informationssystem
TCN	Drittstaatsangehörige/Drittstaatsangehöriger
UN	Vereinte Nationen
UNHRC	UN-Menschenrechtsausschuss
VIS	Visa-Informationssystem
WP29	Artikel-29-Datenschutzgruppe

Einleitung

Technologische Entwicklungen haben zu einer verstärkten Nutzung von Profiling in vielen Bereichen geführt, darunter Marketing, Beschäftigung, Gesundheit, Finanzen, Strafverfolgung, Grenzkontrolle und Sicherheit. Der Einsatz von Profiling-Tools zur Unterstützung der Arbeit von Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten hat in den letzten Jahren mehr Beachtung von den EU-Mitgliedstaaten erhalten. Profiling ist ein verbreitetes und rechtskonformes Verfahren, das von Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten zur Verhinderung, Ermittlung und Verfolgung von Straftaten sowie zur Verhinderung und Aufdeckung irregulärer Migration eingesetzt wird. Rechtswidriges Profiling kann jedoch das Vertrauen in die Behörden, insbesondere in die Polizei, beeinträchtigen und bestimmte Gruppen von Menschen stigmatisieren. Dies wiederum kann zu einer Verschärfung der Spannungen zwischen den Gemeinschaften und Strafverfolgungsbehörden führen; der Einsatz von Profiling wird dann als diskriminierend empfunden.

In diesem Handbuch wird erläutert, was Profiling ist, welcher Rechtsrahmen ihm zugrunde liegt und weshalb Profiling von rechtlicher Seite nicht nur die Grundrechte wahren muss, sondern auch von entscheidender Bedeutung für eine wirksame Polizeiarbeit und ein wirksames Grenzmanagement ist. Das Handbuch enthält außerdem praktische Anweisungen zur Vermeidung von unrechtmäßigem Profiling bei Einsätzen von Polizei und Grenzmanagement. Die Grundsätze und Strategien werden im Handbuch durch Beispiele, Fallstudien und die Rechtsprechung aus der gesamten EU und darüber hinaus unterstützt.

Wozu brauchen wir dieses Handbuch?

Profiling wirft eine Reihe von Grundrechtsfragen auf.[1] Beim Profiling besteht die Gefahr, gegen bewährte Rechtsgrundsätze, einschließlich Gleichbehandlung und Nichtdiskriminierung, sowie gegen die Rechte auf Achtung des Privatlebens und des Datenschutzes zu verstoßen. Darüber hinaus stellen sich Fragen zu seiner Wirksamkeit bei der Bekämpfung rechtswidriger Handlungen sowie zu möglichen negativen Folgen für die Beziehungen zwischen den Behörden (einschließlich Polizei und Grenzmanagement) und den Gemeinschaften, denen sie dienen.

Als Reaktion auf diese Bedenken veröffentlichte die Agentur der Europäischen Union für Grundrechte (FRA) im Jahr 2010 das Handbuch *Für eine effektivere Polizeiarbeit. Diskriminierendes „Ethnic Profiling" erkennen und vermeiden*. Das Handbuch konzentrierte sich auf das Profiling durch die Polizei und insbesondere auf die Ausübung von Befugnissen zu Kontrollen und Durchsuchungen. Ziel des Handbuchs war es, Beamtinnen und Beamten in Positionen der mittleren Ebene Werkzeuge in die Hand zu geben, um diskriminierendes Profiling auf der Grundlage der ethnischen Zugehörigkeit zu vermeiden.

Seitdem haben technologische Entwicklungen das Profiling erheblich verändert. Profiling basiert inzwischen zu großen Teilen auf den Ergebnissen der Computeranalyse umfangreicher Datensätze. Auf rechtlicher Seite wurden durch die überarbeiteten und strengeren Datenschutzvorschriften, die seit Mai 2018 in der EU gelten, neue Standards für die Erhebung, Analyse und Nutzung personenbezogener Daten festgelegt.

In diesem aktualisierten Handbuch werden diese wichtigen Änderungen berücksichtigt; die Ausgabe von 2010 wird weiterentwickelt und erweitert, sodass den neuen rechtlichen und praktischen Gegebenheiten Rechnung getragen wird. Dabei wird ein umfassenderes Konzept für das unrechtmäßige Profiling verfolgt, bei dem Folgendes berücksichtigt wird:

- Profiling im Kontext des Grenzmanagements;
- diskriminierendes Profiling aus den verschiedensten Gründen, einschließlich der Staatsangehörigkeit, des Alters und des Geschlechts, und nicht nur aufgrund der ethnischen Zugehörigkeit;
- algorithmisches oder computergestütztes Profiling.

1 Siehe FRA (2018e), S. 85-87; FRA (2017c), S. 88-89; FRA (2016), S. 83-85.

Die Fassung von 2018 enthält außerdem neue Beispiele und Fallstudien, die die Entwicklungen und Innovationen im Bereich Profiling aufzeigen.

Wer sollte dieses Handbuch nutzen?

Dieses Handbuch richtet sich in erster Linie an die Personen, die Polizei- und Grenzschutzbedienstete ausbilden. Es kann Beamtinnen und Beamte in Positionen der mittleren Ebene auch direkt bei der rechtmäßigen Umsetzung von Profiling-Techniken unterstützen. Ziel ist es, das Verständnis für die Theorie und Praxis des Profilings zu verbessern und konkret zu veranschaulichen, wie Profiling im Einklang mit den Grundrechten durchgeführt werden kann.

Das Handbuch befasst sich mit Profiling durch Polizeivollzugsbeamte, z. B. während Kontrollen und Durchsuchungen, sowie mit Kontrollen durch Grenzschutzbeamtinnen und -beamten an den Grenzübergangsstellen, insbesondere dann, wenn darüber entschieden wird, eine Person einer gründlicheren „Kontrolle in der zweiten Kontrolllinie" zu unterziehen. Im Bereich des Grenzmanagements dient es denjenigen als Unterstützung, die sich bei der Aus- und Fortbildung auf den Gemeinsamen zentralen Lehrplan der Grenzschutzausbildung gemäß Artikel 36 Absatz 5 der Verordnung über die Europäische Grenz- und Küstenwache (Verordnung (EU) 2016/1624) stützen.

Das Handbuch befasst sich auch mit Profiling anhand der Analyse umfangreicher Datensätze, einschließlich solcher, die durch Unionsrecht geregelt sind. Profiling in sonstigen Situationen, etwa im privaten Sektor für kommerzielle Zwecke, ist nicht Gegenstand dieses Handbuchs. Zu diesem Thema führt die FRA weitere Untersuchungen durch.[2]

Wie ist das Handbuch zu verwenden?

Dieses Handbuch gibt einen Überblick über die wichtigsten Grundsätze und Strategien des Profilings im Bereich von Strafverfolgung und Grenzmanagement. Es kann als Ganzes gelesen oder als Referenz zur Unterstützung von Aus- und Fortbildungstätigkeiten herangezogen werden.

Das Handbuch enthält drei Kapitel. Im ersten Kapitel wird das Konzept von Profiling erläutert und verdeutlicht, wann Profiling unrechtmäßig wird/würde. Außerdem

2 Siehe das Projekt der FRA zum Thema „Artificial Intelligence, Big Data and Fundamental Rights".

werden die möglichen negativen Auswirkungen auf Einzelpersonen und Gemeinschaften sowie auf die Ausübung der Befugnisse von Polizei und Grenzmanagement beschrieben. Im zweiten Kapitel werden die Grundsätze und Strategien beschrieben, die Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten als Leitfaden für rechtmäßiges Profiling dienen sollen. Kapitel 3 konzentriert sich schließlich auf algorithmisches Profiling. Da die Praxis in diesem Bereich nicht so weit entwickelt ist, enthält dieser Abschnitt weniger konkrete Beispiele. Stattdessen werden die Hauptrisiken für die Grundrechte im Zusammenhang mit computergestütztem Profiling dargelegt und die wichtigsten rechtlichen Anforderungen erörtert, die in der Datenschutz-Grundverordnung (DSGVO) und der Polizeirichtlinie festgelegt sind.

Die verschiedenen Aspekte des Handbuchs werden durch visuelle Elemente gekennzeichnet. Die Hauptaussagen sind in Kernpunkten zusammengefasst und in gelben Kästen hervorgehoben. Hellblaue Kästen weisen auf zentrale Aspekte des Rechtsrahmens hin, und grüne Kästen enthalten praktische Beispiele. Andere Kästen enthalten wichtige Punkte sowie Fallstudien und Beispiele aus der Rechtsprechung. Trotz der Bemühungen, vielfältige Fallstudien auszuwählen, sind die Beispiele aus dem Vereinigten Königreich überrepräsentiert. Dies ist darauf zurückzuführen, dass das Vereinigte Königreich seit den 1980er-Jahren gegen unrechtmäßiges Profiling vorgeht, während dies in anderen Mitgliedstaaten erst seit Kurzem der Fall ist. Das bedeutet, dass das Vereinigte Königreich auf diesem Gebiet umfassendere und langjährig bewährte Maßnahmen und Strategien entwickelt hat, aus denen Beispiele abgeleitet werden können.

Wie wurde dieses Handbuch entwickelt?

Die FRA organisierte ein Treffen mit Experten aus verschiedenen Bereichen, um einen ersten Entwurf des Leitfadens zu erörtern und Unterstützung bei der Fertigstellung einzuholen.

In diesem Zusammenhang dankt die FRA den Experten des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte (OHCHR), der Europäischen Agentur für die Grenz- und Küstenwache (Frontex), des Büros für demokratische Institutionen und Menschenrechte (BDIMR) bei der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), von Amnesty International, des Europäischen Netzes gegen Rassismus (ENAR), des Internationalen Zentrums für Migrationspolitikentwicklung (ICMPD), des Leibniz Instituts für Informationsinfrastruktur Karlsruhe, von European Digital Rights, der Open Society Initiative for Europe sowie den Vertretern des französischen Bürgerbeauftragten, der niederländischen, dänischen und österreichischen Polizeikräfte und des polnischen Grenzschutzes für ihre wertvollen Rückmeldungen bei dem Verfassen des Handbuchs.

Zusammenfassung der wichtigsten Punkte

1. Geschützte Merkmale können niemals die einzige Grundlage für Profiling sein

- Profiling umfasst die **Kategorisierung von Einzelpersonen** entsprechend ihrer Merkmale.
- Für die Erhebung und Verarbeitung **personenbezogener Daten** müssen die Strafverfolgungs- und Grenzschutzbehörden eine Rechtsgrundlage, ein gültiges und rechtmäßiges Ziel sowie die Notwendigkeit und Verhältnismäßigkeit sicherstellen.
- **Geschützte Merkmale** wie Rasse, ethnische Zugehörigkeit, Geschlecht oder Religion können zu den Faktoren gehören, die Strafverfolgungsbehörden und Grenzschutzbeamtinnen und -beamte bei der Ausübung ihrer Befugnisse berücksichtigen, aber sie **dürfen nicht der einzige oder wesentliche Grund sein, eine einzelne Person herauszugreifen.** (Nähere Informationen zu „geschützten Merkmalen" sind in Abschnitt 1.2.1 zu finden).
- Profiling, das ausschließlich oder hauptsächlich auf einem oder mehreren geschützten Merkmalen beruht, stellt eine unmittelbare Diskriminierung dar: Es **verstößt gegen die Rechte und Freiheiten des Einzelnen** und ist daher **unrechtmäßig**.

2. Begegnungen mit Einzelpersonen sollten stets respektvoll, professionell und informativ sein

- Eine **gute Qualität des Zusammentreffens** an sich verhindert voreingenommenes Profiling nicht, aber sie erhöht die Wahrscheinlichkeit einer erfolgreichen Begegnung und verringert die möglichen negativen Auswirkungen, die bei einer Kontrolle durch eine bzw. einen Polizei- oder Grenzschutzbeamten oder beamtin auftreten können. Im Bereich des Grenzmanagements wird professionelles und respektvolles Verhalten ausdrücklich als rechtliche Verpflichtung bezeichnet.
- **Professionelles und respektvolles Verhalten** erhöht im Allgemeinen die Zufriedenheit einer Person beim Zusammentreffen.
- Das **Erklären der Gründe für das Anhalten** trägt dazu bei, das Vertrauen der Öffentlichkeit in Polizei- und Grenzschutzeinsätze zu stärken, und verringert den Eindruck von voreingenommenem Profiling.
- Dennoch rechtfertigen Respekt und Höflichkeit niemals **unrechtmäßige Grenzkontrollen oder Kontrollen und Durchsuchungen**.

3. Profiling sollte objektive und angemessene Gründe haben

- Damit es rechtmäßig ist, Personen anzuhalten oder in eine zweite Kontrolllinie zu verweisen, **müssen angemessene und objektive Gründe für einen Verdacht vorliegen**.
- Persönliche Merkmale können als rechtmäßige Faktoren für das Profiling dienen. Zur Vermeidung einer Diskriminierung **müssen *außerdem* angemessene Gründe für einen Verdacht** vorliegen, die über die geschützten Merkmale hinausgehen.
- Strafverfolgungs- und Grenzschutzmaßnahmen, die sich auf **spezifische und aktuelle Erkenntnisse stützen**, sind mit höherer Wahrscheinlichkeit **objektiv**.
- Besonders wichtig ist, dass die Entscheidung, eine Person anzuhalten oder sie in eine zweiten Kontrolllinie zu verweisen, **nicht ausschließlich auf dem *Gefühl*** einer Beamtin oder eines Beamten im Hinblick auf diese Person basieren sollte, da in diesem Fall das Risiko von Voreingenommenheit, Stereotypen und/oder Vorurteilen bestünde.

4. Unrechtmäßiges Profiling wirkt sich negativ auf die Polizeiarbeit und das Grenzmanagement aus

- **Unrechtmäßiges Profiling beeinträchtigt das Vertrauen in die Polizei und die Grenzschutzbeamtinnen und -beamten.** Dadurch verschlechtert sich unter Umständen die Beziehung zwischen Polizei-/Grenzschutzbeamtinnen und -beamten und Angehörigen von Minderheiten und anderen Gemeinschaften, die sich herausgegriffen fühlen könnten. Dieses Gefühl der Ungerechtigkeit kann zur Folge haben, dass einzelne Personen und Gruppen das Vertrauen in die Polizei und andere Behörden verlieren, was möglicherweise zu einer sinkenden Meldung von Straftaten an die Polizei und weniger Zusammenarbeit mit den Behörden führt. Die Behörden ihrerseits beobachten bestimmte Gruppen unter Umständen mit größerem Argwohn, was unrechtmäßiges Profiling begünstigen kann.
- **Unrechtmäßiges Profiling beeinträchtigt die Wirksamkeit von Profiling**, weil die Häufigkeit, mit der einzelne Personen von der Polizei oder an der Grenze angehalten werden, nicht zwangsläufig mit den Straftatenquoten verschiedener Gruppen einhergeht.
- Es besteht das Risiko einer **selbsterfüllenden Prophezeiung**, wenn bestimmte Minderheiten in unverhältnismäßiger Weise von Polizei- oder Grenzschutzbeamtinnen und -beamten ausgewählt werden und dies zu mehr Festnahmen oder Grenzkontrollen führt.

5. Unrechtmäßiges Profiling hat rechtliche und finanzielle Konsequenzen, und die Beamtinnen und Beamten sind dafür verantwortlich

- Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte sind dafür **verantwortlich**, Profiling gesetzeskonform durchzuführen.
- **Die Erhebung zuverlässiger, genauer und aktueller Daten** ist unabdingbar, um die Rechenschaftspflicht zu gewährleisten.
- **Wirksame Beschwerdemechanismen** können Machtmissbrauch verhindern und dazu beitragen, das Vertrauen der Öffentlichkeit in die Tätigkeit der Polizei- und Grenzschutzbehörden wiederherzustellen bzw. zu stärken.
- **Feedback-Treffen mit Mitgliedern der Öffentlichkeit** dienen dazu, deren Meinungen anzuhören, über Profiling zu sprechen und Rückmeldungen zu Einätzen einzuholen, Gelegenheiten für wichtige Lehren zu bieten und das Profiling zu verbessern.

6. Algorithmisches Profiling muss bestimmte Datenschutzgarantien einhalten

- Bei der Entwicklung und Nutzung von algorithmischem Profiling wird möglicherweise bei jedem Schritt des Prozesses eine **Verzerrung** eingeführt. Um dies und spätere mögliche Grundrechtsverletzungen zu vermeiden, sollten sowohl die **IT-Expertinnen und Experten als auch die Beamtinnen und Beamten, die die Daten auswerten, ein klares Verständnis der Grundrechte haben**.
- Die **Zuverlässigkeit der Daten** ist entscheidend. Wenn Daten in einen Algorithmus eingegeben werden, die Verzerrungen enthalten oder aus unzuverlässigen Quellen stammen, führt dies unweigerlich zu verzerrten und unzuverlässigen Ergebnissen.
- Algorithmisches Profiling muss **rechtmäßig, notwendig** und **verhältnismäßig** sein.
- Die Verarbeitung der Daten muss einen **bestimmten Zweck** erfüllen.
- Einzelpersonen haben ein **Recht darauf,** über die erhobenen und gespeicherten personenbezogenen Daten, deren Verarbeitung und Zweck sowie über ihre Rechte **informiert zu werden.**
- Die Daten sollten **sicher erfasst, verarbeitet und gespeichert** werden. Von den Behörden wird erwartet, dass sie die Verarbeitungstätigkeiten (auch was mit den Daten geschieht) und die damit verbundenen Protokolle (einschließlich der Informationen über die Person(en), die ein Auskunftsrecht bezüglich dieser Daten hat/haben) aufzeichnen.
- Unrechtmäßige Datenverarbeitung muss **verhindert und aufgedeckt** werden: 1) durch vorherige Folgenabschätzungen und 2) durch den Einsatz von Instrumenten zum Schutz der Privatsphäre, die in den Algorithmus vorintegriert sind.

Einschlägige Websites

Europäische Union
Gerichtshof der Europäischen Union (EuGH): http://www.curia.eu
EU-Rechtsvorschriften: http://eur-lex.europa.eu/
Agentur der Europäischen Union für Grundrechte (FRA): http://www.fra.europa.eu
Europäisches Parlament: http://www.europarl.europa.eu

Europarat
Ministerkomitee des Europarates: http://www.coe.int/cm
Europäischer Gerichtshof für Menschenrechte (EGMR): http://www.echr.coe.int

Vereinte Nationen
Amt des Hohen Kommissars der Vereinten Nationen für Menschenrechte (OHCHR): http://www.ohchr.org

Kampf gegen Diskriminierung
Europäische Kommission gegen Rassismus und Intoleranz (ECRI): http://www.coe.int/ecri
Europäisches Netzwerk von Gleichstellungsstellen (Equinet): http://www.equineteurope.org/
Nationale Gleichstellungsstellen: http://www.equineteurope.org/-Equinet-Members-

Datenschutz
Europäischer Datenschutzbeauftragter (EDSB): https://edps.europa.eu/
Europäischer Datenschutzausschuss (EDSA): https://edpb.europa.eu
Nationale Datenschutzbehörden: https://edpb.europa.eu/about-edpb/board/members_en

Strafverfolgung
Netzwerk unabhängiger Behörden für Beschwerden über die Polizei (IPCAN): https://ipcan.org/
Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL): https://www.cepol.europa.eu/
Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (EUROPOL): https://www.europol.europa.eu/

Grenzmanagement
Europäische Agentur für die Grenz- und Küstenwache (Frontex): https://frontex.europa.eu/

Europäisches Unterstützungsbüro für Asylfragen (EASO): https://www.easo.europa.eu/

Umfangreiche Datenbanken
Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA): https://www.eulisa.europa.eu/

1 Hintergrund: Was ist Profiling?

In diesem Kapitel wird erklärt, was Profiling ist und welche Grundrechte davon insbesondere betroffen sein können. Beim Profiling im Bereich der Strafverfolgung und des Grenzmanagements werden drei wesentliche Faktoren betrachtet:

- Das Konzept des Profilings und dessen Einsatz durch Strafverfolgungs- und Grenzschutzbehörden. In diesem Abschnitt werden auch verschiedene Arten von Profiling vorgestellt.

- Die wichtigsten Grundrechtsprinzipien, die zur Gewährleistung eines rechtmäßigen Profilings eingehalten werden müssen, nämlich Nichtdiskriminierung, das Recht auf Achtung des Privatlebens und das Recht auf Datenschutz.

- Die potenziellen negativen Auswirkungen des Profilings, einschließlich der möglichen Folgen für Einzelpersonen und die Beziehungen zu Gemeinschaften, sowie das Vertrauen in die Polizei- und Grenzschutzbehörden.

1.1. Definition von Profiling

Profiling umfasst die **Kategorisierung von Einzelpersonen** entsprechend ihren persönlichen Merkmalen. Dabei kann es sich um „unveränderliche" Merkmale (wie Alter oder Körpergröße) oder „veränderliche" Merkmale (wie Kleidung, Gewohnheiten, Vorlieben und andere Verhaltensweisen) handeln. Beim Profiling kommt Data Mining zum Einsatz, wobei Personen **„kategorisiert werden, da anhand einiger**

beobachtbarer Eigenschaften auf andere Eigenschaften geschlossen werden kann, die sich nicht beobachten lassen".[3]

Kernpunkte

- Profiling umfasst die **Kategorisierung von Einzelpersonen** entsprechend ihren abgeleiteten Merkmalen.
- Im Kontext der Strafverfolgung und des Grenzmanagements erfüllt das Profiling zwei wesentliche Ziele: **Identifizierung bekannter Personen anhand von Erkenntnissen über eine bestimmte Person** und **Vorhersagemethode** zur Ermittlung „unbekannter" Personen, die für die Strafverfolgungs- und Grenzschutzbehörden von Interesse sein könnten. In beiden Fällen kann bewusste oder unbewusste Voreingenommenheit auftreten, durch die Einzelpersonen möglicherweise diskriminiert werden.
- Die Profiling-Aktivitäten von Grenzschutz- und Strafverfolgungsbeamten sind unter Umständen durch Vorurteile beeinflusst, die sich sowohl aus individuellen als auch aus institutionellen Erfahrungen ergeben können. Diese Vorurteile können die Profiling-Bewertung beeinflussen und verändern, was sich sowohl auf die Rechtmäßigkeit als auch auf die Wirksamkeit der Polizeiarbeit auswirkt.
- Stereotype können eine gewisse statistische Wahrheit widerspiegeln. Doch selbst dann **bleiben sie problematisch**, wenn sie dazu führen, dass eine Einzelperson als Mitglied einer Gruppe behandelt wird anstatt auf Grundlage ihrer individuellen Situation.
- Bei der Entwicklung und Nutzung von algorithmischem Profiling **wird möglicherweise bei jedem Schritt des Prozesses eine Verzerrung eingeführt**. Um dies und spätere mögliche Grundrechtsverletzungen zu vermeiden, sollten sowohl die IT-Expertinnen und Experten, die die Algorithmen entwickeln, als auch die Beamtinnen und Beamten, die die Daten erheben und auswerten, ein klares Verständnis der Grundrechte und deren Anwendung in diesem Kontext haben.

Profiling wird zu folgenden Zwecken genutzt:

- Gewinnung von Wissen durch die Analyse vorhandener Daten, um Annahmen über eine Person zu treffen. Dabei werden anhand früherer Erfahrungen und statistischer Analysen Korrelationen zwischen bestimmten Merkmalen und Ergebnissen oder Verhaltensweisen hergestellt;

- Unterstützung von Entscheidungsprozessen, indem diese Korrelationen genutzt werden, um Entscheidungen über zu ergreifende Maßnahmen zu treffen.

3 Dinant, J.-M., Lazaro, C., Poullet, Y., Lefever, N. und Rouvroy, A. (2008), S. 3.

Dadurch ist Profiling ein wirkungsvolles Instrument für Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte. Es birgt jedoch erhebliche Risiken:

- Beim Profiling werden allgemeine Korrelationen hergestellt, die nicht unbedingt auf jeden Einzelnen zutreffen. Jede Einzelperson kann die Ausnahme von der Regel bilden;
- Bei der Erstellung von Profilen kann es zu falschen Korrelationen kommen, sowohl in Bezug auf bestimmte Einzelpersonen als auch auf Gruppen;
- Profile können zu gefährlichen Stereotypen und somit zu Diskriminierung führen;
- Einige Stereotype spiegeln unter Umständen eine statistische Wahrheit wider. Doch selbst dann bleiben Stereotype problematisch, wenn sie dazu führen, dass eine Person als Mitglied einer Gruppe und nicht als Einzelperson behandelt wird.

Beispiele

Potenziell ungenaues Profiling

Die Annahme, dass „Frauen länger leben als Männer", wird durch faktische Forschung untermauert; allerdings kann ein bestimmter Mann länger leben als eine bestimmte Frau. Jede Entscheidung gegenüber einer Frau, die auf dieser Annahme beruht, birgt die Gefahr, dass sie im Einzelfall falsch ist, und bliebe nur im Durchschnitt wahr.

Einzelpersonen können es ihren Angehörigen oder Freunden erlauben, ihren Pkw zu benutzen, was jegliches Risikoprofil eines riskanten Fahrverhaltens, das sich nach dem Eigentümer eines Pkw richtet, unzuverlässig macht.

1.1.1. Profiling im Kontext von Strafverfolgung und Grenzmanagement

Profiling ist ein verbreitetes und rechtmäßiges Verfahren, das von Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten zur Verhinderung, Ermittlung und Verfolgung von Straftaten sowie zur Verhinderung und Aufdeckung irregulärer Migration eingesetzt wird.

Profiling bezeichnet „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".[4] Die Ergebnisse dieser Datenverarbeitung dienen der Steuerung von Maßnahmen im Bereich des Grenzmanagements und der Strafverfolgung, wie Kontrollen und Durchsuchungen, Festnahmen, Zutrittsverweigerungen zu bestimmten Orten oder Verweis an eine gründlichere Kontrolle in der zweiten Kontrolllinie an der Grenze. Es gibt zwei Hauptarten des Profilings:

- Ermittlung von Personen auf der Grundlage spezifischer Erkenntnisse. Dabei wird ein Profil verwendet, in dem die Merkmale bestimmter Verdächtiger auf der Grundlage von Erkenntnissen aufgeführt sind, die zu einem bestimmten Ereignis zusammengetragen wurden;

- Als Vorhersagemethode zur Ermittlung „unbekannter" Einzelpersonen, die für die Strafverfolgungs- und Grenzschutzbehörden von Interesse sein könnten. Dies basiert auf Datenanalysen und fundierten Annahmen, die aus früheren Erfahrungen abgeleitet werden. Idealerweise liegt der Schwerpunkt bei der Vorhersagemethode auf dem Verhalten. In der Praxis liegt der Schwerpunkt jedoch häufig nicht (oder nicht nur) auf dem Verhalten, sondern auf sichtbaren physischen Merkmalen wie Alter, Geschlecht oder ethnischer Zugehörigkeit.

Tabelle 1 enthält einen Vergleich der Hauptmerkmale dieser beiden Arten des Profilings im Rahmen der Polizeiarbeit.

4 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 (Polizeirichtlinie), Art. 3 Abs. 4).

Tabelle 1: Merkmale der erkenntnisgestützten Polizeiarbeit und der vorhersagenden Polizeiarbeit

	Spezifische erkenntnisgestützte Polizeiarbeit	Vorhersagende Polizeiarbeit
Hintergrund	Eine Straftat wurde begangen, oder eine bestimmte Person wurde zur Fahndung ausgeschrieben.	Es wurde keine Straftat begangen, oder es wurde keine Warnung zu einer bestimmter Person ausgegeben.
Ansatz	Reaktiv	Proaktiv
Zielsetzung	Festnahme verdächtiger Person(en)	Vorhersage darüber, wo und wann Verbrechen begangen werden könnten oder wer möglicherweise versuchen könnte, irregulär in das Land zu gelangen
Datengrund-lage	Spezifische Erkenntnisse im Zusammenhang mit dem Fall („individuelles Profil“)	Allgemeine Erkenntnisse zu mehreren Fällen
Art des Prozesses	Kombination aus datengesteuerten und menschlichen Prozessen	Hauptsächlich datengesteuert („Risikoanalyse“)

Quelle: *FRA, 2018*

Beide Arten des Profilings können unrechtmäßig sein, wenn nicht bestimmte Garantien eingehalten werden, einschließlich einer objektiven und angemessenen Begründung für das Profiling. Kapitel 2 und Kapitel 3 liefern praktische Informationen darüber, wie sichergestellt werden kann, dass das Profiling sowohl rechtmäßig als auch im Einklang mit den Menschenrechten erfolgt.

1.1.2. Definition von algorithmischem Profiling

Durch die rasanten technologischen Entwicklungen erfolgt Profiling zunehmend auf Basis von Daten, die in Datenbanken und IT-Systemen gespeichert sind. Beim algorithmischen Profiling werden verschiedene Techniken genutzt, um anhand von Korrelationen und Datenmuster Profile von Personen zu erstellen. Mithilfe von algorithmischem Profiling können Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte Einzelpersonen oder bestimmte Gruppen ins Auge fassen, die auf Grundlage der Datenanalyse ein gewisses Risiko darstellen.

Das algorithmische Profiling wirft erhebliche Grundrechtsfragen auf, z. B. eine mögliche Diskriminierung und Verletzung des Rechts auf Achtung des Privatlebens und

des Rechts auf Datenschutz. In diesem Abschnitt des Handbuchs geht es vor allem um die Frage, wie Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte Daten bei ihrer täglichen Arbeit im Einklang mit den Grundrechtsprinzipien nutzen und verarbeiten können.

Verarbeitung personenbezogener Daten: Wie ist die Rechtslage?

Die rechtlichen Standards für die Verarbeitung personenbezogener Daten zur Erstellung von Profilen sind im Datenschutz-Rechtsrahmen der EU festgelegt. Gemäß Artikel 4 Absatz 4 der Datenschutz-Grundverordnung (DSGVO) und Artikel 3 Absatz 4 der Polizeirichtlinie bezeichnet „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".

Nach Artikel 22 Absatz 1 der Datenschutz-Grundverordnung kann Profiling nur akzeptiert werden, wenn die Entscheidung nicht ausschließlich auf einer automatisierten Verarbeitung beruht und keine rechtliche Wirkung gegenüber der betroffenen Person entfaltet, die sie erheblich beeinträchtigen würde.

Profiling, das in den Geltungsbereich der Polizeirichtlinie fällt (siehe Abschnitt 3.1 zu algorithmischem Profiling und Datenschutz), sollte Artikel 11 Absatz 3 der Polizeirichtlinie entsprechen. Darin ist Folgendes vorgesehen: „Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10* diskriminiert werden, ist nach dem Unionsrecht verboten."

* „Besondere Kategorien personenbezogener Daten" sind „personenbezogene[...] Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie [...] genetische[...] Daten, biometrische[...] Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten

zum Sexualleben oder der sexuellen Orientierung". *Siehe Polizeirichtlinie, Artikel 10 Absatz 1.*

Die Methode, nach der Profile für das algorithmische Profiling erstellt werden, ähnelt einer Technik, die als „**Verhaltensanalyse**" bezeichnet wird und bei der Verbindungen zwischen bestimmten Merkmalen und Verhaltensmustern hergestellt werden. Abbildung 1 zeigt, wie Algorithmen verwendet werden können, um Vorhersagen zu treffen.

Im Fokus: So unterstützen Algorithmen die Entscheidungsfindung

Angesichts der steigenden Verfügbarkeit und Nutzung von Daten wird die Entscheidungsfindung zunehmend erleichtert oder durch modellbasierte Vorhersagemethoden ersetzt, häufig in Form von Algorithmen. Ein Algorithmus ist eine Abfolge von Befehlen, anhand derer ein Computer eine Eingabe in eine Ausgabe umwandelt. Viele Algorithmen basieren auf statistischen Methoden und verwenden Techniken, die Beziehungen zwischen verschiedenen Variablen berechnen. So können beispielsweise die Daten über den Alkoholkonsum einer Gruppe von Personen mit den Daten über die Lebenserwartung dieser Gruppe kombiniert werden, um den durchschnittlichen Einfluss von Alkoholkonsum auf die Lebenserwartung zu berechnen.

Die Ausgabe von Algorithmen gibt stets eine Wahrscheinlichkeit wieder, d. h., es besteht eine gewisse Unsicherheit im Hinblick auf die berechneten Beziehungen oder Klassifikationen. E-Mail-Anbieter beispielsweise verwenden Algorithmen, um Spam-Nachrichten zu erkennen und diese in den Junk-/Spam-Ordner zu verschieben. Die Algorithmen funktionieren gut, sind aber nicht perfekt. Manchmal wird Spam nicht entdeckt und landet im Posteingang; dann liegt ein falsch negatives Ergebnis vor (d. h., die Nachricht wurde fälschlicherweise nicht als Spam erkannt). Seltener kommt es vor, dass eine seriöse E-Mail vom Spamfilter herausgegriffen und in den Junk-/Spam-Ordner verschoben wird; in diesem Fall liegt ein falsch positives Ergebnis vor.

Wenn Fachleute aus der Praxis ein grundlegendes Verständnis davon haben, wie Algorithmen die Entscheidungsfindung unterstützen, können sie mögliche Probleme bei der Anwendung von Algorithmen, z. B. das Potenzial zur Diskriminierung und zur Verletzung des Rechts auf Achtung

des Privatlebens und des Rechts auf Datenschutz, erkennen und die richtigen Fragen stellen.

Weitere Informationen sind FRA (2018b) zu entnehmen.

Die Entwicklung von Algorithmen für die Vorhersage ist ein komplexer Prozess, bei dem mehrere Menschen viele Entscheidungen treffen müssen. Somit umfasst die Entwicklung nicht nur Regeln, die von einem Computer befolgt werden, sondern auch den Vorgang der Erhebung, Aufbereitung und Analyse von Daten. Dabei handelt es sich um einen menschlichen Prozess, der mehrere Phasen umfasst, einschließlich Entscheidungen von Entwicklern und Managern. Die statistische Methode ist nur ein Teil des Prozesses zur Ausarbeitung der endgültigen Regeln für die Vorhersage, Einstufung oder Entscheidungsfindung.[5] Die Art und Weise, wie die Daten erhoben und verwendet werden, kann in jedem Fall diskriminierend sein.

Beispiel

Damit eine Gesichtserkennungssoftware wirksam und genau ist, müssen große Mengen an Bildern und Daten eingespeist werden. Je mehr Daten vorhanden sind, desto genauer sind die Ergebnisse. Bislang wurden die Algorithmen zu Trainingszwecken jedoch überwiegend mit Bildern von weißen Männern und vergleichsweise wenigen Bildern von Frauen und/oder Personen mit anderem ethnischen Hintergrund versorgt. Die von der Software ausgegebenen Ergebnisse sind dadurch ungenauer, und bei Einzelpersonen, die diesen Gruppen angehören, besteht eine höhere Wahrscheinlichkeit für Ungenauigkeiten. Wenn Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte diese Ergebnisse dann für das Profiling von Personen und für Entscheidungen, z. B. im Hinblick auf deren Festnahme, verwenden, kann dies zu Fehlern und möglicherweise zu einer starken Beeinträchtigung der Rechte und Freiheiten des Einzelnen führen.

Weitere Informationen finden Sie in Center on Privacy and Technology at Georgetown Law (2016); und Buolamwini J., Gebru T. (2018).

5 FRA (2018b), S. 4.

Abbildung 1: Algorithmisches Profiling im Kontext von Strafverfolgung und Grenzmanagement

Quelle: FRA, 2018 (angelehnt an/basierend auf Perry, W. L., et al. (2013), S. 11-15, und Zarsky, T. Z. (2002-2003), S. 6-18)

In jeder Phase des Prozesses des algorithmischen Profilings kann es zu einer Verzerrung kommen. Um diskriminierende Voreingenommenheit und Verletzungen der Rechte auf Privatsphäre und Datenschutz zu vermeiden, sollten sowohl die Personen, die die Algorithmen entwickeln, als auch die Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten, die die Daten erheben und auswerten, ein klares Verständnis der Grundrechte und deren Anwendung in diesem Kontext haben.

Die Zuverlässigkeit der Daten ist entscheidend. Beim algorithmischen Profiling muss die Qualität der verwendeten Daten bewertet werden, um deren Zuverlässigkeit sicherzustellen: je geringer die Abweichung, desto höher die Zuverlässigkeit. Werden bei der Entwicklung eines Algorithmus Daten verwendet, die bestehende Vorurteile widerspiegeln oder aus unzuverlässigen Quellen stammen, führt dies

unweigerlich zu verzerrten und unzuverlässigen Ergebnissen. Auch bei den Vorhersagen, die aus den Daten abgeleitet werden, können Fehler auftreten:

- bei falsch positiven Ergebnissen werden Einzelpersonen aufgrund der fehlerhaften Vorhersage, dass sie ein Risiko darstellen, herausgegriffen und einer näheren Überprüfung unterzogen;

- bei falsch negativen Vorhersagen werden Einzelpersonen, die ein tatsächliches Risiko im Zusammenhang mit den Maßnahmen von Strafverfolgung und Grenzmanagement darstellen, vom System nicht als solche erkannt.

1.2. Wann ist Profiling unrechtmäßig?

Kernpunkte

- Persönliche Merkmale können als rechtmäßige Faktoren für das Profiling dienen. Um zu vermeiden, dass Profiling diskriminierend und dadurch unrechtmäßig ist, müssen jedoch außerdem angemessene Gründe für einen Verdacht bestehen, die über die **Schutzmerkmale** hinausgehen.
  - Zu den Schutzmerkmalen gehören Geschlecht, Rasse, Hautfarbe, ethnische oder soziale Herkunft, genetische Merkmale, Sprache, Religion oder Weltanschauung, politische oder sonstige Anschauung, Zugehörigkeit zu einer nationalen Minderheit, Vermögen, Geburt, Behinderung, Alter oder sexuelle Ausrichtung;
  - Schutzmerkmale können durch sonstige personenbezogene Daten offengelegt, abgeleitet oder vorhergesagt werden.
- Für die Erhebung und Verarbeitung **personenbezogener Daten** müssen die Strafverfolgungs- und Grenzschutzbehörden eine Rechtsgrundlage, ein gültiges und rechtmäßiges Ziel sowie die Notwendigkeit und Verhältnismäßigkeit sicherstellen.
  - Personenbezogene Daten sind alle Informationen, die zur direkten oder indirekten Bestimmung einer Person verwendet werden können, z. B. ein Name, eine Kennnummer, Standortdaten oder physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität.

Bei zulässiger Nutzung ist Profiling ein **rechtmäßiges Untersuchungsverfahren**. Damit es rechtmäßig ist, muss es auf **objektiven und angemessenen Begründungen** basieren und mit den Grundrechten wie dem Recht auf Nichtdiskriminierung und dem Recht auf den Schutz personenbezogener Daten im Einklang stehen. Eine objektive und angemessene Begründung gilt beim Profiling als nicht gegeben,

„wenn mit ihr nicht ein rechtmäßiges Ziel verfolgt wird oder keine angemessene Verhältnismäßigkeit der Mittel im Hinblick auf die angestrebte Zielsetzung besteht".[6]

Profiling kann viele verschiedene Grundrechte berühren. In diesem Abschnitt geht es um die Grundrechte, die hauptsächlich von unrechtmäßigem Profiling betroffen sind: das Recht auf Nichtdiskriminierung und die Rechte auf Privatsphäre und Datenschutz. Profiling wird als unrechtmäßig erachtet, wenn:

- es eine ungerechtfertigte Ungleichbehandlung von Personen auf der Grundlage von Schutzmerkmalen umfasst (siehe Abschnitt 1.2.1) oder

- es das Leben von Privatpersonen unnötig beeinträchtigt und/oder die Vorschriften für die Verarbeitung der personenbezogenen Daten nicht eingehalten werden (siehe Abschnitt 1.2.2).

1.2.1. Diskriminierungsverbot

Diskriminierungsverbot: Wie ist die Rechtslage?

„**Diskriminierungen** insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung **sind verboten**."*

Artikel 21 der EU-Grundrechtecharta

„Der Genuss eines jeden gesetzlich niedergelegten Rechtes ist ohne Diskriminierung insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt oder eines sonstigen Status **zu gewährleisten**. Niemand darf von einer Behörde diskriminiert werden, insbesondere nicht aus einem der in Absatz 1 genannten Gründe."

Artikel 1 des Protokolls Nr. 12 zur Europäischen Menschenrechtskonvention

6 Europäische Kommission gegen Rassismus und Intoleranz (ECRI) (2007), Randnummer 28.

** Es ist anzumerken, dass in der Praxis viele Mitgliedstaaten den Schutz vor Diskriminierung über die Gründe hinaus ausgeweitet haben, die in der Charta und der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) niedergelegt sind.*

Diskriminierung liegt vor, „wenn eine Person [...] in einer vergleichbaren Situation eine weniger günstige Behandlung als eine andere Person erfährt, erfahren hat oder erfahren würde", und zwar auf der Grundlage einer vermuteten oder tatsächlichen persönlichen Eigenschaft.[7] Diese Eigenschaften werden im Antidiskriminierungsrecht als „Schutzmerkmale" oder „geschützte Merkmale" bezeichnet. Weitere Informationen über das europäische Recht und die Rechtsprechung auf dem Gebiet der Nichtdiskriminierung finden Sie in der Ausgabe 2018 des von der FRA und dem Europarat veröffentlichten Handbuchs zum europäischen Antidiskriminierungsrecht.[8]

Diskriminierung kann verschiedene Formen annehmen:

Unmittelbare Diskriminierung liegt vor, wenn eine Person *ausschließlich oder hauptsächlich* aufgrund eines Schutzmerkmals wie Rasse, Geschlecht, Alter, Behinderung oder ethnischer Herkunft benachteiligt wird.[9]

Beispiel

Als Reaktion auf eine terroristische Bedrohung erhält die Polizei die Befugnis, alle Personen anzuhalten und zu durchsuchen, von denen sie denkt, dass sie mit terroristischen Handlungen in Beziehung stehen könnten. Es wird vermutet, dass die Bedrohung von einer terroristischen Organisation ausgeht, die in einer bestimmten Region der Welt tätig ist, aber es gibt keine weiteren spezifischen Erkenntnisse. Hält ein Polizeibeamter einen Mann ausschließlich oder hauptsächlich deshalb an, weil sein Aussehen darauf hindeutet, dass er möglicherweise aus derselben Region der Welt stammt, so würde dies eine unmittelbare Diskriminierung darstellen und wäre unrechtmäßig.

7 Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft, ABl. L 180, Art. 2, und Richtlinie 2000/78/EG des Rates vom 27. November 2000 zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf, ABl. L 303, Art. 2.

8 FRA und Europarat (2018).

9 Ebenda, S. 47.

Mittelbare Diskriminierung (im Kontext von Strafverfolgung und Grenzmanagement auch als „Diskriminierung mit unverhältnismäßigen Auswirkungen" bezeichnet) liegt vor, wenn *dem Anschein nach neutrale* Bestimmungen, Kriterien oder Verfahren Personen mit besonderen geschützten Merkmalen gegenüber anderen Personen in besonderer Weise benachteiligen können, es sei denn, diese Bestimmungen, Kriterien oder Verfahren sind durch ein rechtmäßiges Ziel sachlich gerechtfertigt, und die Mittel zur Erreichung dieses Ziels sind angemessen und erforderlich.[10] Die mittelbare Diskriminierung erfordert im Allgemeinen Statistiken, um zu beurteilen, ob eine Person aufgrund ihrer Zugehörigkeit zu einer Gruppe mit besonderen geschützten Merkmalen in der Praxis eine weniger günstige Behandlung erfährt als eine andere.

Beispiel

Zur Durchführung von Routinekontrollen beschließen die Strafverfolgungsbehörden, in der Stadt X zwischen 21.00 und 1.00 Uhr jeden zehnten Pkw anzuhalten; 60 % der Einwohner der Stadt X, die während dieser Zeit Auto fahren, sind afro-karibischer Abstammung, während die afro-karibische Bevölkerung in der Stadt und ihrer Umgebung nur bei 30 % liegt. Da diese Gruppe wahrscheinlich stärker nachteilig betroffenen sein wird als andere, würde hier eine mittelbare Diskriminierung vorliegen.

Die Betrachtung der Diskriminierung anhand eines einzigen Grundes wird den vielen Erscheinungsformen der Ungleichbehandlung nicht gerecht. **Mehrfachdiskriminierung** beschreibt eine Diskriminierung, bei der mehrere, getrennt voneinander wirkende Gründe zum Tragen kommen. So kann eine Person nicht nur wegen ihrer ethnischen Herkunft, sondern auch wegen ihres Alters und ihres Geschlechts diskriminiert werden.[11] **Intersektionelle Diskriminierung** beschreibt eine Situation, in der mehrere Gründe gleichzeitig und untrennbar zusammenwirken und spezifische Arten der Diskriminierung hervorbringen (siehe Beispiel im Kasten).

10 Richtlinie 2000/78/EG des Rates vom 27. November 2000 zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf, ABl. L 303 (Richtlinie zur Gleichbehandlung in Beschäftigung und Beruf), Art. 2; siehe auch FRA und Europarat (2018), S. 59.

11 FRA und Europarat (2018), S. 67.

Beispiel

Ein Polizeibeamter kontrolliert und durchsucht einen jungen Mann afrikanischer Abstammung, ohne dass der begründete Verdacht besteht, dass dieser eine Straftat begangen hat. Der Mann wird nicht nur aufgrund seines Alters (nicht alle jungen Menschen werden angehalten) oder aufgrund seiner ethnischen Herkunft (nicht alle Menschen afrikanischer Abstammung werden angehalten) diskriminiert, sondern genau deshalb, weil er sowohl jung als auch afrikanischer Abstammung ist.

Diskriminierung kann sich auch aus der automatischen Verarbeitung personenbezogener Daten und dem Einsatz von algorithmischem Profiling ergeben. Diskriminierung kann bei der Entwicklung und Implementierung von Algorithmen auftreten, sowohl durch Verzerrungen, die – bewusst oder unbewusst – in den Algorithmus eingebaut werden, als auch bei Entscheidungen, die auf der Grundlage der erlangten Informationen getroffen werden.

In Artikel 9 Absatz 1 der Datenschutz-Grundverordnung ist ausdrücklich festgelegt, dass die Verarbeitung besonderer Kategorien personenbezogener Daten, aus denen persönliche Merkmale wie die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, verboten ist (vollständige Liste geschützter Merkmale siehe Abbildung 9 in Abschnitt 2.2.4). Dieses Verbot kann in bestimmten Fällen aufgehoben werden, etwa zum Schutz des öffentlichen Interesses, sofern die Ausnahme eine Rechtsgrundlage hat, verhältnismäßig und notwendig ist und angemessene Garantien vorsieht.[12]

Ebenso verbietet Artikel 11 Absatz 3 der Polizeirichtlinie über die automatisierte Entscheidungsfindung im Einzelfall im Rahmen der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten das „Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10 diskriminiert werden", einschließlich Daten, aus denen die rassische oder ethnische Herkunft, religiöse Überzeugungen und genetische oder biometrische Daten hervorgehen.[13] Auch hier sind in bestimmten Fällen Ausnahmen von diesem Verbot zulässig; diese müssen jedoch notwendig und mit geeigneten Garantien verbunden sein und

12 Datenschutz-Grundverordnung (DSGVO), Art. 9 Abs 2 Buchst. g.

13 Weitere Informationen: siehe Artikel-29-Datenschutzgruppe (2017b).

sollten entweder eine Rechtsgrundlage oder das Ziel haben, lebenswichtige Interessen einer Person zu wahren.[14]

Verbot von diskriminierendem Profiling: Wie ist die Rechtslage?

„Ein **Profiling, das zur Folge hat**, dass natürliche Personen aufgrund von personenbezogenen Daten **diskriminiert werden**, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, **sollte** gemäß den Bestimmungen der Artikel 21 und 52 der Charta [der Grundrechte] **verboten werden**."

Erwägungsgrund 38 der Polizeirichtlinie

„**Profiling, das zur Folge hat**, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10* **diskriminiert werden**, **ist** nach dem Unionsrecht **verboten**."

Artikel 11 Absatz 3 der Polizeirichtlinie

** Artikel 10 der Polizeirichtlinie: „Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung".*

„Bei der Durchführung der Grenzübertrittskontrollen dürfen die Grenzschutzbeamten Personen **nicht** aus Gründen des Geschlechts, der Rasse, der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung **diskriminieren**."

Artikel 7 des Schengener Grenzkodex

Das Diskriminierungsverbot bedeutet nicht, dass persönliche Merkmale nicht als legitime Faktoren für das Profiling im Kontext strafrechtlicher Ermittlungen oder Grenzübertrittskontrollen herangezogen werden können (siehe Abschnitt 2.3). Es müssen jedoch angemessene Gründe für einen Verdacht vorliegen, die über die

14 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 (Polizeirichtlinie), Art. 10.

geschützten Merkmale hinausgehen. So kann es vorkommen, dass auf eine Person die genaue Beschreibung eines Verdächtigen zutrifft oder ihr Aussehen nicht zu den Angaben in ihrem Reisedokument passt.[15]

Im Fokus: Diskriminierung aus Gründen der Staatsangehörigkeit

Artikel 21 der EU-Grundrechtecharta **beschränkt das Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit auf EU-Bürger**. Die Richtlinie zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse zählt die Staatsangehörigkeit nicht zu den geschützten Merkmalen.

Die Mitgliedstaaten haben jedoch den Geltungsbereich des Diskriminierungsverbots so ausgeweitet, dass die Staatsangehörigkeit auf verschiedene Arten abgedeckt ist. Dies schließt die Anerkennung der Tatsache ein, dass die Staatsangehörigkeit manchmal stellvertretend für die Rasse, ethnische Herkunft oder Religion verwendet wird. In einigen solcher Fälle werden Ungleichbehandlungen aufgrund der Staatsangehörigkeit als Verstoß gegen die Rechtsprechung angesehen, die eine Diskriminierung aus diesen Gründen untersagt (siehe Europäisches Netzwerk von Rechtsexperten für Gleichstellung und Nichtdiskriminierung, 2016, S. 99). In der Praxis sind die Diskriminierung aus Gründen der Staatsangehörigkeit und die Diskriminierung aus Gründen der ethnischen Zugehörigkeit oft schwer zu unterscheiden.

Die Tatsache, dass die Staatsangehörigkeit in Artikel 21 der Charta nicht ausdrücklich als möglicher Diskriminierungsgrund genannt wird, spiegelt in erster Linie den unterschiedlichen Status von EU-Bürgern (und anderen Personen, die nach Unionsrecht Anspruch auf freien Personenverkehr haben) und Drittstaatsangehörigen gemäß dem Unionsrecht wider. Von besonderer Bedeutung ist dies bei grenzüberschreitenden Verfahren, bei denen die Staatsangehörigkeit entscheidend dafür ist, ob eine Person einer gründlichen Kontrolle unterzogen wird und ob sie ein Visum für die Einreise in oder die Durchreise durch den Schengen-Raum besitzen muss.

15 Vereinigtes Königreich, House of Lords (2006), Lord Scott, Opinions of the Lords of appeal for judgment in *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.,* [2006] UKHL 12, 8. März 2006, Randnummer 67.

Gleichzeitig besteht bei einem systematischen Verweis aller Personen einer bestimmten Staatsangehörigkeit an eine Kontrolle in der zweiten Kontrolllinie das Risiko einer Diskriminierung. Die Staatsangehörigkeit kann als legitimer Bestandteil von Risikoprofilen herangezogen werden, um irreguläre Migration oder mutmaßliche Opfer von Menschenhandel zu ermitteln, sie darf jedoch nicht der einzige oder primäre Auslöser einer Kontrolle in der zweiten Kontrolllinie sein. Darüber hinaus ist eine Ungleichbehandlung aufgrund der Staatsangehörigkeit, ebenso wie in anderen Fällen, diskriminierend und daher unrechtmäßig, wenn sie stellvertretend für eine Diskriminierung aufgrund von Schutzmerkmalen verwendet wird, die eng mit der Staatsangehörigkeit verbunden sind, wie Rasse, ethnischer Herkunft oder Religion.

In seinen empfohlenen Grundsätzen und Leitlinien zu Menschenrechten an internationalen Grenzen aus dem Jahr 2014 zählt das Amt des Hohen Kommissars der Vereinten Nationen für Menschenrechte die Staatsangehörigkeit zu den Schutzmerkmalen, die nicht für das Profiling von Migranten verwendet werden sollten (Grundsatz 8).

Rechtsprechung

In der Rechtssache *Rosalind Williams Lecraft gegen Spanien* war eine Frau auf einem Bahnsteig in Spanien von einem Polizeibeamten aufgefordert worden, sich auszuweisen Auf die Frage, weshalb niemand sonst auf dem Bahnsteig sich ausweisen müsse, erhielt sie zur Antwort: „Wegen Ihrer dunklen Hautfarbe." Der UN-Menschenrechtsausschuss betonte in seinem Urteil, dass Personenkontrollen im Interesse der öffentlichen Sicherheit, der Verbrechensvorbeugung und der Verhinderung illegaler Einwanderung im Allgemeinen zulässig seien. Er stellte allerdings auch fest, dass „die Behörden bei der Ausübung dieser Kontrollen jedoch die körperlichen oder ethnischen Merkmale der gezielt kontrollierten Personen nicht als Begründung eines Verdachts auf ihren Aufenthaltsstatus nehmen dürfen. Außerdem dürfen nicht gezielt Personen mit bestimmten körperlichen Merkmalen oder einer bestimmten ethnischen Herkunft kontrolliert werden. Dies verstößt nicht nur gegen die Würde der Betroffenen, sondern fördert auch fremdenfeindliche Stimmungen in der Bevölkerung; ferner widerspricht es einer wirkungsvollen Bekämpfung ethnisch begründeter Diskriminierung".

Im Jahr 2017 wurde eine ähnliche Beschwerde beim EGMR eingereicht, in der es um die Behandlung eines pakistanischen Staatsangehörigen während und nach einer Polizeikontrolle in Spanien geht. Das Gericht muss entscheiden, ob der Beschwerdeführer bei der Personenkontrolle eine Diskriminierung aus Gründen der ethnischen Herkunft erfahren hat und ob Artikel 8 (Recht auf Achtung des Privat- und Familienlebens) verletzt wurde, da die spanischen Behörden nicht alle angemessenen Maßnahmen ergriffen haben, um etwaige rassistische Beweggründe für den Vorfall aufzudecken. Das Urteil steht zum Zeitpunkt der Entstehung dieses Handbuchs noch aus.

Weitere Informationen: siehe UNHRC, Rosalind Williams Lecraft v. Spain, Mitteilung Nr. 1493/2006, und EGMR, Zeshan Muhammad gegen Spanien, Nr. 34085/17, eingereicht am 6. Mai 2017. Siehe auch FRA und Europarat (2018).

In der Rechtssache *B. S. gegen Spanien* machte eine Sexarbeiterin nigerianischer Herkunft, die sich rechtmäßig in Spanien aufhielt, geltend, dass die spanische Polizei sie aufgrund ihrer Rasse, ihres Geschlechts und ihres Berufs körperlich und verbal misshandelt habe. Sie führte aus, dass sie im Gegensatz zu anderen Sexarbeiterinnen europäischer Herkunft wiederholten Polizeikontrollen unterzogen worden und Opfer rassistischer und sexistischer Beschimpfungen geworden sei. Zwei Drittparteien – das AIRE Centre und die European Social Research Unit der Universität Barcelona – forderten den EGMR auf, die intersektionelle Diskriminierung anzuerkennen, was einen auf mehrfachen Gründen fußenden Ansatz verlangte. Der Gerichtshof stellte eine Verletzung von Artikel 3 (Verbot von unmenschlicher oder erniedrigender Behandlung) fest, fuhr jedoch mit einer separaten Ermittlung in der Frage fort, ob auch versäumt wurde, einen möglichen Kausalzusammenhang zwischen der mutmaßlich rassistischen Haltung und den Gewaltakten der Polizei zu untersuchen. In dieser Frage stellte der EGMR eine Verletzung von Artikel 14 (Diskriminierungsverbot) fest, weil die inländischen Gerichte es unterlassen hätten, die besondere Schutzbedürftigkeit der Beschwerdeführerin als afrikanische Frau, die als Prostituierte arbeitete, zu berücksichtigen. Obwohl ein intersektioneller Ansatz verfolgt wurde, wurde der Begriff „Intersektionalität" im Urteil nicht verwendet.

Weitere Informationen: siehe EGMR, B. S. vs. Spain, Nr. 47159/08, 24. Juli 2012.

Im Fokus: Beweislast

Im Jahr 2016 fällte der französische Kassationshof zum ersten Mal eine Entscheidung bezüglich der Frage diskriminierender Personenkontrollen. In seinen *Entscheidungen vom 9. November 2016* entschied das Gericht, dass die Polizei bei drei von 13 Männern afrikanischer oder arabischer Herkunft diskriminierende Personenkontrollen durchgeführt hatte. Es stellte fest, dass der Staat in diesen Fällen zuständig war, und verurteilte ihn zur Zahlung einer Entschädigung an die drei Beschwerdeführer. In acht weiteren Fällen entschied das Gericht, dass die strittigen Identitätskontrollen rechtmäßig waren, da sie auf objektiven und daher nichtdiskriminierenden Faktoren beruhten. In den beiden anderen Fällen trafen die Richter kein Urteil und verwiesen die Fälle für eine Wiederaufnahme des Verfahrens zurück an die vorinstanzlichen Gerichte.

Das Gericht regelte außerdem die Beweislast in solchen Fällen. Personenkontrollen werden nicht aufgezeichnet, wenn sie nicht zu Gerichts- oder Verwaltungsverfahren führen. Das Gericht erklärte, dass die Beschwerdeführer den Gerichten Nachweise für eine Diskriminierung vorlegen sollten. Die Polizei muss entweder nachweisen, dass es bei der Durchführung der Personenkontrollen keine Ungleichbehandlung gab oder dass die Ungleichbehandlung durch objektive Faktoren gerechtfertigt war.

Darüber hinaus stellte das Gericht fest, dass Richter als Belege Studien und statistische Daten berücksichtigen können, mit denen die Häufigkeit von Identitätskontrollen aus diskriminierenden Gründen belegt wird, die bei der Bevölkerungsgruppe, der der Beschwerdeführer angehört, durchgeführt werden (d. h. sichtbare Minderheiten, die anhand physischer Merkmale bestimmt werden, die sich aus der tatsächlichen oder vermeintlichen ethnischen Herkunft ergeben). Diese Belege allein reichen jedoch nicht aus, um eine Diskriminierung nahezulegen.

Das Gericht stellte daher fest, dass eine Personenkontrolle auf der Grundlage physischer Merkmale, die auf die tatsächliche oder vermeintliche ethnische Herkunft schließen lassen, ohne vorherige objektive Rechtfertigung diskriminierend ist und eine schwere Verfehlung darstellt, die in diesen drei Fällen in die Zuständigkeit des Staates fiel.

Weitere Informationen: siehe *Frankreich, Kassationshof (Cour de Cassation), Décision 1245, 9. November 2016.*

1.2.2. Das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten

Nach Unionsrecht sind das Recht auf Achtung des Privatlebens (Artikel 7 der Charta) und der Schutz personenbezogener Daten (Artikel 8 der Charta) eigenständige, wenn auch eng verwandte Rechte. Das Recht auf Privatleben (oder Recht auf Privatsphäre) ist ein umfassenderes Recht, das *jegliche Eingriffe* in das Privatleben einer Person verbietet. Das Privatleben ist nicht nur als etwas zu verstehen, das vertraulich bleiben soll, sondern auch als Mittel, mit dem ein Mensch seine Persönlichkeit ausdrückt, z. B. durch die Wahl der Personen, mit denen er Kontakt hat, oder die Wahl seiner Kleidung. Der Schutz personenbezogener Daten ist auf die Bewertung der Rechtmäßigkeit in Bezug auf die *Verarbeitung personenbezogener Daten* beschränkt.[16] Wenn nicht ausdrücklich auf das Unionsrecht Bezug genommen wird, werden beide Rechte für die Zwecke dieses Handbuchs synonym verwendet. Diese Rechte sind nicht absolut und können unter bestimmten Umständen eingeschränkt werden (siehe Artikel 8 EMRK und Artikel 52 der Charta).

Recht auf Privatsphäre und den Schutz personenbezogener Daten: Wie ist die Rechtslage?

„1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

Artikel 8 der Europäischen Menschenrechtskonvention

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."

16 FRA, EDSB und Europarat (2018).

Artikel 7 der EU-Grundrechtecharta

„1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. […]"

Artikel 8 der EU-Grundrechtecharta

„1. Die betroffene Person hat das Recht, nicht einer **ausschließlich auf einer automatisierten Verarbeitung –** einschließlich Profiling – **beruhenden Entscheidung** unterworfen zu werden, die ihr gegenüber **rechtliche Wirkung entfaltet oder sie** in ähnlicher Weise **erheblich beeinträchtigt**.

2. Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags […] erforderlich ist;

b) aufgrund von Rechtsvorschriften […] zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Artikel 22 Absätze 1 und 2 der Datenschutz-Grundverordnung

„Die Mitgliedstaaten sehen vor, dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung – einschließlich Profiling –, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, verboten ist, es sei denn, sie ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, erlaubt."

Artikel 11 Absatz 1 der Polizeirichtlinie

Das EU-Sekundärrecht behandelt das Recht auf Privatsphäre und den Schutz personenbezogener Daten. In zwei Rechtsvorschriften ist festgelegt, wie personenbezogene Daten erhoben und verarbeitet werden dürfen. Die Verordnung (EU)

2016/679, die Datenschutz-Grundverordnung (DSGVO), enthält allgemeine Grundsätze und Garantien für die Verarbeitung personenbezogener Daten. Die Richtlinie (EU) 2016/680, die sogenannte Polizeirichtlinie, legt spezifischere Vorschriften für die Verarbeitung personenbezogener Daten im Rahmen von Strafverfolgungsmaßnahmen zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten fest. Die wichtigsten Grundsätze und einige wesentliche Unterschiede zwischen den beiden sind in Tabelle 2 dargestellt. Auch die Gesetze zu den großen EU-Datenbanken, die für das Grenzmanagement verwendet werden, z. B. das Visa-Informationssystem (VIS), das Einreise-/Ausreisesystem (EES) oder das Europäische Reiseinformations- und genehmigungssystem (ETIAS), enthalten jeweils einen Datenschutzrahmen (siehe Abschnitt 3.2 zu umfangreichen Datenbanken).

Tabelle 2: Datenschutzvorschriften – Unterschiede zwischen der Polizeirichtlinie und der Datenschutz-Grundverordnung

Datenschutzgrundsatz	DSGVO	Polizeirichtlinie
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben **und in einer nachvollziehbaren Weise** verarbeitet werden.	Personenbezogene Daten müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden.
Zweckbindung	Personenbezogene Daten, die für einen bestimmten Zweck erhoben werden, sollten nicht für einen nicht zu vereinbarenden Zweck weiterverarbeitet werden; **eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt nicht als mit den ursprünglichen Zwecken unvereinbar**.	Personenbezogene Daten, die für einen bestimmten Zweck erhoben werden, sollten anschließend nicht für einen nicht zu vereinbarenden Zweck verarbeitet werden; andere Zwecke gelten als mit dem ursprünglichen Zweck vereinbar, wenn diese Verarbeitung gesetzlich zulässig ist und wenn sie erforderlich und verhältnismäßig ist.
Datenminimierung	Die erhobenen personenbezogenen Daten müssen dem Zweck angemessen und erheblich **sowie auf das** für die Zwecke der Verarbeitung **notwendige Maß beschränkt** sein.	Die erhobenen personenbezogenen Daten müssen dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie erhoben wurden, **nicht übermäßig** sein.

Speicherbegrenzung	Personenbezogene Daten sollten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie erhoben wurden, erforderlich ist; für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke dürfen Daten länger gespeichert werden.	Personenbezogene Daten sollten nicht länger, als es für die Zwecke, für die sie erhoben wurden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht.
Richtigkeit	Die erhobenen personenbezogenen Daten sollten sachlich richtig und auf dem neuesten Stand sein. Unrichtige personenbezogene Daten sollten gelöscht oder berichtigt werden.	
Integrität und Vertraulichkeit	Personenbezogene Daten sollten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt werden.	

Quelle: FRA, 2018

Beispiele

Ein Grenzschutzbeamter übermittelt die Liste der Passagiere in einem Flugzeug an Unbefugte. Sobald die personenbezogenen Daten weitergegeben wurden, können sie für andere, u. a. private, Zwecke verwendet werden. Dies stellt einen klaren Verstoß gegen die Datenschutzgrundsätze dar.

Eine Polizeibeamtin verlässt ihr Büro, während auf ihrem Computerbildschirm eine Liste personenbezogener Daten im Zusammenhang mit Verdächtigen zu sehen ist. Dadurch wird der Grundsatz der Sicherheit personenbezogener Daten untergraben, was einen Verstoß gegen die Datenschutzgrundsätze darstellt.

Rechtsprechung

Gerichtsurteile geben Aufschluss darüber, wie diese Grundsätze in der Praxis angewandt werden.

Zweckbindung

In der Rechtssache *Heinz Huber gegen Bundesrepublik Deutschland* prüfte der EuGH die Rechtmäßigkeit des Ausländerzentralregisters (AZR), das bestimmte personenbezogene Daten von Ausländern – sowohl von EU-Bürgern als auch von Nicht-EU-Bürgern – enthält, die sich länger als drei Monate in Deutschland aufhalten. Der EuGH kam zu dem Schluss, dass die für einen bestimmten Zweck erhobenen Daten nicht für einen anderen Zweck verwendet werden dürfen. Nach Auffassung des Gerichts ist das AZR ein legitimes Instrument zur Anwendung aufenthaltsrechtlicher Vorschriften, und die unterschiedliche Behandlung von Ausländern und deutschen Staatsangehörigen, von denen weniger Daten gespeichert werden, ist angesichts des vorgesehenen Zwecks gerechtfertigt. Der EuGH stellte jedoch fest, dass im AZR gespeicherte Daten nicht zur Bekämpfung der Kriminalität im Allgemeinen verwendet werden dürfen, da dies ein anderer Zweck ist als der, für den die Daten ursprünglich erhoben wurden.

Weitere Informationen: siehe EuGH, Fall C524/06, Heinz Huber gegen Bundesrepublik Deutschland*, 16. Dezember 2008.*

Speicherbegrenzung

In der Rechtssache *S. und Marper gegen Vereinigtes Königreich* forderten die Beschwerdeführer die Löschung ihrer Daten (Fingerabdrücke, Zellproben und DNA-Profile) aus der DNA-Datenbank, die im Vereinigten Königreich zur Überwachung von Straftätern genutzt wird. Sie waren bei ihrer Gerichtsverhandlung freigesprochen worden und hatten Bedenken in Bezug auf die mögliche aktuelle und zukünftige Nutzung ihrer Daten. Die Polizei lehnte dies ab. Der EGMR gelangte zu dem Schluss, dass die zeitlich unbefristete Speicherung der DNA-Proben von Personen, die festgenommen, die später aber freigesprochen wurden oder deren Anklage aufgehoben wurde, einen Verstoß gegen das Recht auf Privatsphäre darstellt. Das Gericht betonte das Risiko der Stigmatisierung, da die Daten von Personen, die nicht wegen einer Straftat verurteilt worden waren, genauso behandelt wurden

wie die Daten von verurteilten Personen. Das Gericht erkannte ferner an, dass der mögliche Schaden, der durch die Speicherung dieser Daten entsteht, insbesondere bei Kindern angesichts der Bedeutung ihrer Entwicklung und Integration in die Gesellschaft erheblich ist.

Weitere Informationen: siehe EGMR, S. and Marper v. United Kingdom*, Nr. 30562/04 und 30566/04, 4. Dezember 2008.*

Um personenbezogene Daten für Profiling-Zwecke zu erheben und zu verarbeiten, müssen die Strafverfolgungs- und Grenzschutzbehörden vier wesentliche rechtliche Kriterien erfüllen. Die Erhebung und Verarbeitung der Daten muss

- **rechtlich festgelegt und geregelt sein (*Rechtsgrundlage*)**: Jede Einschränkung des Rechts auf Achtung des Privatlebens und des Rechts auf Datenschutz muss gesetzlich festgelegt sein und den Wesensgehalt dieser Rechte achten. Das Gesetz muss die Standards der Klarheit und Qualität erfüllen, d. h., die Öffentlichkeit muss darauf zugreifen können, und es muss eindeutig und präzise genug formuliert sein, damit die Öffentlichkeit seine Anwendung und Konsequenzen verstehen kann;

- **einen gültigen, rechtmäßigen und angemessenen Zweck haben (*rechtmäßiges Ziel*):** Rechtmäßige Ziele sind gesetzlich verankert und können nicht ausgeweitet werden. Sie können sich auf die nationale Sicherheit, die Gesundheit, die öffentliche Ordnung oder die Verhütung von Straftaten beziehen;

- **für die Erreichung dieses Zweckes unerlässlich sein (*Notwendigkeit*):** Die Verarbeitung personenbezogener Daten sollte auf das Maß beschränkt werden, das für den Zweck, zu dem die Daten erhoben wurden, erforderlich ist;

- **nicht übermäßig sein (*Verhältnismäßigkeit*):** Die Behörden, die personenbezogene Daten verarbeiten, sollten ein angemessenes Gleichgewicht zwischen dem Zweck und den dafür eingesetzten Mitteln herstellen. Mit anderen Worten: Der Mehrwert der Verarbeitung sollte die potenziellen negativen Auswirkungen nicht aufwiegen.

In Kapitel 3 wird erläutert, wie diese Grundsätze in der Praxis angewandt werden können.

Abbildung 2 zeigt, wie diese Grundsätze verwendet werden können, um zu bewerten, ob eine Maßnahme eventuell das Recht auf Achtung des Privat- und Familienlebens und das Recht auf Datenschutz verletzt (siehe auch Abschnitt 2.3.3 zu Beschwerdemechanismen). Die Rechtssache *Gillan und Quinton gegen Vereinigtes Königreich*, die Polizeikontrollen betraf, macht deutlich, wie der EGMR diese Grundsätze anwandte, um zu bestimmen, ob gegen die Rechte auf Datenschutz und Privatsphäre verstoßen wurde (siehe Kasten zur Rechtsprechung).

Abbildung 2: Verletzung der Privatsphäre und des Datenschutzes – Bewertungsverfahren

Quelle: *FRA, 2018 (basierend auf Europarat (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)*

Rechtsprechung

In der Rechtssache *Gillan und Quinton gegen Vereinigtes Königreich* fochten die Beschwerdeführer, zwei britische Staatsangehörige, die Rechtmäßigkeit der Befugnisse für Kontrollen und Durchsuchungen an, die gegen sie im Rahmen einer gerichtlichen Prüfung angewandt wurden.

Ist die ergriffene Maßnahme gesetzlich vorgeschrieben? Die Maßnahme erfolgte im Einklang mit den Abschnitten 44 bis 47 des Terrorism Act 2000 (Gesetz über den Terrorismus von 2000), in denen Folgendes festgelegt war: 1) zur Verhinderung terroristischer Handlungen konnten leitende Polizeibeamte einem beliebigen uniformierten Polizeibeamten in einem bestimmten Gebiet die Genehmigung erteilen, Kontrollen und Durchsuchungen durchzuführen; 2) eine Genehmigung musste vom Minister (Secretary of State) bestätigt werden und war zeitlich begrenzt, konnte jedoch beliebig oft verlängert werden; 3) obwohl der Zweck solcher Durchsuchungen darin bestand, Gegenstände ausfindig zu machen, die für terroristische Handlungen verwendet werden könnten, musste den Kontrollen und Durchsuchungen kein Verdacht zugrunde liegen, dass die angehaltene(n) Person(en) solche Gegenstände bei sich hatte(n); und 4) Personen, die eine Durchsuchung verweigerten, mussten mit einer Freiheitsstrafe, Geldstrafe oder beidem rechnen (*Gillan und Quinton*, Randnummern 76-80).

Beeinträchtigt die ergriffene Maßnahme die Privatsphäre und/oder den Datenschutz? Die Ausübung von mit Zwang verbundenen Befugnissen durch Strafverfolgungsbehörden, um eine Person anzuhalten und ihre Kleidung und ihre persönlichen Gegenstände zu durchsuchen, stellt einen klaren Eingriff in das Recht auf Achtung des Privatlebens dar. Dieser wird durch die Offenlegung persönlicher Informationen in der Öffentlichkeit verstärkt, was zu Demütigung und Bloßstellung führt (*Gillan und Quinton*, Randnummer 63).

Bewertung der Verhältnismäßigkeit und Notwendigkeit: Das Gericht brachte eine Reihe von Bedenken hinsichtlich der Verhältnismäßigkeit und Notwendigkeit des Gesetzes zum Ausdruck (*Gillan und Quinton*, Randnummern 80-86):

- der gesetzliche Standard für die Genehmigung von Kontrollen war nicht belastend;
- die gesetzlichen Befugnisse sind so umfangreich, dass Einzelpersonen vor gewaltigen Hindernissen stehen, wenn sie nachweisen sollen, dass eine Genehmigung und Bestätigung über die Befugnisse der zuständigen Behörden hinausgeht (*ultra vires*) oder einen Machtmissbrauch darstellt;

- die von der Genehmigung abgedeckten geografischen Gebiete waren sehr weit gefasst, und die Frist wurde wiederholt verlängert, wodurch sich der angestrebte Charakter der Genehmigung verringerte;
- Beschränkungen auf das Ermessen einzelner Beamter waren eher formal als materiell;
- es gab nur geringe Aussichten auf einen gerichtlichen Rechtsbehelf, da der Beamte, der die Durchsuchung durchführte, die Angemessenheit seines Verdachts nicht nachweisen musste; ein Nachweis darüber, dass die Befugnis nicht ordnungsgemäß ausgeübt wurde, war daher nahezu unmöglich.

Aufgrund dieser Erwägungen gelangte der EGMR zu dem Schluss, dass die entsprechenden Abschnitte des Terrorism Act weder hinreichend eingegrenzt seien noch angemessenen rechtlichen Garantien gegen Missbrauch unterlägen und damit Artikel 8 der EMRK verletzten.

Weitere Informationen: siehe EGMR, Gillan and Quinton v. the United Kingdom*, Nr. 4158/05, 12. Januar 2010.*

Die rechtlichen Anforderungen an das Profiling, die im überarbeiteten Datenschutz-Rechtsrahmen der EU enthalten sind, werden in Kapitel 3 erläutert.

1.3. Welche möglichen negativen Auswirkungen ergeben sich aus unrechtmäßigem Profiling für die Strafverfolgung und das Grenzmanagement?

Profiling, das nur auf weit gefassten Kategorien wie Rasse, ethnischer Herkunft oder Religion basiert, ist nicht nur unrechtmäßig, sondern kann sich auch negativ auf die wirksame Arbeit der Polizei- und Grenzschutzbehörden auswirken. In diesem Abschnitt werden zwei mögliche negative Auswirkungen betrachtet:

- Die größte Schwierigkeit hängt damit zusammen, dass die Beziehungen zu Personengruppen belastet werden können. Profiling kann zu Ressentiments bei den besonders betroffenen Gemeinschaften führen und das Vertrauen in die

Polizei- und Grenzschutzbehörden verringern. Dies wiederum kann die Wirksamkeit von Methoden beeinträchtigen, die von einer Zusammenarbeit mit der Öffentlichkeit abhängig sind.

- Es bestehen außerdem Zweifel an der Wirksamkeit weit gefasster Kategorien von Profilen im Bereich des Grenzmanagements oder der Strafverfolgung, z. B. wenn sie dazu führen, dass eine Person fälschlicherweise unter Verdacht gerät.[17]

Wenn Profiling auf unrechtmäßige Weise durchgeführt wird, besteht zudem die Möglichkeit von Beschwerdeverfahren oder rechtlichen Maßnahmen gegen die betreffenden Behörden oder Beamtinnen und Beamten. Dabei kann es sich um eine interne Kontrolle durch Behörden für Beschwerden über die Polizei, spezielle Beschwerdestellen, Kontrollstellen oder das Zivil- und Strafgerichtssystem handeln (siehe Abschnitt 2.3). Einzelnen Beamtinnen und Beamte und Führungskräften in Positionen der mittleren Ebene können im Falle einer Beteiligung an oder Duldung von unrechtmäßigem Profiling administrative und/oder strafrechtliche Sanktionen auferlegt werden. Dies kann zu einem Verlust von Ressourcen führen und die Moral und das Ansehen der Behörden beschädigen.

Kernpunkte

- **Unrechtmäßiges Profiling beeinträchtigt das Vertrauen** in die Strafverfolgungs- und Grenzschutzbehörden und kann zu einer Verschlechterung der Beziehungen mit lokalen Gemeinschaften beitragen.
- Es bestehen **Zweifel an der tatsächlichen Wirksamkeit von weit gefasstem Profiling** zur Aufdeckung von Straftaten und beim Grenzmanagement. Es gibt keine eindeutigen Anhaltspunkte dafür, ob ein solches Profiling die Erfolgsquote von Maßnahmen der Strafverfolgung oder des Grenzmanagements erhöht.

17 FRA (2017d), S. 56.

1.3.1. Auswirkungen auf das Vertrauen in die Polizei und das Grenzmanagement und gute Beziehungen zur Öffentlichkeit

Untersuchungen zeigen, welche negativen Auswirkungen die Verwendung weit gefasster Profile auf die gezielt kontrollierten Personen und die Gemeinschaften, denen sie angehören, haben kann.[18] Im nachstehenden Kasten finden Sie die Reaktionen einiger Personen, nachdem sie einer Kontrolle und Durchsuchung oder einer Grenzkontrolle unterzogen worden sind.

Beispiele

Auswirkungen von Kontrollen und Durchsuchungen oder Grenzkontrollen bei Einzelpersonen

1. Polizeikontrollen – Keskinen, S. et al (2018)

Zwischen 2015 und 2017 befragte die Swedish School of Social Science an der Universität Helsinki 185 Menschen zu ihren Erfahrungen mit Ethnic Profiling. Die Untersuchung ergab, dass die meisten Befragten Kontrollen als unangenehm, lästig oder demütigend empfanden. Nachstehend sind einige Auszüge aus den Erfahrungsberichten der Befragten aufgeführt.

„Ein wenig später hielt mich dann ein anderer Polizist an […], während ich mit zwei weißen Freunden, einem Finnen und einem Niederländer, die Straße entlangging. Und er machte genau das Gleiche, … stellte dieselbe Frage. Ich war sauer, weil ich nicht wusste, warum ich herausgegriffen wurde. Ich habe sie gefragt, und sie meinten, dass sie nur ihre Arbeit machen." (Weiblich, ca. 30 Jahre, afrikanisches Land)

„Einmal, als meine Mutter und mein Bruder in der Stadt unterwegs waren, wurden sie von Polizisten angehalten und aufgefordert, sich auszuweisen. Meiner Meinung nach ist das Ethnic Profiling. Mein Bruder erklärte daraufhin [auf Finnisch]: „Wir haben unsere Pässe nicht dabei, wir tragen sie nicht immer bei uns." Als sie merkten, dass er fließend Finnisch spricht, sagten sie ‚Schon gut". Ich war wütend, weil ich weiß, dass Ethnic Profiling illegal ist,

18 FRA (2017d).

aber meine Mutter und mein Bruder wussten das nicht. Ich hatte das Gefühl, dass sie schlecht behandelt wurden. Ich war also sehr wütend. Einmal habe ich ihnen gesagt, dass das, was ihnen passiert ist, illegal war; offensichtlich wussten sie, dass sie angehalten worden waren, weil sie […] nicht finnisch aussehen, sondern ausländisch." (Weiblich, ca. 20 Jahre, Somalia-Finnland)

„Sie haben immer eine ähnliche Beschreibung. Ich frage mich, wenn sie schon seit 11 Jahren immer nach derselben Person suchen, die ihnen die ganze Zeit entwischt, ob sie ihre Arbeit nicht besonders gut machen, denn ihre Beschreibung [Grenzkontrolle] ist immer ähnlich, und sie passt immer zu mir [lacht]." (Männlich, ca. 30 Jahre, afrikanisches Land-Finnland)

Weitere Informationen: siehe Keskinen, S. et al (2018), The Stopped – Ethnic Profiling in Finland.

2. Grenzkontrollen – FRA (2014a und 2014b)

„Ich verstehe, warum [der Grenzschutzbeamte] mich kontrolliert hat, aber er hätte mich nicht hierher [Kontrolle in der zweiten Kontrolllinie/Polizeirevier] schicken oder mich wie einen Straftäter behandeln müssen. Das machen sie mit allen Osteuropäern."
(Passagier aus Serbien, männlich, am Frankfurter Flughafen befragt)

Frage: *„Wie war Ihrer Ansicht nach die Behandlung bei der Erstkontrolle?"*

Antwort: *„Sie war nicht gut. Sie war demütigend. Er hat mich schlecht behandelt. Er hat bloß meinen Pass genommen, ihn angesehen und dann die Einwanderungsbehörde informiert. Er hat mir einige Fragen gestellt und lauter gesprochen, aber ich habe nichts verstanden. Sie haben mich aus der Reihe geholt, aber sie haben mich nicht respektiert und mir Angst gemacht."*

F: *„Warum hatten Sie Angst und fühlten sich gedemütigt?"*

A: *„Weil ich nicht wusste, was passiert, und sie konnten mir nichts erklären. Außerdem waren viele Leute in der Nähe, und der Beamte sprach mit seinen Kollegen, aber nicht mit mir. Dann musste ich warten, und ich wusste immer noch nicht, warum ich dort war."*
(Passagier aus Angola, männlich, am Flughafen Schiphol befragt)

„Ich verstehe die […] Grenzschutzbeamten wirklich. Es ist für sie auch sehr schwierig, stundenlang in den Kabinen zu arbeiten. Also sind sie gegenüber Leuten wie uns manchmal unfreundlich und werden zum Beispiel auch laut."
(Männlich, türkischer Staatsangehöriger, Lkw-Fahrer, der häufig die Grenze überquert, Kipi)

Zusammengenommen wirken sich diese Einzelerfahrungen möglicherweise negativ auf eine Gruppe aus.[19] Dies kann zu einer deutlichen Verschlechterung der Beziehungen zwischen den Polizei- und Grenzschutzbeamtinnen und -beamten und den Angehörigen von Minderheiten beitragen, die häufig Kontrollen und Durchsuchungen oder verstärkten Grenzkontrollen unterzogen werden.

Fallstudie

Die Rolle von Kontrollen und Durchsuchungen bei Störungen der öffentlichen Ordnung (Vereinigtes Königreich 2011 und Frankreich 2005)

Nach Ausschreitungen in mehreren großen britischen Städten im August 2011 befragten die London School of Economics und die Zeitung The Guardian 270 Beteiligte, warum sie bei den Aufständen mitgemacht hatten. Der Studie zufolge waren Misstrauen und Antipathie gegenüber der Polizei ein entscheidender Faktor, und die häufigsten Beschwerden betrafen die Alltagserfahrung mit der Polizei, wobei viele Menschen sehr frustriert darüber waren, wie Mitglieder ihrer Gemeinschaften von Kontrollen und Durchsuchungen betroffen waren.

Weitere Informationen: siehe London School of Economics (2011).

Eine ähnliche Dynamik wurde auch in anderen EU-Mitgliedstaaten festgestellt. In Frankreich wurden die Ausschreitungen im November 2005 durch ein Ereignis ausgelöst, bei dem zwei Jugendliche, die Minderheiten angehörten, bei einer angeblichen Verfolgung durch die Polizei unbeabsichtigt ums Leben kamen (siehe Jobard, 2008, und Body-Gendrot, 2016).

Weitere Informationen: siehe Hörnqvist (2016).

19 Vereinte Nationen (UN) (2007), Randnummer 57.

In diesem Zusammenhang kann Profiling zu einer stärkeren Feindseligkeit bei anderen Begegnungen zwischen Einzelpersonen und der Polizei oder anderen Strafverfolgungsbehörden führen. Eine größere Feindseligkeit erhöht die Wahrscheinlichkeit, dass routinemäßige Zusammentreffen eskalieren und zu Aggression und Konflikten führen, woraus sich sowohl für die Beamtinnen und Beamten als auch für die Mitglieder der Gemeinschaft Sicherheitsbedenken ergeben.

Weiterhin zeigen aktuelle Untersuchungen, dass Kontrollen, Festnahmen, Verurteilungen oder Inhaftierungen die Menschen von anderen öffentlichen Diensten fernhalten, die über das Strafrechtssystem hinausgehen, z. B. Gesundheits-, Beschäftigungs- und Bildungsorganisationen.[20] Ohne die rechtmäßigen Gründe zu untergraben, die zur Festnahme verurteilter Personen führen, darf nicht vergessen werden, dass es die soziale Eingliederung und Integration von Minderheiten beeinträchtigen kann, wenn Bevölkerungsgruppen, die bereits ausgegrenzt sind, von solchen Einrichtungen ausgeschlossen werden.

Im Fokus: Erkenntnisse der FRA aus der Erhebung EU-MIDIS II

2015 und 2016 erhob die FRA Daten von mehr als 25 500 Personen aus verschiedenen ethnischen Minderheiten und mit unterschiedlichem Migrationshintergrund in allen 28 EU-Mitgliedstaaten.

Welche Daten wurden erhoben?

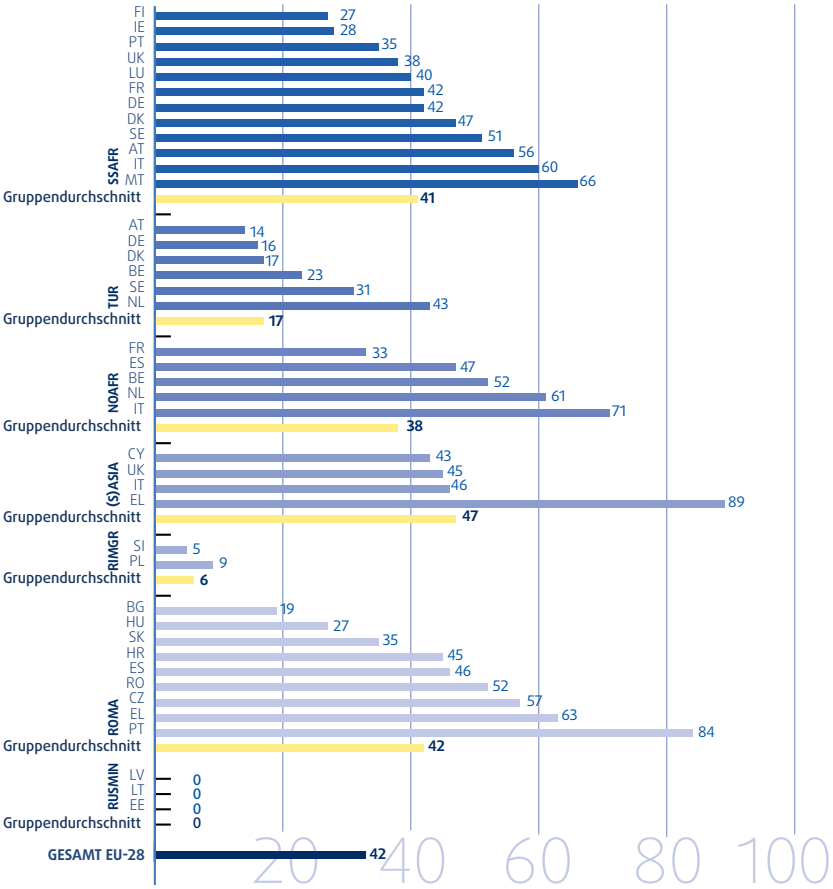
In Bezug auf das Profiling wurden die Teilnehmerinnen und Teilnehmer danach gefragt, ob sie glaubten, dass sie aufgrund ihres Migrations- bzw. ethnischen Minderheitenhintergrunds von der Polizei angehalten worden waren, und danach, wie sie von der Polizei behandelt wurden, was auch Erfahrungen mit körperlicher Gewaltanwendung durch die Polizei einschließt. Begegnungen im Rahmen von Grenzmanagement wurden in der Studie nicht berücksichtigt.

Was zeigen die Ergebnisse?

Kontrollen und ethnische Herkunft: Die Ergebnisse zeigen, dass 26 % aller im Rahmen von EU-MIDIS II Befragten in den fünf Jahren vor der Erhebung von der Polizei angehalten wurden. Von denen, die in den fünf Jahren vor

20 Brayne, S. (2014), S. 367-391.

Abbildung 3: **Jüngste Polizeikontrollen, die von Personen, die in den fünf Jahren vor der Erhebung EU-MIDIS II angehalten wurden, als diskriminierendes Profiling erlebt wurden, nach EU-Mitgliedstaat und Zielgruppe (%)** [a,b,c,d]



Anmerkungen: [a] *Von den muslimischen Befragten, die in den fünf Jahren vor der Erhebung von der Polizei kontrolliert wurden (n = 6787); gewichtete Ergebnisse.*

[b] *Auf einer kleinen Zahl von Antworten fußende Ergebnisse sind statistisch weniger zuverlässig. Daher sind Ergebnisse, die auf 20 bis 49 ungewichteten Beobachtungen in einer Gruppensumme oder auf Zellen mit weniger als 20 ungewichteten Beobachtungen beruhen, in Klammern*

gesetzt. Ergebnisse, die auf weniger als 20 ungewichteten Beobachtungen in einer Gruppensumme beruhen, werden nicht veröffentlicht.

[c] *Fragen: „Wurden Sie in den letzten fünf Jahren in [LAND] (oder seit Sie sich in [LAND] befinden) jemals von der Polizei kontrolliert, durchsucht oder vernommen?" „Glauben Sie, dass Sie bei der LETZTEN Kontrolle aufgrund ihrer ethnischen Herkunft bzw. Ihres Migrationshintergrunds kontrolliert wurden?"*

[d] *Die Akronyme für Zielgruppen beziehen sich auf Zuwanderinnen und Zuwanderer aus [Land/Region] und ihre Nachkommen: TUR = Türkei, SSAFR = subsaharisches Afrika, NOAFR = Nordafrika, SASIA = Südasien, ASIA = Asien, ROMA = Minderheit der Roma*

Quelle: *FRA, 2017b*

der Erhebung angehalten worden waren, gaben 33 % an, dass dies wegen ihrer ethnischen Herkunft bzw. ihres Migrationshintergrunds geschehen sei.

Wahrnehmung von Diskriminierung: Im Durchschnitt gab fast jede zweite befragte Person mit asiatischem (47 %), afrikanischem (subsaharisches Afrika) (41 %) und nordafrikanischem (38 %) Hintergrund, die in diesem Zeitraum angehalten wurde, an, dass dies wegen ihrer ethnischen Herkunft oder ihres Migrationshintergrunds geschehen sei. Ebenso war bei den befragten Roma fast jede zweite Person (42 %) der Ansicht, aufgrund ihrer ethnischen Herkunft angehalten worden zu sein. Dagegen ist der Anteil bei den angehaltenen Personen mit türkischem Hintergrund wesentlich geringer (17 %) (siehe Abbildung 3).

Respekt: Die Ergebnisse zeigen, dass die Mehrheit (59 %) aller Befragten, die in den fünf Jahren vor der Erhebung von der Polizei angehalten wurden, den Eindruck hatte, respektvoll behandelt worden zu sein (25 % „sehr respektvoll", 34 % „ziemlich respektvoll"). Jede(r) vierte (24 %) Befragte erklärte, von der Polizei „weder respektvoll noch respektlos" behandelt worden zu sein. Indes gaben 17 % an, dass die Polizei sie respektlos behandelt habe (8 % „ziemlich respektlos" und 9 % „sehr respektlos"). Befragte Roma und Befragte mit einem nordafrikanischen Hintergrund, die angehalten wurden, gaben häufiger als andere Gruppen an, bei der letzten Kontrolle ein respektloses Verhalten der Polizei erfahren zu haben (25 % bzw. 21 %).

Weitere Informationen: siehe FRA (2017b)

Im Fokus: Bedeutung und Nutzen der Datenerhebung bei Polizeikontrollen

Von den 28 EU-Mitgliedstaaten ist das Vereinigte Königreich derzeit der einzige, in dem die Datenerhebung bei Polizeikontrollen systematisch Informationen zur ethnischen Zugehörigkeit der angehaltenen Person umfasst (siehe auch Abschnitt 2.2.5 und Abschnitt 2.3.1).

Mit den erhobenen Daten wird die Quote für Kontrollen und Durchsuchungen bei verschiedenen ethnischen Gruppen in England und Wales gemessen. Die verwendeten ethnischen Kategorien entsprechen denen aus der Volkszählung des Vereinigten Königreichs aus dem Jahr 2001. Bei dieser Volkszählung wurden 16 Kategorien ermittelt, die in fünf größere Gruppen zusammengefasst wurden:

- Weiß: englisch/walisisch/schottisch/nordirisch/britisch; irisch; sonstiger weißer Hintergrund.
- Gemischter Hintergrund/gemischte ethnische Gruppen: weiß und schwarz-karibisch; weiß und schwarz-afrikanisch; weiß und asiatisch; sonstiger gemischter Hintergrund/gemischter ethnischer Hintergrund.
- Asiatisch/asiatisch-britisch: indisch; pakistanisch; bangladeschisch; sonstiger asiatischer Hintergrund.
- Schwarz/afrikanisch/karibisch/schwarz-britisch: afrikanisch; karibisch; sonstiger schwarzer/afrikanischer/karibischer Hintergrund.
- Sonstige ethnische Gruppen: chinesisch; sonstige ethnische Gruppen.

Mit den erhobenen Daten zu Kontrollen und Durchsuchungen wird die Zahl der kontrollierten Personen einer bestimmten ethnischen Gruppe mit der Gesamtzahl der Angehörigen dieser ethnischen Gruppe, die in diesem Gebiet leben, verglichen; anschließend wird eine Quote pro 1 000 Personen berechnet.

Für 2016/2017 ergab die Analyse der erhobenen Daten, dass 4 von 1 000 weißen Personen und 29 von 1 000 schwarzen Personen angehalten wurden. Die Daten zeigen außerdem, dass die höchsten Quoten bei den drei schwarzen ethnischen Gruppen vorliegen: sonstiger schwarzer Hintergrund (70 Kontrollen pro 1 000 Personen), schwarz-karibisch (28 pro 1 000 Personen) und schwarz-afrikanisch (19 pro 1 000 Personen).

Ohne Nachweise aus aufgeschlüsselten Daten ist es schwer zu belegen, ob sich die Polizei gegenüber bestimmten ethnischen Gruppen unterschiedlich verhält und, wenn ja, ob diese unterschiedliche Behandlung auf diskriminierendes Profiling zurückzuführen ist. In England und Wales sind aufgeschlüsselte Daten öffentlich zugänglich und nach Polizeieinheiten untergliedert. So können abweichende Vorgehensweisen zwischen den Polizeieinheiten ermittelt werden, die entweder als rechtmäßig erklärt werden oder zur Ermittlung potenzieller Diskriminierung bei der Polizeiarbeit herangezogen werden können. Die Daten werden auch auf der Ebene einzelner Polizistinnen und Polizisten verwendet, um diskriminierende Vorgehensweisen bei ihrer Arbeit aufzudecken.

Weitere Informationen: siehe Webseite zu Kontrollen und Durchsuchungen von Gov.uk, Website des Independent Office for Police Conduct sowie Website mit offenen Daten zu Kriminalität und Polizeiarbeit des Home Office. *Siehe auch Vereinigtes Königreich (2018).*

Anweisungen zu Aufzeichnungsmethoden: siehe Open Society Justice Initiative (2018b)

Fallstudie

Erhebung zu den Beziehungen zwischen Polizei und Öffentlichkeit in Frankreich

Im Jahr 2016 führte der französische Bürgerbeauftragte (*Défenseur des droits)* eine Erhebung über den Zugang zu Rechten durch. Der *Défenseur des droits* agiert auch als nationale Stelle für Beschwerden über die Polizei. Die Erhebung umfasste eine repräsentative Stichprobe von mehr als 5 000 Personen.

Im ersten Teil des Berichts werden die Ergebnisse im Zusammenhang mit dem Verhalten der Strafverfolgungsbehörden vorgestellt. Insgesamt lässt die Erhebung auf gute Beziehungen zwischen der Öffentlichkeit und der Polizei schließen. Die große Mehrheit der Befragten gab an, der Polizei zu vertrauen (82 %).

Bei der gezielten Betrachtung von Personenkontrollen zeigt die Erhebung, dass die meisten Menschen keiner Personenkontrolle unterzogen wurden: 84 % der Befragten gaben an, in den letzten fünf Jahren nicht kontrolliert worden zu sein (90 % der Frauen und 77 % der Männer). Von denjenigen, die angaben, dass sie kontrolliert worden waren, berichteten nur wenige von Verhaltensweisen bei der letzten Kontrolle, die die Berufsethik der Sicherheitskräfte verletzen, z. B. informelle Arten der Anrede (16 %), Brutalität (8 %) oder Beleidigungen (7 %). Allerdings meldeten 29 % einen Mangel an Höflichkeit, und mehr als die Hälfte der Befragten (59 %), die kontrolliert worden waren, gab an, dass die Gründe für die Kontrolle nicht erläutert worden waren. Im Allgemeinen werden Personenkontrollen eher als legitim angesehen, wenn die Sicherheitskräfte sich die Zeit nehmen, die Gründe für die Kontrolle zu erläutern.

Aus den Daten geht außerdem hervor, dass bestimmte Personengruppen eher von negativen Erfahrungen berichten. Bei jungen Männern zwischen 18 und 24 Jahren ist die Wahrscheinlichkeit häufiger Personenkontrollen (d. h. mehr als fünfmal in den letzten fünf Jahren) fast 7mal so hoch wie bei der Gesamtbevölkerung, und Männer, die als schwarz oder arabisch wahrgenommen werden, sind zwischen 6- und 11mal stärker von häufigen Personenkontrollen betroffen als der Rest der männlichen Bevölkerung. Bei der Kombination dieser beiden Kriterien wurden 80 % der Männer unter 25 Jahren, die als arabisch oder schwarz wahrgenommen werden, in den letzten fünf Jahren mindestens einmal kontrolliert (im Vergleich zu 16 % der übrigen Befragten). Die Wahrscheinlichkeit einer Personenkontrolle ist bei dieser Gruppe 20mal so hoch wie bei der Gesamtbevölkerung.

Darüber hinaus berichteten junge Männer, die als schwarz oder arabisch wahrgenommen werden, häufiger von problematischem Verhalten bei der letzten Personenkontrolle, etwa der Verwendung informeller Arten der Anrede (40 % gegenüber 16 % der insgesamt Befragten), Beleidigungen (21 % gegenüber 7 %) oder Brutalität (20 % gegenüber 8 %). Diese negativen Erfahrungen und die Häufigkeit von Kontrollen werden mit geringem Vertrauen in die Polizei assoziiert. In der Tat berichtete diese Gruppe von einer Verschlechterung der Beziehungen zur Polizei.

Schließlich zeigen die Ergebnisse, dass nur wenige Befragte (5 %), die auf Verstöße gegen die Berufsethik bei Personenkontrollen hinweisen, Schritte

unternehmen, um diese zu melden. Sie geben vor allem an, dass sie ihre Erfahrungen nicht melden, da sie diese Maßnahmen für nutzlos halten.

Weitere Informationen: siehe Défenseur des droits (2017).

Werden weit gefasste Profile bei einer Minderheitengruppe verwendet, kann dies in Verbindung mit anderen stigmatisierenden politischen Maßnahmen zu einer negativen Eigenwahrnehmung dieser Gruppe führen. Darüber hinaus kann die Gesamtbevölkerung eine negative Wahrnehmung gegenüber dieser Gruppe entwickeln. Die Minderheitengruppe wird unter Umständen zu einer „suspekten Gemeinschaft", die von der Öffentlichkeit mit Kriminalität in Verbindung gebracht wird.[21] Dies kann dazu führen, dass Vorurteile zunehmen.

Die Minderheitengruppe wird möglicherweise das Ziel von unverhältnismäßig vielen Polizeiressourcen, was wiederum wahrscheinlich zu mehr Festnahmen oder Kontrollen an der Grenze führt. In der Folge kann eine selbsterfüllende Korrelation zwischen intensiver Polizeiarbeit und höheren Verhaftungsquoten entstehen (siehe Kasten).[22]

Im Fokus: Das Risiko einer „selbsterfüllenden Prophezeiung"

Wenn Polizeibeamte Profiling nicht auf Basis angemessener Gründe, sondern anhand von Vorurteilen vornehmen, ist es wahrscheinlich, dass sie Informationen so auslegen, dass ihre eigenen Vorurteile bestätigt werden. Dies wird als „Bestätigungsfehler" bezeichnet. Dieser tritt auf, wenn Polizeibeamte aufgrund ihrer Vorurteile ein unrechtmäßiges Verhalten einer Person wegen der tatsächlichen oder vermuteten Rasse, der ethnischen Herkunft, des Geschlechts, der sexuellen Ausrichtung, der Religion oder eines anderen Schutzmerkmals der Person erwarten. Aufgrund dieser Art der Voreingenommenheit greifen Beamtinnen und Beamte mit solchen Vorurteilen mit höherer Wahrscheinlichkeit mehr Personen heraus, die dieser Beschreibung entsprechen.

Da bei Personen, die kontrolliert werden, mit höherer Wahrscheinlichkeit Nachweise über Kriminalität gefunden werden als bei Personen, die nicht

21 Europäische Stelle zur Beobachtung von Rassismus und Fremdenfeindlichkeit (2006), S. 61.

22 Harcourt, B. (2004), S. 1329-1330; House of Commons Home Affairs Committee (2009), Randnummer 16; Vereinte Nationen (2007).

kontrolliert werden, verstärken sich die bestehenden Stereotype einer Beamtin oder eines Beamten durch voreingenommenes Profiling weiter. Dieser falsche „Nachweis" darüber, dass die Entscheidung zum Anhalten dieser Personen korrekt war, wird als „selbsterfüllende Prophezeiung" bezeichnet. Ein solches voreingenommenes Profiling ist diskriminierend, unrechtmäßig und unwirksam und trägt zur Aufrechterhaltung von Stereotypen bei.

Abbildung 4 beschreibt, wie die Kriminalisierung von Personen durch die „selbsterfüllende Prophezeiung" aufrechterhalten wird.

Abbildung 4: Der Kreislauf der selbsterfüllenden Prophezeiung

Quelle: *FRA, 2018*

1.3.2. Die Wirksamkeit von Profiling

Darüber hinaus bestehen Zweifel an der Wirksamkeit von Profiling auf der Grundlage weit gefasster Kategorien zur Aufdeckung von Straftaten. Es ist nicht klar, ob Profiling die Erfolgsquote (oder „Trefferquote") von Strafverfolgungsmaßnahmen tatsächlich erhöht.

Es gibt Anzeichen dafür, dass die Häufigkeit, mit der einzelne Personen angehalten und durchsucht werden, nicht zwangsläufig mit den Straftatenquoten der verschiedenen ethnischen oder Rassengruppen einhergeht (siehe Kasten). Es ist darauf hinzuweisen, dass die Daten zum Strafrecht in den meisten EU-Mitgliedstaaten keinen Überblick über individuelle Verfahren durch die Strafgerichtsbarkeit geben. Daher kann zurzeit nicht nachvollzogen werden, ob eine Festnahme zu einer Strafverfolgung und Verurteilung führt.

Fallstudie

Höhere „Trefferquote" durch geänderte Suchmuster (1998-2000, USA)

Im Jahr 1998 betrafen 43 % der von der US-amerikanischen Zollbehörde durchgeführten Durchsuchungen schwarze Personen und Latinos, was ihren Anteil an den Reisenden deutlich überstieg. Ein besonders großer Teil der Durchsuchungen, einschließlich stark in die Privatsphäre eingreifender Röntgenkontrollen und Leibesvisitationen, wurde bei Latinas und schwarzen Frauen durchgeführt, die als Drogenkuriere verdächtigt wurden. Dies basierte auf einem Profil, das sich stark auf Nationalität und ethnische Zugehörigkeit stützte. Die Trefferquoten waren bei diesen Durchsuchungen für alle Gruppen niedrig: 5,8 % bei Weißen, 5,9 % bei Schwarzen und 1,4 % bei Latinas. Sie waren bei Latinas besonders niedrig. Bei diesen Personen war es in der Tat am wenigsten wahrscheinlich, dass sie an oder in ihrem Körper versteckte Drogen mit sich führten. Im Jahr 1999 änderte die Zollbehörde ihre Verfahren und klammerte die ethnische Zugehörigkeit aus den Faktoren aus, die bei Personenkontrollen zu berücksichtigen sind. Stattdessen wurden Beobachtungstechniken eingeführt, die sich auf Verhaltensweisen wie Nervosität und auf inkonsistente Erklärungen von Passagieren stützen. Darüber hinaus wurden Erkenntnisse aus der Aufklärungsarbeit vermehrt eingesetzt, und es wurde eine stärkere Überwachung der Kontroll- und Durchsuchungsentscheidungen vorgeschrieben. Bis zum Jahr 2000 waren die Unterschiede betreffend die ethnische Zugehörigkeit bei den Durchsuchungen am Zoll nahezu verschwunden. Die Zahl der durchgeführten Durchsuchungen

ging um 75 % zurück, während die Trefferquote von knapp 5 % auf über 13 % stieg und einen nahezu identischen Wert für alle ethnischen Gruppen annahm.

Weitere Informationen: siehe Harris (2002), USA (2000).

Unwirksamkeit von unrechtmäßigem Profiling (2007-2008, Ungarn)

Untersuchungen in Ungarn zeigten, dass Roma unverhältnismäßig häufig Personenkontrollen unterzogen wurden. Rund 22 % aller von der Polizei kontrollierten Personen gehörten der Gemeinschaft der Roma an, während der Anteil der Roma in der Bevölkerung bei rund 6 % lag. Die unverhältnismäßig hohe Zahl von Personenkontrollen bei Roma spiegelte sich nicht in Nachweisen über rechtswidriges Verhalten wider: Bei 78 % der Personenkontrollen bei Roma leitete die Polizei keine Maßnahmen ein, und 19 % wurden mit einer Ordnungswidrigkeit in Verbindung gebracht * (verglichen mit 18 % der Kontrollen bei der Gesamtbevölkerung). Darüber hinaus waren die Verhaftungsquoten bei der Roma-Gemeinschaft und der Gesamtbevölkerung ähnlich.

Weitere Informationen: siehe Tóth, B. M. und Kádár, A. (2011).

* „Ordnungswidrigkeiten sind Quasi-Straftaten, erfüllen jedoch keinen Straftatbestand (sind also nicht im Strafgesetzbuch geregelt). Ordnungswidrigkeiten bezeichnen Übertretungen, die durch eine 60tägige Freiheitsstrafe geahndet werden können, wie Prostitution oder körperliche Drohungen, oder auch Vergehen, die mit weniger strengen Maßnahmen geahndet werden können (z. B. Geldstrafe, Beschlagnahme von Waren oder Zutrittsverbot bei bestimmten Ereignissen). Beispiele für solche Vergehen sind kleinere Diebstähle oder Verkehrsverstöße." *Siehe Kádár, A., Körner, J., Moldova, Z. und Tóth, B. (2008), S. 23.*

Es werden auch Fragen zu den Gründen gestellt, aus denen bestimmte Personen angehalten werden. Laut einer Studie des Vereinigten Königreichs enthielt „ein alarmierend hoher Anteil von 27 % (2 338) der untersuchten Aufzeichnungen zu Kontrollen und Durchsuchungen [...] keine angemessenen Gründe für die Durchsuchung von Personen, obwohl viele dieser Aufzeichnungen von Vorgesetzten gebilligt worden waren".[23] Dies bedeutet der Untersuchung zufolge, dass „die Polizeikräfte unter Umständen nicht in vollem Umfang den Erfordernissen der Gleichheit im

23 Vereinigtes Königreich, Her Majesty's Inspectorate of Constabulary (HMIC), (2013), S. 6.

öffentlichen Dienst [entsprechen], wonach sie darauf achten müssen, rechtswidrige Diskriminierung abzuschaffen und die Chancengleichheit zu stärken, gute Beziehungen zu fördern und zu diesem Zweck sicherzustellen, dass sie in angemessener Weise Daten erheben, analysieren und veröffentlichen, um nachzuweisen, dass sie über ausreichende Informationen verfügen, um die Auswirkungen ihrer Arbeit zu verstehen."

2 Rechtmäßiges Profiling: Grundsätze und Verfahren

In diesem Kapitel liegt der Schwerpunkt auf dem Profiling durch Polizeivollzugsbeamte, insbesondere bei Kontrollen und Durchsuchungen, sowie durch Grenzschutzbeamtinnen und -beamte, insbesondere bei Grenzkontrollen in der zweiten Kontrolllinie. Es werden die wichtigsten Grundsätze und Verfahren erläutert, die dazu beitragen können, das Risiko von unrechtmäßigem Profiling zu verringern. Diese Maßnahmen können sowohl auf Managementebene als auch auf operativer Ebene ergriffen werden. Dabei werden die unterschiedlichen rechtlichen und praktischen Rahmenbedingungen für Kontrollen und Durchsuchungen sowie Grenzkontrollen berücksichtigt.

Im Hinblick auf das Grenzmanagement enthält der Schengener Grenzkodex (Verordnung (EU) 2016/399)[24] einheitliche Regeln für die Grenzkontrollen an den Außengrenzen der EU. Dies bedeutet, dass einige der in diesem Kapitel dargelegten Grundsätze – beispielsweise in Bezug auf die Informationen, die Drittstaatsangehörige erhalten müssen, die einer Kontrolle in der zweiten Kontrolllinie unterzogen werden – gesetzlich vorgeschrieben und für die Mitgliedstaaten verbindlich sind. Darüber hinaus spielt Frontex eine wichtige Rolle bei der Förderung eines einheitlich hohen Standards bei Grenzkontrollen. Insbesondere die Verordnung über die Europäische Grenz- und Küstenwache aus dem Jahr 2016 sieht vor, dass die Mitgliedstaaten bei der Aus- und Fortbildung von Grenzschutzbeamtinnen und -beamten die gemeinsamen zentralen Lehrpläne zu befolgen haben, die von Frontex entwickelt wurden. Der 2012 veröffentlichte gemeinsame zentrale Lehrplan enthält eine

24 Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex), ABl. L 77 vom 23.3.2016.

Grundrechtskomponente, die auch das Profiling umfasst (siehe Abschnitt 2.2.3 zu gezielten Schulungen).

Im Fokus: Gründe für eine Zweitkontrolle an der Grenze

Aufgrund des systematischen Charakters der Grenzkontrollen muss jeder Reisende eine grundlegende Erstkontrolle durchlaufen, bei der Reisedokumente und andere Einreiseanforderungen überprüft werden. Einige Reisende können darüber hinaus an eine Kontrolle in der zweiten Kontrolllinie verwiesen werden. Dafür kann es verschiedenen Gründe geben: ein Treffer in einer Datenbank, ein verdächtiges Reisedokument, Übereinstimmung mit einem Risikoprofil oder verdächtiges Verhalten.

Bei der Erstkontrolle kann sich die Grenzschutzbeamtin oder der Grenzschutzbeamte auf Informationen stützen, die sich aus einem Abgleich der Daten aus dem maschinenlesbaren Reisedokument (einschließlich biometrischer Identifikatoren) mit den in nationalen, EU- und internationalen Datenbanken wie dem Schengener Informationssystem und dem Visa-Informationssystem sowie den in den Datenbanken von Europol und Interpol gespeicherten Daten ergeben. In der Praxis kommt es häufig aufgrund eines Treffers in einer der Datenbanken zu einem Verweis an eine Kontrolle in der zweiten Kontrolllinie.

Eine Person kann jedoch auch aus anderen Gründen einer Kontrolle in der zweiten Kontrolllinie unterzogen werden, z. B. wenn sie einem Risikoprofil entspricht oder der Beamtinnen und Beamte einen sonstigen Verdacht hinsichtlich der Person hat. Im Schengen-Katalog heißt es, dass das Ziel der Erstkontrollen neben der Durchführung von Grenzkontrollen gemäß dem Schengener Grenzkodex darin bestehen sollte, Profile von Passagieren zu erstellen und verdächtige Personen zu ermitteln, die einer eingehenderen Kontrolle in der zweiten Kontrolllinie unterzogen werden sollen *. Die Grenzschutzbeamtinnen und -beamten müssen daher eine Kombination anderer Indikatoren und Kriterien prüfen, um festzustellen, ob eine Person möglicherweise versucht, illegal einzureisen, ein Sicherheitsrisiko darstellen könnte oder beispielsweise ein Opfer von Menschenhandel sein könnte. Unabhängig davon, ob sie ein bestimmtes bestehendes Risikoprofil anwenden oder nicht, nutzen die Grenzschutzbeamtinnen und -beamten in diesen Situationen das Profiling.

Da sie für einen reibungslosen Verkehr der Reisenden sorgen müssen, haben die Grenzschutzbeamtinnen und -beamten nur begrenzt Zeit, um objektiv zu beurteilen, ob eine Person einer Kontrolle in der zweiten Kontrolllinie unterzogen werden soll. Aus Informationen von Frontex geht hervor, dass die Beamtinnen und Beamten in den EU-Mitgliedstaaten durchschnittlich in nur 12 Sekunden entscheiden müssen, ob sie eine Person für eine eingehendere Prüfung herausgreifen sollen **. Sie stehen also unter erheblichem Druck, rasch eine richtige Entscheidung zu treffen.

* *Rat der Europäischen Union (2009), Empfehlung 43.*
** *Europäische Agentur für die Grenz- und Küstenwache (Frontex) (2015).*

Die in diesem Kapitel dargelegten Grundsätze und praktischen Instrumente bieten Informationen, um Diskussionen und Maßnahmen zu fördern, die den Beamtinnen und Beamten und ihren übergeordneten Organisationen helfen können, ihre Profiling-Aktivitäten rechtmäßig durchzuführen. Die drei wichtigsten erörterten Grundsätze sind:

- Die Würde des einzelnen Menschen wahren.
- Sicherstellen, dass das Profiling auf angemessenen und objektiven Gründen beruht.
- Die Rechenschaftspflicht gewährleisten.

Mit jedem dieser Grundsätze ist die Notwendigkeit verbunden, sicherzustellen, dass Polizei- und Grenzschutzbeamtinnen und -beamte bei der Anwendung von Profiling gesetzeskonform handeln.

2.1. Die Würde des einzelnen Menschen wahren

Kernpunkte

- Durch Gewährleistung einer **guten Qualität des Zusammentreffens** wird diskriminierendes Profiling nicht an sich ausgeschlossen. Es ist jedoch wahrscheinlich, dass eine Begegnung erfolgreicher verläuft und die möglichen negativen Auswirkungen von Kontrollen und Durchsuchungen verringert werden. Im Bereich des Grenzmanagements ist professionelles und respektvolles Verhalten eine rechtliche Verpflichtung.
- **Professionelles und respektvolles Verhalten** erhöht im Allgemeinen die Zufriedenheit einer Person beim Zusammentreffen.
- Eine **Erklärung der Gründe für das Anhalten** trägt dazu bei, das Vertrauen einer Person in Polizei- und Grenzschutzeinsätze zu stärken, und verringert den Eindruck von diskriminierendem Profiling.
- Respekt und Höflichkeit **rechtfertigen niemals unrechtmäßige Grenzkontrollen oder Kontrollen und Durchsuchungen durch die Polizei.**

Die Wahrung der Würde des Einzelnen ist nicht nur ein Grundrecht, sondern auch ein Kernprinzip bei Polizei- und Grenzschutzeinsätzen. Bei Einsätzen, die Menschen betreffen, sind die Art und Weise, wie Polizei- und Grenzschutzbeamtinnen und -beamte mit den angehaltenen Personen sprechen und umgehen sowie die Informationen, die sie ihnen geben, von entscheidender Bedeutung.

Es sollte bedacht werden, dass das Herausgreifen von Einzelpersonen – egal wie höflich und professionell die Beamtinnen und Beamten vorgehen – eine eingreifende Erfahrung ist, die stets auf zulässigen Gründen beruhen muss. Die Wahrnehmung von diskriminierendem Profiling hängt auch von der Häufigkeit und der Anzahl der Begegnungen mit den Polizei- und Grenzschutzbehörden ab. Dies unterstreicht, wie wichtig es ist, sicherzustellen, dass immer objektive und angemessene Gründe für das Anhalten einer Person vorliegen.

Was besagen die Standards?

„Grenzübertrittskontrollen sollten auf eine Weise durchgeführt werden, bei der die menschliche Würde in vollem Umfang gewahrt wird. Die Durchführung von Grenzkontrollen sollte auf professionelle und respektvolle Weise erfolgen und, gemessen an den verfolgten Zielen, verhältnismäßig sein."

Erwägungsgrund 7 des Schengener Grenzkodexes

„Alle Reisenden haben entsprechend dem geltenden internationalen, gemeinschaftlichen und nationalen Recht Anspruch darauf, über die Art der Kontrolle informiert und professionell, freundlich und höflich behandelt zu werden."

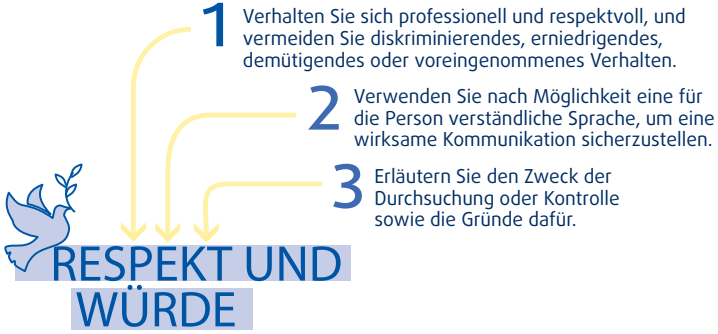
Abschnitt 1.2 des Leitfadens für Grenzschutzbeamte (Schengen-Handbuch)

„Das Polizeipersonal muss gegenüber der Bevölkerung integer und respektvoll handeln und spezielle die Situation jener Person berücksichtigen, die einer besonders gefährdeten Gruppe angehört."

Empfehlung 44 des Europäischen Kodex für die Polizeiethik

Sicherzustellen, dass die Polizei- und Grenzschutzbeamtinnen und -beamten in angespannten und schwierigen Situationen höflich sind und ausreichend informieren, ist nicht immer einfach. Es gibt jedoch Belege dafür, dass ein respektvoller Umgangston die Zufriedenheit im Rahmen der Begegnung erheblich steigert.[25] Abbildung 5 vermittelt einige Faktoren für eine respektvolle Begegnung.

Abbildung 5: Drei Faktoren für ein respektvolles Zusammentreffen



Quelle: *FRA, 2018*

25 FRA (2014b).

Einige Bestandteile von Grenzkontrollen werden durch den Schengener Grenzkodex geregelt, z. B. die Anforderungen, dass Kontrollen auf professionelle und respektvolle Weise durchzuführen sind, und dass Auskünfte über den Zweck und das Verfahren der Kontrolle zu erteilen sind (Schengener Grenzkodex, Erwägungsgrund 7, Artikel 7 sowie Artikel 8 Absatz 5). Die Verwendung einer gemeinsamen Sprache hingegen ist im Zusammenhang mit dem Grenzmanagement aufgrund der naturgemäß unterschiedlichen Art des Grenzverkehrs keine absolute Anforderung. Nach dem Schengener Grenzkodex sollen die Mitgliedstaaten die Grenzschutzbeamtinnen und -beamten allerdings dazu anhalten, die zur Wahrnehmung ihrer Aufgaben erforderlichen Sprachen zu erlernen (Artikel 16 Absatz 1). Der Schengen-Katalog, der eine Reihe von Empfehlungen und bewährten Verfahren für Kontrollen an den Außengrenzen enthält, empfiehlt außerdem, dass die Grenzschutzbeamtinnen und -beamten in der Lage sind, bei der Erfüllung ihrer täglichen Aufgaben in Fremdsprachen zu kommunizieren. Als ein bewährtes Verfahren bezeichnet er die ausreichende Kenntnis der Sprachen der Nachbarländer sowie anderer Sprachen abhängig von der Art des Grenzverkehrs. Idealerweise sollten in jeder Schicht Beamtinnen und Beamte mit entsprechenden Sprachkenntnissen vertreten sein.[26]

Mangelnde Rücksicht und mangelnder Respekt bei Polizeikontrollen kann sich direkt auf die Wirksamkeit der Polizeiarbeit auswirken (siehe Abschnitt 1.3.2). In dem im Vereinigten Königreich ausgearbeiteten Verhaltenskodex im Rahmen des Police and Criminal Evidence Act (PACE, Polizei- und Beweismittelgesetz) heißt es: „Alle Kontrollen und Durchsuchungen müssen höflich, rücksichtsvoll und respektvoll gegenüber der betreffenden Person durchgeführt werden. Dies hat erhebliche Auswirkungen auf das Vertrauen der Öffentlichkeit in die Polizei. Es müssen alle zumutbaren Anstrengungen unternommen werden, um die Bloßstellung zu minimieren, die eine Person bei einer Durchsuchung möglicherweise empfindet."[27]

Einige wichtige Faktoren für die Wahrung der Würde, z. B. die Erläuterung der Gründe für die Kontrolle und die Möglichkeit, dass Einzelpersonen ihre Meinung äußern dürfen, sind grundlegende Bestandteile der Verfahren von Polizei und Grenzmanagement. Formulare zu Kontrollen und Durchsuchungen können dabei helfen, strukturiert zu informieren (siehe Abschnitt 2.3.1).

Beim Grenzmanagement sind Standardformulare ein nützliches Instrument, um Reisende über den Zweck und das Verfahren der Kontrolle in der zweiten Kontrolllinie

26 Rat der Europäischen Union (2009), Empfehlungen 27 und 41.

27 Vereinigtes Königreich, Home Office (2014a), Abschnitt 3.1.

zu informieren. Sie können die Kommunikation mit den Reisenden erleichtern, sofern sie ausgehändigt und nötigenfalls durch weitere mündliche Erklärungen ergänzt werden. Der Schengener Grenzkodex schreibt vor, dass Personen, die einer Kontrolle in der zweiten Kontrolllinie unterzogen werden, schriftlich in einer Sprache, die sie verstehen oder bei der vernünftigerweise davon ausgegangen werden kann, dass sie sie verstehen, über den Zweck und das Verfahren der Kontrolle unterrichtet werden. Die Informationen sollten:

- in allen Amtssprachen der Union sowie in den Sprachen der an den betreffenden Mitgliedstaat angrenzenden Staaten verfügbar sein;

- darauf hinweisen, dass der Reisende um den Namen oder die Dienstausweisnummer des Grenzschutzbeamtinnen und -beamten, der die Kontrolle durchführt, sowie um die Bezeichnung der Grenzübergangsstelle und um das Datum, an dem die Grenze überschritten wurde, ersuchen kann.

Diese Faktoren für eine respektvolle Begegnung im Zusammenhang mit Kommunikations- und zwischenmenschlichen Fähigkeiten sind in den Arbeitsanweisungen schwieriger zu beschreiben und müssen bei der Aus- und Fortbildung möglicherweise stärker berücksichtigt werden. Aus folgenden Gründen kann es schwierig sein, bei der Begegnung einen positiven Umgangston zu pflegen:

- begrenzte Kommunikationsfähigkeiten;

- Unfähigkeit, den Grund für die Maßnahme anzugeben; und

- Versäumnis, persönliche und institutionelle Vorurteile und negative Stereotypen sowie Feindseligkeiten in Gruppen innerhalb der Gemeinschaft zu überwinden.

2.2. Angemessene und objektive Gründe

Kernpunkte

- Strafverfolgungs- und Grenzschutzmaßnahmen, die sich auf spezifische und aktuelle Erkenntnisse stützen, sind mit höherer Wahrscheinlichkeit objektiv.
- Damit Kontrollen und Durchsuchungen sowie Verweise an die zweite Kontrolllinie rechtmäßig sind, müssen **angemessene und objektive Gründe für einen Verdacht** bestehen. Ein „Bauchgefühl" ist kein angemessener oder objektiver Grund für die Kontrolle und Durchsuchung einer Person oder den Verweis einer Person an eine Kontrolle in der zweiten Kontrolllinie.
- Geschützte Merkmale wie Rasse, ethnische Zugehörigkeit, Geschlecht oder Religion können zu den Faktoren gehören, die Strafverfolgungsbehörden und Grenzschutzbeamtinnen und -beamte bei der Ausübung ihrer Befugnisse berücksichtigen, aber **sie dürfen nicht der einzige oder wesentliche Grund sein, um eine einzelne Person herauszugreifen**.
- Profiling, das ausschließlich oder hauptsächlich auf einem oder mehreren geschützten Merkmalen beruht, ist unrechtmäßig.

Objektivität ist ein wichtiger Grundsatz der Arbeit von Polizei und Grenzmanagement. Beim Profiling sollten Einzelpersonen nur auf der Grundlage angemessener und objektiver Verdachtsgründe angehalten und durchsucht oder einer Grenzkontrolle in der zweiten Kontrolllinie unterzogen werden. Zu den objektiven Gründen gehören beispielsweise das Verhalten der Person, spezifische Erkenntnisse oder Umstände, die eine oder mehrere Personen mit mutmaßlich rechtswidrigen Handlungen in Verbindung bringen.

Um Objektivität beim Profiling zu gewährleisten, ist Folgendes erforderlich:

- Vermeidung von Voreingenommenheit, auch durch eindeutige Vorgaben und gezielte Schulungen; und
- effiziente Nutzung von Erkenntnissen und Informationen.

2.2.1. Vermeidung von Voreingenommenheit

Der Europäische Kodex für die Polizeiethik enthält Anweisungen zum Verhalten der Polizei in Bereichen wie Polizeiaktion und intervention, Verantwortlichkeit der Polizei

und Polizeiaufsicht.[28] Er unterstreicht folgenden allgemeinen Grundsatz: „Die Polizei muss ihren Auftrag in gerechter Form erfüllen und sich dabei insbesondere an die Grundsätze der Unparteilichkeit und der Nichtdiskriminierung halten".[29]

Werden Personen *ausschließlich oder hauptsächlich* aufgrund ihrer tatsächlichen oder vermuteten Rasse, der ethnischen Herkunft, des Geschlechts, der sexuellen Ausrichtung, der Religion oder eines anderen verbotenen Grundes herausgegriffen, verstößt dies gegen die Grundrechte. Außerdem kann dies erhebliche negative Folgen sowohl für die Behörden als auch für die Gemeinschaften haben (siehe Abschnitt 1.3).

Diskriminierendes Profiling kann sowohl persönliche als auch institutionelle Vorurteile widerspiegeln. Zusätzlich zu persönlichen Vorurteilen können bestimmte Vorgehensweisen bei Strafverfolgungs- und Grenzschutzbehörden zu Stereotypen und diskriminierendem Verhalten führen. Eine transparentere Gestaltung der institutionellen Verfahren und Vorgehensweisen kann dazu beitragen, Diskriminierung und das Aufrechterhalten von Stereotypen zu bekämpfen.

Die Erkennung tief verwurzelter Vorurteile kann schwierig sein. Polizei- und Grenzschutzbeamtinnen und -beamte gehen möglicherweise davon aus, dass sie Einzelpersonen aus angemessenen und objektiven Gründen (z. B. dem Verhalten) herausgreifen, obwohl diese Entscheidungen in Wirklichkeit ihre Vorurteile widerspiegeln.

Wenn die Beamtinnen und Beamten Einzelpersonen anhalten, führen sie die Entscheidung für das Herausgreifen einer bestimmten Person häufig auf ein „Bauchgefühl" oder eine „Intuition" zurück. Dieses bzw. diese gründet sich wahrscheinlich auf eine Kombination aus Sachverstand und früheren Erfahrungen, aber auch ein bewusstes oder unbewusstes Vorurteil der Beamtin oder des Beamten kann sich darin widerspiegeln. Um unrechtmäßiges Profiling zu vermeiden, sollten die Beamtinnen und Beamten darüber nachdenken, ob ihre Entscheidung durch objektive Informationen gerechtfertigt ist. Ein „Bauchgefühl" ist kein angemessener oder objektiver Grund für die Kontrolle und Durchsuchung einer Person oder den Verweis einer Person an eine gründlichere Grenzkontrolle.

28 Europarat, Ministerkomitee (2001), Empfehlung Rec(2001)10 des Ministerkomitees an die Mitgliedstaaten über den Europäischen Kodex für die Polizeiethik, 19. September 2001.

29 Ebenda, Randnummer 40.

2.2.2. Eindeutige Anweisungen für Beamtinnen und Beamte

Praktische, verständliche und einsatzfähige Anweisungen sind von besonderer Bedeutung, wenn es darum geht, Strafverfolgungsbeamten im Vollzugsdienst und Grenzschutzbeamtinnen und -beamten dabei zu helfen, unrechtmäßiges Profiling zu vermeiden. Anweisungen können viele Formen haben: Sie können Rechtsvorschriften beigefügt, von Strafverfolgungs- und Grenzschutzbehörden selbst ausgegeben oder täglich von leitenden Beamtinnen und Beamten erteilt werden. Beispiele aus der Praxis, die zeigen, was in bestimmten Situationen zu tun ist, dürften wirkungsvoller sein als eine Erläuterung der Vorschriften und Verfahren.

Beamtinnen und Beamte in Führungspositionen müssen das Personal darüber informieren, dass die tatsächliche oder vermutete Rasse, die ethnische Herkunft, das Geschlecht, die sexuelle Ausrichtung, die Religion oder ein anderer verbotener Diskriminierungsgrund nicht der ausschlaggebende Faktor für die Einleitung von Maßnahmen der Strafverfolgung oder des Grenzmanagements gegen eine Person sein kann. Die Klärung der Frage, wann und wie persönliche Merkmale herangezogen werden können, kann dazu beitragen, das Risiko unterschiedlicher Auslegungen sowie der Abhängigkeit von Stereotypen und Vorurteilen zu verringern. Die Vorgaben sollten außerdem Fragen im Zusammenhang mit dem Schutz der Privatsphäre und dem Datenschutz abdecken.

Tabelle 3 zeigt einige Arten von Vorgaben, die verwendet werden können, und wichtige Funktionen, die berücksichtigt werden sollten.

Tabelle 3: Arten und Merkmale von Vorgaben sowie Beteiligung von Interessenträgern

Arten von Vorgaben	Merkmale von Vorgaben	Beteiligung von Interessenträgern

• Standardarbeitsanweisungen (Standard Operating Procedures)
• Verhaltensregeln
• regelmäßige Anweisung durch leitende Beamte
	• detailliert und spezifisch
	• Abdeckung aller Tätigkeiten, bei denen voreingenommenes Profiling auftreten kann:
	  ◦ Kontrolle und Durchsuchung
	  ◦ Festnahmen
	  ◦ Grenzkontrollen
	  ◦ Gewaltanwendung usw.
		• Vorgaben mit anderen Interessenträgern entwickeln
		• Vorgaben für Gemeinschaften bereitstellen
		• Rückmeldungen der Gemeinschaften zu den Vorgaben fördern

Quelle: *FRA, 2018*

Fallstudie

Verhaltenskodex und Botschafter-Ansatz (niederländische Polizei)

Die niederländische Polizei hat gemeinsam mit zivilgesellschaftlichen Organisationen wie Amnesty International einen Verhaltenskodex entwickelt, in dem die vier Grundsätze einer professionell durchgeführten Kontrolle beschrieben werden:

☑ rechtmäßige und gerechtfertigte Auswahl von Personen

☑ Begründung der Kontrolle und Durchsuchung

☑ Professionelle Kommunikation

☑ Beamtinnen und Beamte, die über ihre Vorgehensweisen nachdenken und sich gegenseitig Rückmeldung geben

Die Änderung von Vorgehensweisen, die nicht als problematisch wahrgenommen werden, wie etwa die Praxis der proaktiven Polizeiarbeit, die zu Ethnic Profiling führen kann, ist schwierig. Die Polizei in Amsterdam hat einen Bottom-up-Ansatz entwickelt, an dem Beamtinnen und Beamte vor Ort (Botschafter) in den Teams mitwirken, die von ihren Managern

und Ausbildern unterstützt werden. Der erste Schritt soll sensibilisieren, indem die Auswirkungen der proaktiven Kontrollen auf die betroffenen Personen gezeigt und erörtert werden und ein gerechter und wirksamer alternativer Rahmen eingeführt wird. Der zweite Schritt besteht darin, dass die Beamtinnen und Beamten diese neue Vorgehensweise umsetzen.

Weitere Informationen in niederländischer Sprache können Sie der Website der Polizei entnehmen.

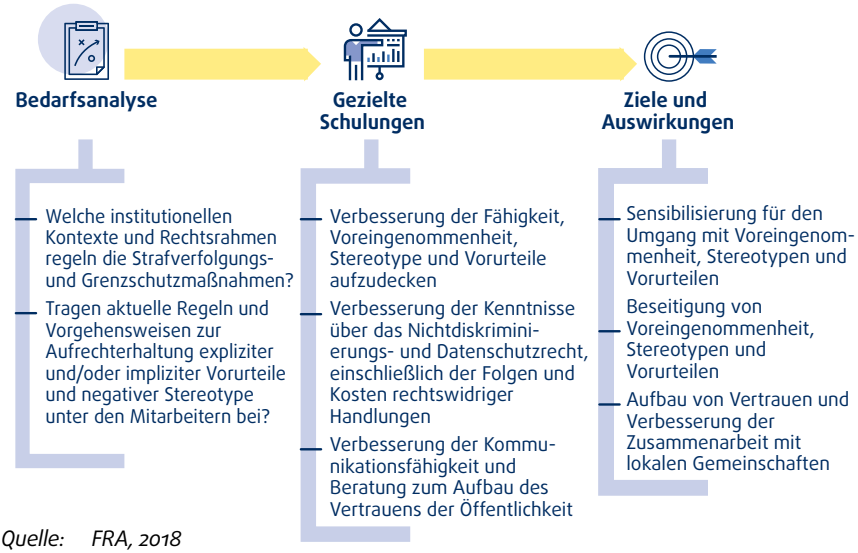
2.2.3. Gezielte Schulungen

Die Aus- und Fortbildung von Polizei- und Grenzschutzbeamtinnen und -beamten ist ein weiteres wichtiges Instrument, um das Risiko eines unrechtmäßigen Profilings zu minimieren. Es gibt viele verschiedene Arten von Schulungen, die in verschiedenen Phasen der Laufbahn einer Beamtinnen oder eines Beamten stattfinden können, beispielsweise im Rahmen der Grundausbildung, Fortbildung und der fortlaufenden beruflichen Weiterbildung. Unabhängig von der Art sollten die Schulungsmodule die Organisationskultur berücksichtigen und Kurse anbieten, die Strategien zur Ablösung und Bekämpfung von Stereotypen beinhalten. Schließlich ist es entscheidend, die Wirkung der Schulung zu beurteilen, um zu überwachen, wie sie dazu beigetragen hat, die Wahrnehmung der Beamtinnen und Beamten zu verändern und ihre Vorgehensweise zu verbessern, und um Lücken zu ermitteln, die weitere Schulungen erfordern. Abbildung 6 hebt einige Punkte hervor, die bei der Entwicklung gezielter Schulungen zu berücksichtigen sind.

Bestimmte Arten von Aus- und Fortbildungsmaßnahmen für Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte sind in einigen Ländern bereits etabliert, z. B. in Form von Schulungen zu Diversität oder zur Sensibilisierung. Bei Schulungen zu Diversität geht es um persönliche Gefühle über ethnische Zugehörigkeit, Unterschiede und Stereotype sowie die Art und Weise, wie diese unser tägliches Leben beeinflussen. In einigen Kursen zu Diversität wird jedoch nicht unbedingt auf Diskriminierung eingegangen. In manchen Studien wird argumentiert, dass Schulungen zu Kultur und Diversität Unterschiede sogar noch hervorheben und verstärken, wodurch sie die Stereotypisierung erhöhen, anstatt sie zu verringern.[30] Schulungen zur kulturellen Sensibilisierung (im Gegensatz zu Schulungen zu Diversität im Allgemeinen) zielen darauf ab, Polizei- und Strafverfolgungsbeamtinnen und -beamte

30 Wrench, J. (2007).

Abbildung 6: Prozess und Ziele bei der Entwicklung gezielter Schulungen



Quelle: *FRA, 2018*

über die Kultur bestimmter ethnischer Gruppen zu informieren, denen sie häufig begegnen, mit denen sie jedoch nicht vertraut sind. In diesen Schulungen werden Verhaltensregeln vermittelt, und die Teilnehmerinnen und Teilnehmer lernen, was Höflichkeit aus der Sicht verschiedener ethnischer, religiöser oder nationaler Gruppen bedeutet. Aus- und Fortbildungsmaßnahmen im Bereich der kulturellen Sensibilisierung sind am wirksamsten, wenn sie mit Unterstützung und Beteiligung von Menschen aus den betreffenden Gemeinschaften entwickelt und durchgeführt werden.

Fallstudie

Schulung zu rechtmäßigem Profiling

Schulungen zu Profiling für Polizeibeamte (Italien)

Die italienische Beobachtungsstelle für den Schutz vor diskriminierenden Handlungen (*Osservatorio per la sicurezza contro gli atti discriminatori*) hat 2014 ein Schulungsmodul zum Ethnic Profiling für Polizeibeamtinnen und -beamte und Polizeischülerinnen und schüler eingeführt. Dabei geht es vor

allem um angenommene Vorurteile, die das Profiling beeinflussen können, die Folgen für die Effizienz der polizeilichen Tätigkeiten und die negativen Auswirkungen auf die Beziehungen zu Gemeinschaften. Bisher haben rund 5 000 Personen an dem Schulungsmodul teilgenommen. Seit 2017 steht auch ein E-Training-Modul für Auffrischungskurse bei der Polizei zur Verfügung.

Weitere Informationen finden Sie auf der Website der italienischen Nationalpolizei.

Instrument für Grundrechte bei der Aus- und Fortbildung von Grenzschutzbeamtinnen und -beamten (EU)

Im Gemeinsamen zentralen Lehrplan (CCC) für europäische Grenzschutzbeamte wird der Mindeststandard der Fähigkeiten und Kenntnisse festgelegt, die jede europäische Grenzschutzbeamtin und jeder europäische Grenzschutzbeamte besitzen muss. Er enthält Kapitel über Soziologie und die Grundrechte. Außerdem gibt es spezifische Abschnitte über Nichtdiskriminierung (1.5.4) und Ethnic Profiling (1.7.10), die von den Ausbilderinnen und Ausbildern genutzt werden können. Der Gemeinsame zentrale Lehrplan weist auf mögliche Risiken im Zusammenhang mit Vorurteilen, Rassismus, Rassendiskriminierung, Fremdenfeindlichkeit, Islamfeindlichkeit, Homophobie und anderen damit zusammenhängenden Formen der Intoleranz hin, die bei der Durchführung von Profiling auftreten können. Die aktualisierte Version des Lehrplans aus dem Jahr 2017 enthält Abschnitte zu neuen Kompetenzen, insbesondere im Bereich der Grundrechte.

Darüber hinaus entwickelte Frontex in Absprache mit Hochschulen und internationalen Organisationen ein Schulungshandbuch (siehe Frontex, 2013). Darin finden die Ausbilderinnen und Ausbilder Methoden, mit denen das Wissen und die Fähigkeiten von Grenzschutzbeamtinnen und -beamten im Bereich der Grundrechte und des internationalen Schutzes erweitert werden können. In dem Handbuch wird ausdrücklich auf Profiling hingewiesen, und es werden Grundregeln für die Vermeidung von Diskriminierung festgelegt. Schulungen werden regelmäßig durchgeführt. Es gibt jedoch keinen dauerhaften Mechanismus, um die Erreichung der Ausbildungsziele zu bewerten.

Weitere Informationen: siehe Frontex (2012).

Studientage zum Thema Profiling für leitende Beamtinnen und Beamte (Belgien)

Im Jahr 2015 organisierte das Centre for Policing and Security (CPS) in Gent (Belgien) unter Beteiligung der belgischen Gleichstellungsstelle (Unia) einen Studientag zum Thema Ethnic Profiling (*Profilage ethnique: l'égalité sous pression?*). Dabei wurden verschiedene Aspekte des Themas behandelt, darunter die Fragen, ob und wie Polizeibeamtinnen und -beamte mit Migrationshintergrund die Beziehungen zu den Gemeinschaften ethnischer Minderheiten verbessern können, wie oft Polizeibeamtinnen und -beamte Ethnic Profiling einsetzen und wie es bewertet wurde.

Im Jahr 2016 organisierte Unia zwei Studientage für leitende Polizeibeamtinnen und -beamte aus dem Norden von Brüssel, um für Ethnic Profiling zu sensibilisieren und zum Nachdenken über Profiling durch Beamtinnen und Beamte im Vollzugsdienst anzuregen. Polizeibeamtinnen und -beamte aus Spanien und dem Vereinigten Königreich stellten einem Publikum aus Strafverfolgungsbeamtinnen und -beamten, Forscherinnen und Forschern sowie Nichtregierungsorganisationen Beispiele für bewährte Verfahren vor. Insbesondere zeigten sie, dass durch eine Reduzierung von Profiling auf Basis der ethnischen Herkunft die Zahl der erfolgreichen Festnahmen gesuchter Personen anstieg. Dies sei durch korrekte Aufzeichnung jeder Kontrolle sowie durch die Gewährleistung der Transparenz hinter den Motiven für die Kontrollen möglich geworden. Ziel der Schulung war es, ein gemeinsames Verständnis von Ethnic Profiling zu entwickeln, um die künftige Entwicklung der Forschung zu den Maßnahmen zu fördern, die derzeit von der Polizei in diesem Bereich angewandt werden.

Weitere Informationen: siehe Belgien (2015 und 2017).

In der Aus- und Fortbildung sollten Vorurteile und Stereotype behandelt werden, die unter Umständen in den Strafverfolgungs- und Grenzschutzbehörden selbst vorhanden sind. Bevor eine Schulung zur Vermeidung von unrechtmäßigem Profiling durchgeführt wird, sollten der breitere institutionelle Kontext und die bestehenden internen Strategien untersucht werden, z. B. die vorhandenen Beschwerdemechanismen und der „Kodex der Verschwiegenheit" unter den Kolleginnen und Kollegen. Die Lehrpläne sollten auf Vorurteile und Stereotype, die in Handlungen der Polizei

wie Kontrollen und Durchsuchungen, Festnahmen und Inhaftnahme integriert sind, sowie auf Gewaltanwendung eingehen.

Leitende Beamtinnen und Beamte und solche in Positionen der mittleren Ebene spielen eine Schlüsselrolle beim Erfolg der Aus- und Fortbildung – einerseits als Teilnehmerinnen bzw. Teilnehmer und andererseits, indem sie der Ausbildung Bedeutung beimessen.[31] Als Teilnehmer bzw. Teilnehmerinnen können leitende Beamtinnen und Beamte neue Verfahren und Fertigkeiten erlernen, die sie an die Beamtinnen und Beamten im Außendienst weitergeben können. Die Organisationskultur, die größtenteils von den Beamtinnen und Beamten der oberen Führungsebene festgelegt wird, hat erhebliche Auswirkungen auf das tägliche Verhalten der Polizei- und Grenzschutzbeamtinnen und -beamten, einschließlich der Art und Weise, wie sie sich gegenüber der Öffentlichkeit verhalten.

Die leitenden Beamtinnen und Beamten können auch dafür sorgen, dass die Schulung positiv gesehen wird. Die Mitarbeiterinnen und Mitarbeiter in Führungspositionen können durch ihr Verhalten das Interesse und Engagement in Bezug auf die Schulungen erheblich beeinflussen, z. B. durch die Art und Weise, wie sie gegenüber den Beamtinnen und Beamten über den Zweck der Schulung sprechen, und ob sie ihnen mitteilen, ob sie nach dem Zufallsprinzip ausgewählt wurden oder weil sie als „problematisch" angesehen werden. Die Schulungen sind wirkungsvoller, wenn die Beamtinnen und Beamten dazu animiert werden, sich aktiv an den Schulungsprogrammen zu beteiligen und für eine Verhaltensänderung bei ihrer täglichen Arbeit offen zu sein.[32]

Im Anschluss an eine Schulung sollte diese bewertet werden, und ihre Auswirkungen in Bezug auf Sensibilisierung und Verhaltensänderungen sollte beurteilt werden.

31 Siehe Europäische Kommission (2017b).

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

Im Fokus: Leitsätze der Aus- und Fortbildung

Spezielle Schulungen sind für eine rechtmäßige Nutzung des Profilings entscheidend. Die Europäische Kommission hat einige zentrale Leitsätze dazu entwickelt, wie wirksame und hochwertige Schulungen im Hinblick auf Hassverbrechen sichergestellt werden können. Die gleichen Grundsätze gelten für Schulungen zu rechtmäßigem Profiling.

Schulungen zu Hassverbrechen für Strafverfolgungs- und Justizbehörden: 10 zentrale Leitsätze

Sicherstellen von Wirkung und Nachhaltigkeit:

☑ Aus- und Fortbildung in einen umfassenderen Ansatz zur Bekämpfung von Diskriminierung integrieren;

☑ Methodik zur Deckung des Schulungsbedarfs entwickeln.

Ermittlung von Zielen und Aufbau von Synergien:

☑ Programme auf die Mitarbeiter zuschneiden;

☑ Strukturiert mit der Zivilgesellschaft zusammenarbeiten.

Auswahl der richtigen Methodik:

☑ Verschiedene Methoden kombinieren;

☑ Ausbilder ausbilden.

Vermittlung hochwertiger Inhalte:

☑ Ausbildungslehrplan mit hochwertigen Inhalten zusammenstellen;

☑ Ausbildungsmodule zur Bekämpfung von Diskriminierung entwickeln.

Überwachung und Bewertung der Ergebnisse:

☑ Ausbildung mit den Verfahren der Leistungsüberprüfung verknüpfen;

☑ Regelmäßige Überwachung und Bewertung der Ausbildungsmethoden sicherstellen.

Weitere Informationen: siehe Europäische Kommission (2017a).

Durch Aus- und Fortbildung allein können die impliziten Vorurteile der Beamtinnen und Beamten jedoch nicht wirksam bekämpft werden. Wir brauchen eine Veränderung des institutionellen Denkens. Die Behörden müssen daher vielfältige Maßnahmen in Betracht ziehen, um persönlichen und institutionellen Vorurteilen entgegenzuwirken (siehe Fallstudie).

Fallstudie

Bekämpfung des „institutionellen Rassismus" bei der Polizei

Nachdem die Untersuchung der rassistisch motivierten Ermordung von Stephen Lawrence im Vereinigten Königreich Anlass zur Sorge über die Bedeutung des ethnischen Hintergrunds bei polizeilichem Fehlverhalten gegeben hatte, leitete die Regierung des Vereinigten Königreichs eine umfassende Untersuchung ein, um die „Lehren aus der Untersuchung und Verfolgung rassistisch motivierter Straftaten" zu ermitteln.

In dem 1999 veröffentlichten Bericht über die Untersuchung wird betont, wie der „institutionelle Rassismus" bei der Metropolitan Police, einschließlich der Unterschiede bei der Anzahl der Kontrollen und Durchsuchungen, die betroffenen Gemeinschaften beunruhigt. Die Empfehlungen der Untersuchung, die von Schulungen zur Rassismus-Sensibilisierung bis zur Meldung und Aufzeichnung von Vorfällen reichten, wurden durch eine allgemeine Forderung nach mehr Offenheit und Rechenschaftspflicht sowie nach einer Wiederherstellung des Vertrauens bei der Polizei ergänzt.

Überprüfungen, die 2009, also zehn Jahre nach der Untersuchung, veröffentlicht wurden, zeigten Verbesserungen im Umgang mit Gemeinschaften ethnischer Minderheiten und bei der Untersuchung rassistisch motivierter Straftaten. Es wurde jedoch auch festgestellt, dass die Wahrscheinlichkeit von Kontrollen und Durchsuchungen bei schwarzen Menschen nach wie vor deutlich höher ist als bei weißen Menschen.

Weitere Informationen: siehe Vereinigtes Königreich, Home Office (1999), Vereinigtes Königreich, Equality and Human Rights Commission (2009), und Vereinigtes Königreich, House of Commons Home Affairs Committee (2009).

2.2.4. Begründete Verdachtsmomente: effiziente Nutzung von Erkenntnissen und Informationen

Polizei- und Grenzschutzbeamtinnen und -beamte, die eine einzelne Person für eine Kontrolle herausgreifen, stützen ihre Entscheidung in der Regel auf eine Kombination verschiedener Faktoren. Dabei kann es sich sowohl um eher „objektive" Informationen wie beispielsweise spezifische Erkenntnisse, bestimmte Verhaltensweisen, die Kleidung oder von dieser Person mitgeführte Gegenstände handeln als auch um „subjektives" auf Erfahrungen beruhendes Wissen.

All diese Faktoren können auf illegale Aktivitäten hindeuten. Die sich daraus ergebenden Informationen müssen jedoch richtig kombiniert und mit Bedacht genutzt werden. Untersuchungen zeigen, dass es den Beamtinnen und Beamten durchaus schwerfallen kann, in der Praxis zwischen objektiven und subjektiven Faktoren zu unterscheiden. Diese Problematik wird auch in dem nachstehenden Beispiel deutlich.

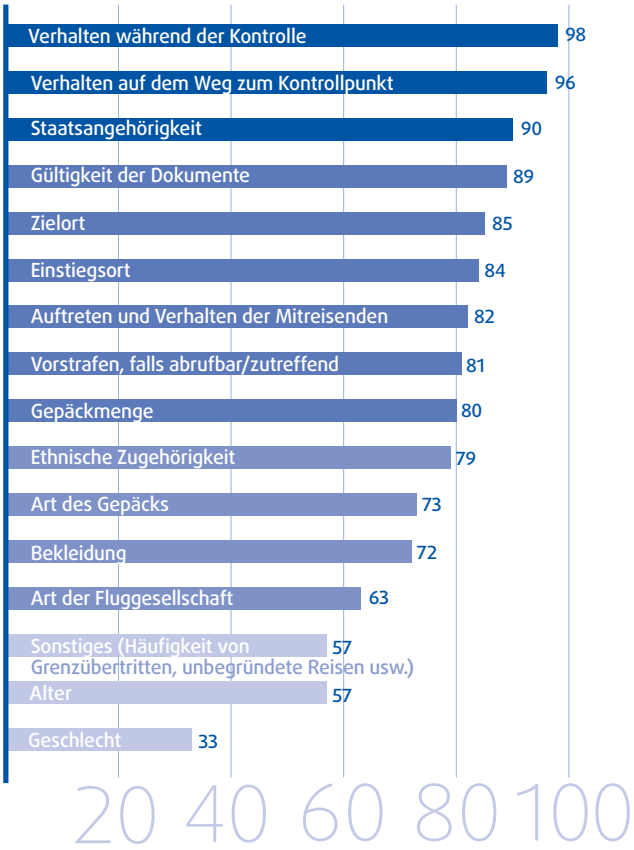
Beispiel

„Diese Einschätzung ist sehr subjektiv. Ausschlaggebend ist der Eindruck, den man von der Person und dem Fall hat. Eine weitere wichtige Rolle spielen aber auch offensichtliche Diskrepanzen in ihren Aussagen sowie Unterschiede zwischen ihren Aussagen und den Aussagen ihres Bürgen, ihren Papieren oder den Gegenständen, die sie mit sich führt. Es gibt also gewisse Anhaltspunkte, aber diese [Dinge] allein würden noch nicht zu einer negativen Entscheidung bezüglich dieser Person führen. Die Beamtin bzw. der Beamte muss sich vielmehr ein Gesamtbild verschaffen und dabei alle Faktoren berücksichtigen."

(Beamter der Einwanderungsbehörde an einem großen britischen Flughafen)

Weitere Informationen: siehe FRA (2014a), S. 46.

Abbildung 7: Als hilfreich oder sehr hilfreich erachtete Indikatoren, die den Beamtinnen und Beamten bereits vor der Gesprächsaufnahme bei der frühzeitigen Erkennung von Personen helfen, die versuchen könnten, auf irregulärem Weg in das Land zu gelangen (in %)



Anmerkung: Zwischen 206 und 216 der insgesamt 223 Befragten haben gültige Angaben gemacht. Die Antworten der Befragten, die zu einem dieser Punkte keine Angaben gemacht haben, wurden aus der Berechnung des jeweiligen Ergebnisses ausgeschlossen. Die Anzahl der Antwortausfälle liegt je nach Thema zwischen sieben und 17 Personen.

Quelle: FRA, Umfrage unter Grenzschutzbeamtinnen und -beamten, 2012 (Frage 17)

Im Fokus: Identifizierung von Personen, die versuchen, irregulär in ein Land zu gelangen

Eine im Jahr 2012 an mehreren Großflughäfen durchgeführte Studie der FRA zeigte, dass Grenzschutzbeamtinnen und -beamte bei der Entscheidung, ob eine Person versucht, irregulär in das Land einzureisen, eine Reihe von Faktoren berücksichtigen. Wie aus Abbildung 7 hervorgeht, handelt es sich dabei häufig um eine Kombination verschiedener „objektiver" Kriterien – beispielsweise das Verhalten der Person auf dem Weg zum Kontrollpunkt und bei der Kontrolle selbst, die Art und Menge des mitgeführten Gepäcks oder die Gültigkeit der Reisedokumente – gepaart mit den persönlichen Erfahrungen der Beamtinnen und Beamten, die sie in früheren Grenzkontrollen gewonnen haben.

Den Grenzschutzbeamtinnen und -beamten zufolge ist das Verhalten während der Kontrolle oder bei der Annäherung zum Kontrollpunkt der hilfreichste Indikator zur Erkennung von Personen, die versuchen, irregulär in das Land einzureisen. Faktoren wie die Staatsangehörigkeit und die ethnische Zugehörigkeit, die in den Bereich des diskriminierenden Profiling fallen könnten, wurden jedoch ebenfalls als bedeutsam erachtet.

Als weiterer hilfreicher Anhaltspunkt wurde die Kleidung der betreffenden Person(en) genannt. Dies macht deutlich, wie scheinbar „objektive" Informationen in der Praxis durchaus vorurteilsbehaftet sein können. Bestimmte Arten von Kleidung könnten mit spezifischen Risikoprofilen in Verbindung gebracht werden. Zum Beispiel tragen Opfer von Menschenhandel, die eine bestimmte Staatsangehörigkeit haben, typischerweise spezielle Arten von Kleidung. Die Kleidung kann jedoch auch darauf hindeuten, dass eine Person einer bestimmten ethnischen oder religiösen Gruppe angehört. Selbst wenn ausreichend andere Gründe vorliegen, die eine Kontrolle in der zweiten Kontrolllinie rechtfertigen, können insbesondere Menschen, die sich stark mit ihrer ethnischen oder religiösen Zugehörigkeit identifizieren, die früher bereits negative Erfahrungen gemacht haben oder die von den Grenzschutzbeamtinnen und -beamten keine angemessene Erklärung erhalten, diese Behandlung als diskriminierend empfinden.

Weitere Informationen: siehe FRA (2014a). Hinweise zu den Profilen der Opfer von Menschenhandel finden Sie in Frontex (2017).

Eine gute Aufklärung über Verhaltensmuster oder Ereignisse kann die Objektivität beim Profiling erhöhen. Diese könnte sich auf kriminelle Aktivitäten oder – im Zusammenhang mit dem Grenzmanagement – auf die irreguläre Migration oder grenzüberschreitende Kriminalität beziehen. Wenn Strafverfolgungs- und Grenzschutzmaßnahmen auf konkreten, zeitlich relevanten Erkenntnissen beruhen, beispielsweise auf Informationen zu einer bestimmten Person und/oder einem spezifischen Kontext, sind sie mit größerer Wahrscheinlichkeit objektiv und basieren mit geringerer Wahrscheinlichkeit auf Stereotypen.

Neben solchen Erkenntnissen und objektiven Faktoren können Informationen zu bestimmten Schutzmerkmalen wie die tatsächliche oder vermutete Rasse, die ethnische Herkunft, die Staatsangehörigkeit, das Geschlecht oder die Religionszugehörigkeit unter bestimmten Umständen ebenfalls als rechtmäßige Komponente für die Profiling-Bewertung herangezogen werden. Damit diese Informationen rechtmäßig verwendet werden können, müssen sie gesetzlich geregelt sein, den Wesensgehalt der betroffenen Rechte und Freiheiten achten, verhältnismäßig (d. h. einen Interessenausgleich gewährleisten) und notwendig sein (d. h. es sollten keine weniger restriktiven Mittel zur Verfügung stehen). Bei Verdachtsmomenten, die sich aus anderen Faktoren als den Schutzmerkmalen ergeben, müssen die Beamtinnen und Beamten hinreichend begründen können, warum sie eine bestimmte Person im Vergleich zu anderen Menschen anders behandeln. Der genannte Grund muss sich konkret auf die jeweilige Person beziehen, wie in dem nachstehend aufgeführten Beispiel.

Beispiel

Den Zeuginnen und Zeugen zufolge trug der Verdächtige bei einem Raubüberfall rote Sportschuhe und eine schwarze Baseballkappe; er ist zwischen 1,60 m und 1,70 m groß und mutmaßlich chinesischer Herkunft. Unter diesen Umständen könnten die Strafverfolgungsbehörden den ethnischen Hintergrund rechtmäßig als einen Faktor heranziehen, der – in Kombination mit weiteren Erkenntnissen – eine maßgebliche Rolle bei der Feststellung spielt, ob eine Person zu den potenziellen Verdächtigen zählt.

Im Fokus: Detaillierte Verdächtigenbeschreibungen

Eine gute Verdächtigenbeschreibung kann das Risiko eines unrechtmäßigen Profilings mindern. Die Beschreibung eines Verdächtigen enthält Angaben zur Person wie Haut-, Haar- und Augenfarbe, Körpergröße und gewicht

sowie zur Kleidung. Diese Informationen stammen entweder vom Opfer der Straftat selbst oder von Zeuginnen und Zeugen, oder sie werden aus anderen spezifischen Erkenntnissen abgeleitet. Eine gute Verdächtigenbeschreibung kann den Beamtinnen und Beamten als Grundlage für Kontroll- und Durchsuchungsmaßnahmen zur Festnahme von Verdächtigen oder für die Auswahl bestimmter Personen an der Grenze für eine weitere Kontrolle in der zweiten Kontrolllinie dienen.

Wenn die Beamtinnen und Beamten der Strafverfolgung jedoch nur eine zu allgemeine Verdächtigenbeschreibung erhalten, die Rasse, ethnische Zugehörigkeit oder ähnliche Merkmale umfasst, sollten sie diese Beschreibung nicht als Grundlage für ihre Einsätze verwenden. In solchen Fällen besteht eine hohe Wahrscheinlichkeit, dass eine große Zahl unschuldiger Personen angehalten würde, die zufällig ebenfalls diese Merkmale aufweisen. Die Beamtinnen und Beamten sollten sich für ihre Untersuchungen vielmehr um konkrete operative Erkenntnisse bemühen.

Weitere Informationen: siehe Europäische Kommission (2017b).

Objektiv erscheinende Informationen müssen nicht unbedingt vorurteilsfrei sein. Wie das nachstehende Beispiel zeigt, können scheinbar objektive Faktoren, wie die Zeit, das Datum oder der Ort, stellvertretend für verbotene Diskriminierungsgründe wie die tatsächliche oder vermutete Rasse, die nationale Herkunft, das Geschlecht, die sexuelle Orientierung oder die Religion herangezogen werden.

Beispiel

Am Freitag Mittag wird im Gebiet X eine Kontroll- und Durchsuchungsmaßnahme durchgeführt. Der gewählte Zeitpunkt deckt sich jedoch genau mit dem Mittagsgebet, der wichtigsten Gebetszeit der Muslimas und Muslime. Da sich in der unmittelbaren Nähe von Gebiet X eine Moschee befindet, könnten die vermeintlich objektiven Faktoren Zeit, Datum und Ort in Wirklichkeit vorgeschoben sein, um Personen aufgrund des eigentlich verbotenen Diskriminierungsgrunds der Religionszugehörigkeit anzuhalten und zu durchsuchen.

Ebenso kann die Feststellung bestimmter verdächtiger Verhaltensweisen wie ein objektiver Weg erscheinen, mögliches Fehlverhalten zu erkennen. Die Beamtinnen und Beamten können das Verhalten einer Person jedoch unterschiedlich auslegen, je nachdem, welche anderen Merkmale ihnen noch auffallen. Untersuchungen zeigen, dass es beim Fachwissen der einzelnen Beamtinnen und Beamten und der Auslegung der gewonnenen Erkenntnisse große Unterschiede geben kann und diese Informationen häufig nicht den tatsächlichen Straftatenmustern entsprechen.[33]

Wenn den Beamtinnen und Beamten rechtzeitig detaillierte Erkenntnisse zur Verfügung gestellt werden, beispielsweise bei Einsatzbesprechungen zu Beginn jeder Schicht, dürfte die Ermessensfreiheit verringert werden, und die Beamtinnen und Beamten verfügen über Vorgaben, wie sie ihre Befugnisse konkreter bei den aktuellen Straftatenmustern und ermittelten Sicherheitsproblemen einsetzen können. Eine mögliche Voreingenommenheit wird dadurch verringert. Die Qualität und die Nutzung von Erkenntnissen, die sich auf verhaltensbedingte Faktoren oder bestimmte Informationen stützen, werden am wirksamsten verbessert, wenn dies mit einer verstärkten Aufsicht und Überwachung einhergeht, wie die Beamtinnen und Beamten von ihren Befugnissen Gebrauch machen.

Fallstudie

Gewährleistung der Objektivität beim Profiling

Einsatzbesprechungen vor Schichtbeginn (EU)

Eine Empfehlung aus dem Schengen-Katalog sieht vor, dass die bzw. der diensthabende Beamtin/Beamte vor jedem Schichtbeginn Informationen über Risikoindikatoren und Risikoprofile erteilt. Einander überlappende Schichten lassen beim Schichtwechsel genügend Zeit für Einsatzbesprechungen und den Informationsaustausch zwischen den Beamtinnen und Beamten.

Weitere Informationen: siehe Rat der Europäischen Union (2009).

Das SDR-Schulungsprogramm (Niederlande)

Das Schulungsprogramm SDR („Search, Detect and React“) zielt darauf ab, Straftaten oder terroristische Handlungen bereits im Vorfeld zu

33 Vereinigtes Königreich, National Policing Improvement Agency (NPIA) (2012).

verhindern, indem die Fähigkeiten des Sicherheitspersonals in Bezug auf das verhaltensbasierte Profiling verbessert werden. Das bedeutet, dass die Aufmerksamkeit nicht mehr auf unveränderlichen Eigenschaften wie der Hautfarbe liegt, sondern dass wieder das Verhalten einer Person im Mittelpunkt steht, um fundierte Entscheidungen bezüglich einer polizeilichen Maßnahme zu treffen. Da die Indikatoren für verdächtiges Verhalten vom Kontext abhängen, sind die Schulungsmaßnahmen an die jeweilige Umgebung angepasst. Die Vorstellung einer allgemeingültigen Lösung wird dabei abgelehnt. Wenn die Beamtinnen und Beamten ein entsprechendes Verhaltensmuster erkannt haben, müssen sie „sensibel" reagieren. In den meisten Fällen führen sie ein formloses Gespräch mit der verdächtigen Person, ohne dabei von formalen polizeilichen Befugnissen Gebrauch zu machen. Das Programm umfasst sowohl theoretischen als auch praktischen Unterricht.

Weitere Informationen können Sie der Website der SDR Academy entnehmen.

Das Tool „Authorised Professional Practice" (APP) für Kontrollen und Durchsuchungen (Vereinigtes Königreich)

Das College of Policing des Vereinigten Königreichs hat praktische APP-Leitlinien entwickelt, die verschiedene Aspekte der Polizeiarbeit behandeln. In den APP-Leitlinien zu Kontrollen und Durchsuchungen wird erklärt, was genau eine Kontroll- und Durchsuchungsmaßnahme ist, warum die damit einhergehenden Befugnisse korrekt angewendet werden müssen und wodurch sich eine rechtmäßige Kontrollmaßnahme auszeichnet. Die Rechtmäßigkeit und Wirksamkeit von Kontrollen und Durchsuchungen wird demnach durch folgende Aspekte gewährleistet:

- **Fairness**: Die Entscheidung einer Beamtin oder eines Beamten, eine Person anzuhalten und zu durchsuchen, darf ausschließlich auf angemessenen und objektiven Faktoren basieren. Eine Person darf niemals ausschließlich oder hauptsächlich aufgrund geschützter Merkmale oder Faktoren wie Vorstrafen angehalten werden.
- **Legalität**: Die Kontrolle und Durchsuchung von Personen muss auf einer rechtlichen Grundlage beruhen, die gesetzeskonform angewendet wird.
- **Professionalität**: Während Kontroll- und Durchsuchungsmaßnahmen müssen die Beamtinnen und Beamten die Verhaltensregeln ihres

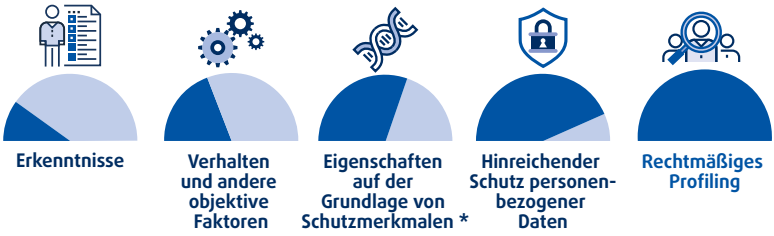
Berufsstands, insbesondere den Kodex der Berufsethik, beachten, effektiv mit den Menschen kommunizieren und sie mit Würde und Respekt behandeln.

- **Transparenz**: Jede einzelne Begegnung muss genau aufgezeichnet werden. Dabei müssen sowohl die wirksame Aufsicht und Überwachung der Maßnahmen als auch die öffentliche Kontrolle sichergestellt werden.

Weitere Informationen: siehe Vereinigtes Königreich, College of Policing (2016).

Abbildung 8 zeigt die verschiedenen Faktoren auf, die beim rechtmäßigen Profiling herangezogen werden können; die Kombinationsmöglichkeiten dieser Faktoren hängen dabei vom jeweiligen Fall ab.

Abbildung 8: Kombination von Faktoren

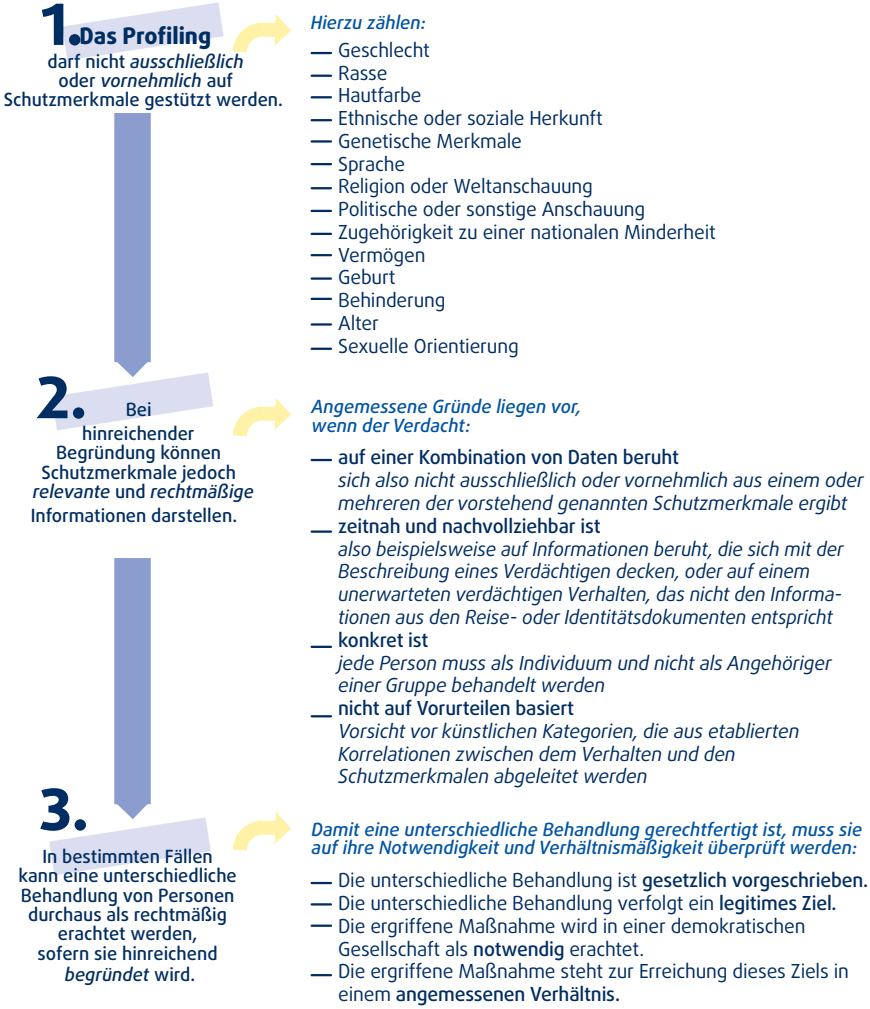


* *Abbildung 9 enthält eine Auflistung der Schutzmerkmale gemäß EU-Recht. Das Profiling sollte niemals ausschließlich oder vornehmlich auf Schutzmerkmale gestützt werden.*

Quelle: *FRA, 2018*

Aus Abbildung 9 geht hervor, wie die verschiedenen Faktoren miteinander kombiniert werden können, um ein diskriminierungsfreies Profiling zu gewährleisten.

Abbildung 9: Elemente eines diskriminierungsfreien Profiling



Anmerkungen: *Die Liste der Schutzmerkmale variiert je nach Mitgliedstaat. Eine Übersicht der Diskriminierungsgründe, die in den Strafgesetzbüchern der einzelnen Mitgliedstaaten enthalten sind, finden Sie in FRA (2018d). Siehe hierzu auch die Website von Equinet, dem Europäischen Netzwerk von Gleichstellungsstellen. Dort sind alle von den nationalen Gleichstellungsstellen abgedeckten Diskriminierungsgründe aufgelistet.*

Quelle: *FRA, 2018*

2.2.5. Formulare zu Kontrollen und Durchsuchungen für das Profiling in der Strafverfolgung

Mithilfe von Formularen zu Kontrollen und Durchsuchungen können die Beamtinnen und Beamten leichter beurteilen, ob die von ihnen vorgenommenen Kontrollen auf angemessenen Gründen beruhen. Zudem ermöglichen sie den leitenden Beamtinnen und Beamten, potenzielle diskriminierende Praktiken bei der Durchführung von Kontrollen und Durchsuchungen durch einzelne Beamtinnen und Beamte zu überwachen. Zwar werden die Formulare manchmal als zu aufwendig empfunden, doch schaffen sie einen Überblick über die durchgeführten Kontrollen und liefern bei entsprechender Sortierung relevante Daten, anhand derer festgestellt werden kann, ob eine Kontrolle rechtmäßig durchgeführt wurde.[34] Dies kann dazu beitragen, die Offenheit und Rechenschaftspflicht gegenüber der Öffentlichkeit zu fördern. Neben Papierformularen können zum Erfassen dieser Informationen auch neue Technologien wie mobile Apps eingesetzt werden.

Im nachstehenden Kasten „Im Fokus" sind einige wichtige Punkte aufgeführt, die bei der Gestaltung von Formularen zu Kontrollen und Durchsuchungen zu beachten sind.

Im Fokus: Wodurch zeichnet sich ein gutes Formular zu Kontrollen und Durchsuchungen aus?

Formulare zu Kontrollen und Durchsuchungen müssen angemessen gestaltet sein, damit sie ihren vorgesehenen Zweck erfüllen. Zunächst einmal bedeutet das Ausfüllen der Formulare einen zusätzlichen Arbeitsaufwand für die Beamtinnen und Beamten. Wenn sie nicht klar gestaltet und ausreichend überschaubar sind, besteht die Gefahr, dass die Beamtinnen und Beamten das Formular nicht vollständig oder nicht sorgfältig genug ausfüllen. Darüber hinaus ermöglichen angemessen gestaltete Formulare das einfache Extrahieren und Zusammenstellen von Daten, die bei der Überwachung und Bewertung von Kontroll- und Durchsuchungsmaßnahmen helfen.

Formulare zu Kontrollen und Durchsuchungen sollten nach Möglichkeit:

- Multiple-Choice-Felder enthalten, da diese schneller ausgefüllt und statistisch leichter verarbeitet werden können;

34 Vereinigtes Königreich, Stop Watch (2011).

- für jedes Element eine umfassende Liste mit Optionen enthalten;
- mehrdeutige Elemente vermeiden;
- leicht verständlich sein, und zwar sowohl für die Beamtinnen und Beamten als auch für die angehaltene Person;
- folgende Punkte enthalten:
  - die Rechtsgründe für die Kontrolle; vorzugsweise einfache Erklärungen anstelle einer Liste von Regeln;
  - Datum, Zeit und Ort der Kontrolle der Person oder des Fahrzeugs;
  - das Objekt der Kontrolle, z. B. Gegenstände, nach denen die Beamtinnen und Beamten suchen;
  - das Ergebnis der Kontrolle;
  - den/die Namen des/der Beamtin(nen) bzw. Beamten, der/die die Kontrolle durchführt/führen, sowie das betreffende Polizeirevier;
  - die persönlichen Informationen zu der kontrollierten Person, wie der Name, die Anschrift oder die Staatsangehörigkeit, können ebenfalls erfasst werden. Die kontrollierte Person kann diese Angaben jedoch verweigern.

Für eine größtmögliche Wirksamkeit sollten die Formulare zum Zeitpunkt der Kontrolle ausgefüllt werden.

Der kontrollierten Person oder dem Fahrer des durchsuchten Fahrzeugs sollte eine Kopie ausgehändigt werden. Im Vereinigten Königreich können die Personen, die für eine Kontrolle angehalten wurden, innerhalb von drei Monaten nach der Kontrolle eine Kopie der entsprechenden Aufzeichnungen anfordern. Dadurch dient das Formular nicht nur für die Polizei als Nachweis der Kontrolle, sondern auch für die kontrollierten Personen.

Weitere Informationen hierzu siehe Vereinigtes Königreich, West Midlands Police (2012), S. 7 und Vereinigtes Königreich, Home Office (2014a).

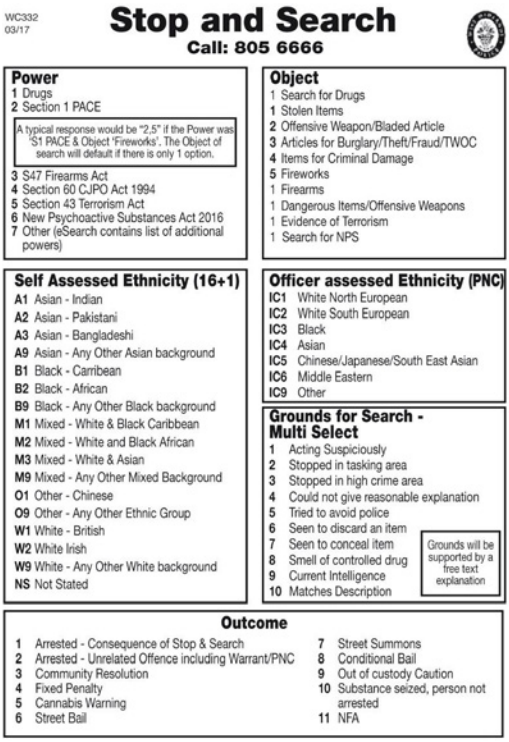
Fallstudie

Formular zu Kontrollen und Durchsuchungen (Vereinigtes Königreich)

Nachstehend ist das von der englischen West Midlands Police verwendete Formular zu Kontrollen und Durchsuchungen abgebildet.

Daraus geht hervor, dass die angehaltene Person dazu aufgefordert wird, sich einer der darin aufgelisteten Kategorien der ethnischen Zugehörigkeit zuzuordnen, wobei auch Optionen wie „Sonstige" („Other") oder „Keine Angabe" („Not stated") verfügbar sind. Die Beamtin oder der Beamte, die bzw. der die Kontrolle durchführt, kann ihre/seine eigene Einschätzung ergänzen, falls sie bzw. er der Selbstauskunft der betroffenen Person nicht zustimmt.

Der im Vereinigten Königreich geltende Verhaltenskodex für die Ausübung der Befugnis zu Kontrollen und Durchsuchungen sieht vor, dass die Beamtinnen und Beamten den zu kontrollierenden Personen erklären, dass die Angaben zur ethnischen Zugehörigkeit erforderlich sind, um ein wahrheitsgetreues Bild der Kontroll- und Durchsuchungsmaßnahmen zu erhalten, die Überwachung ethnischer Gruppen zu verbessern, diskriminierende Praktiken zu bekämpfen und die wirksame Ausübung dieser Befugnisse zu fördern.



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

Weitere Informationen hierzu siehe Vereinigtes Königreich, West Midlands Police (2017a) und Vereinigtes Königreich, Home Office (2014a), S. 19.

Viele Behörden erfassen die Informationen zu den Kontrollen und Durchsuchungen inzwischen nicht mehr in Papierform, sondern setzen verstärkt auf neue Technologien wie mobile Apps, funkgestützte Systeme, mobile Datenterminals oder Laptops. Diese Technologien können den Erfassungsprozess beschleunigen und den bürokratischen Aufwand verringern, bringen gleichzeitig aber auch neue Risiken mit sich, insbesondere im Hinblick auf die algorithmische Nutzung personenbezogener Daten (siehe Kapitel 3).

Fallstudie

Live-Aufzeichnung von Kontroll- und Durchsuchungsmaßnahmen

„eSearch" (West Midlands Police, Vereinigtes Königreich)

Dieses im April 2014 eingeführte System basiert auf dem Szenario, dass die Beamtin oder der Beamte vor Ort eine(n) Mitarbeiter(in) im Kontaktzentrum (Leitstelle) per Anruf kontaktiert. Die Einzelheiten des Kontroll- und Durchsuchungsvorgangs werden in der Leitstelle in Echtzeit protokolliert und in einer Datenbank hinterlegt. Diese Informationen können dann abgerufen und genutzt werden, um die Wirksamkeit von Kontrollen und Durchsuchungen intern und extern zu überprüfen. Mit eSearch wurde die Protokollierung von Kontroll- und Durchsuchungsmaßnahmen grundlegend verändert. Die Aufzeichnungen können in den Polizeisystemen viel schneller eingesehen werden, was nicht nur die Aufklärungsarbeit, sondern auch die Integration dieser Informationen in die operative Polizeiarbeit erleichtert.

Weitere Informationen hierzu siehe Vereinigtes Königreich, West Midlands Police (2014) und Vereinigtes Königreich, West Midlands Police (2016).

Mobile App für Polizeivollzugsbeamte (West Midlands Police, Vereinigtes Königreich)

Im Oktober 2017 wurde eine neue mobile App eingeführt, die Kontrollen und Durchsuchungen beschleunigt und effizienter macht. Mit der eSearch-App können die Beamtinnen und Beamten Details zu Kontrollen auf der Straße direkt über ihr Smartphone erfassen, ohne die Leitstelle kontaktieren zu müssen. Bei jeder Kontrolle wird eine eindeutige Referenznummer vergeben, und der Standort wird automatisch per GPS aufgezeichnet. Es wird erwartet, dass die Zahl der Anrufe in der Leitstelle dank der App um rund 1 000 Anrufe pro Monat zurückgehen wird.

Weitere Informationen: siehe Vereinigtes Königreich, West Midlands Police (2017b).

Die leitenden Beamtinnen und Beamten spielen eine wichtige Rolle, wenn es darum geht, die Rechtmäßigkeit der durchgeführten Kontrollen und Durchsuchungen

sicherzustellen. Das nachstehende Beispiel verdeutlicht, wie die leitenden Beamtinnen und Beamten dabei die Übersicht behalten. Sie sollten außerdem sicherstellen, dass die Zahl der Kontrollen und Durchsuchungen nicht als Leistungskennzahl angesehen wird, die sich auf die Anzahl der durchgeführten Kontrollen stützt.

Fallstudie

Bestätigung der Aufzeichnungen zu Kontrollen und Durchsuchungen (Vereinigtes Königreich)

Seit August 2014 muss jede Aufzeichnung zu einer Kontroll- und Durchsuchungsmaßnahme im Vereinigten Königreich von der oder dem Vorgesetzten der Beamtin/des Beamten, die bzw. der die Kontrolle durchgeführt hat, gegengezeichnet werden. Dabei wird geprüft, ob die Aufzeichnungen den geltenden Standards genügen. Ist dies nicht der Fall, muss die bzw. der meldende Beamtin/Beamtin in der Aufzeichnung eine entsprechende Begründung hinterlegen.

Weitere Informationen: siehe Vereinigtes Königreich, Home Office (2014a).

2.3. Rechenschaftspflicht

Kernpunkte

- Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte sind dafür **verantwortlich**, Profiling gesetzeskonform durchzuführen.
- **Die Erhebung zuverlässiger, genauer und aktueller Daten** zum Profiling ist unabdingbar, um die Rechenschaftspflicht zu gewährleisten.
- **Wirksame Beschwerdemechanismen** können Machtmissbrauch verhindern und dazu beitragen, das Vertrauen der Öffentlichkeit in die Tätigkeit der Polizei- und Grenzschutzbehörden wiederherzustellen bzw. zu stärken.
- **Feedback-Treffen mit Mitgliedern der Öffentlichkeit** dienen dazu, deren Meinungen anzuhören, über Profiling zu sprechen und Rückmeldungen zu Operationen einzuholen, Gelegenheiten für wichtige Lehren zu bieten und das Profiling zu verbessern.

Die Rechenschaftspflicht ist einer der wichtigsten Grundsätze der demokratischen Staatsführung. Ganz allgemein geht es darum, denjenigen Antworten geben zu können, die einen entsprechenden Auskunftsanspruch haben.[35] Die Rechenschaftspflicht betrifft nicht nur die Entscheidungsfindung der oder des Einzelnen, sondern auch die der gesamten Behörde („institutionelle Rechenschaftspflicht"). In ihrer Rolle als öffentliche Bedienstete und Stellen sind Strafverfolgungs- und Grenzschutzbeamtinnen und -beamte sowie deren Behörden der Öffentlichkeit gegenüber für ihre Entscheidungen und Maßnahmen rechenschaftspflichtig. Dazu gehört auch, dass sie gewährleisten müssen, dass das Profiling gesetzeskonform erfolgt.

Die Erhebung zuverlässiger, genauer und aktueller Daten ist unabdingbar, um die Rechenschaftspflicht zu gewährleisten. Da viele der erhobenen Daten personenbezogene Informationen enthalten, müssen sie im Einklang mit den Datenschutzvorschriften und verfahren verarbeitet werden (siehe Kapitel 3).

Checkliste zur Erfüllung der Rechenschaftspflicht

Diese Checkliste gibt einen grundlegenden Überblick über die einzelnen Schritte, die die Strafverfolgungs- und Grenzschutzbehörden ergreifen können, um sicherzustellen, dass sie ihre Rechenschaftspflicht im Hinblick auf die Entscheidungen und Maßnahmen beim Profiling erfüllen. Die in der Liste aufgeführten Schritte können den Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten dabei helfen, ihre Rechenschaftspflicht zu verbessern, sollten von ihnen aber nicht als obligatorisch verstanden werden. Je nach Kontext sind einige der Empfehlungen für die Besonderheiten im Grenzmanagement möglicherweise nicht relevant.

1. Identifizieren

- ☑ Das Problem von unrechtmäßigem Profiling feststellen und **anerkennen**. Vorurteile und Stereotype bestehen und bergen Risiken für alle Beteiligten, einschließlich der Beamtinnen und Beamten und lokalen Gemeinschaften.
- ☑ **Aufgeschlüsselte Daten sammeln und nutzen**: Diese Vorgehensweise ist ein wichtiges Instrument zur Bewertung von Wirksamkeit und Leistung.

35 Bovens, M., Schillermans, T. und Goodlin, R. E. (2014), S. 1-11.

☑ An externen Gremien der Gemeinschaft oder der Zivilgesellschaft mitwirken, um **Feedback** zu Maßnahmen zu erhalten und das Vertrauen in die Einsätze von Beamtinnen und Beamten und Behörden zu stärken.

2. Informationen sammeln

☑ Erfüllung der Rechenschaftspflicht durch **Aufzeichnungen** des Profilings gewährleisten.

☑ Vorbehaltlich der erforderlichen Garantien können **Videoüberwachung** und/oder **am Körper getragene Kameras** die Rechenschaftspflicht verbessern und Beweise liefern, die Maßnahmen zur Änderung vorurteilsbehafteter Verhaltensmuster stützen können.

☑ **Formulare zu Kontrollen und Durchsuchungen** erstellen, die nach jeder Kontrolle von den beteiligten Beamtinnen und Beamten ausgefüllt werden müssen.

3. Handeln und vorbeugen

☑ **Bewertungen** durchführen, um zu ermitteln, ob Regeln und Praktiken bestehen, die zur Aufrechterhaltung expliziter oder impliziter Vorurteile und negativer Stereotype führen.

☑ Spezifische Kurse und/oder **Schulungseinheiten** einführen, deren Schwerpunkt auf der Bekämpfung persönlicher und institutioneller Vorurteile und Stereotype liegt.

☑ Einzelpersonen, die einer Kontrolle unterzogen werden, entsprechend **informieren**, um deren Eindruck zu erhöhen, dass die Kontrolle fair abläuft. Außerdem sollten den Personen ausreichende Informationen bereitgestellt werden, die ihnen bei der Entscheidung helfen, ob sie einen Rechtsbehelf einlegen sollten. Bei einem Verweis an eine Kontrolle in der zweiten Kontrolllinie an Grenzübergangsstellen ist die Bereitstellung dieser Informationen gesetzlich vorgeschrieben.

☑ **Null-Toleranz-Politik** innerhalb der Organisation bei von Voreingenommenheit geprägten Vorfällen.

☑ **Interne Mechanismen** für die Überwachung und Kontrolle einführen, beispielsweise interne Gremien, in denen erörtert wird, ob hinreichende Gründe für eine Kontrolle vorlagen.

- ☑ Sicherstellen, dass **Leistungsindikatoren** so verknüpft sind, dass Vorurteile und Stereotype vermieden werden.
- ☑ **Beschwerdemechanismen** einführen, um Machtmissbrauch zu verhindern und die Rechenschaftspflicht zu gewährleisten.

Quelle: *FRA, 2018*

2.3.1. Interne Überwachung

Die Führungs- und Verwaltungsebene in Polizei- und Grenzschutzbehörden spielt eine wichtige Rolle bei der Schaffung eines ethischen Bewusstseins, das die Rechte des einzelnen Menschen und den Grundsatz der Nichtdiskriminierung sowohl innerhalb der Organisation als auch im Umgang mit der Öffentlichkeit wahrt. Sie trägt außerdem dazu bei, ein Klima der Verantwortung und Transparenz zu schaffen. Eine offene Kommunikation zwischen den Mitarbeiterinnen und Mitarbeitern (sowohl horizontal als auch vertikal) und die Festlegung klarer Verhaltensnormen, wie beispielsweise berufsständische Verhaltenskodizes, sind zwei der internen Elemente, die zur Verbesserung der Rechenschaftspflicht vorhanden sein sollten. Auch die Personaleinstellung und ausbildung spielt eine wichtige Rolle (siehe Abschnitt 2.2.3).

Nach EU-Recht muss jede Behörde oder Einrichtung eine(n) **Datenschutzbeauftragte(n)** benennen. Er/Sie berät die Polizei- und Grenzschutzbeamtinnen und -beamten in Bezug auf ihre Datenschutzpflichten, einschließlich der Führung von Aufzeichnungen über die Datenverarbeitung oder der Durchführung von Datenschutz-Folgenabschätzungen. Im Rahmen des Profilings überwacht der/die Datenschutzbeauftragte beispielsweise, ob die während oder zum Zwecke des Profilings erhobenen personenbezogenen Daten rechtmäßig verarbeitet und gespeichert werden, und berät die betreffenden Beamtinnen und Beamten entsprechend.

Im Fokus: Die Rolle des/der Datenschutzbeauftragten

In der **Polizeirichtlinie** ist festgelegt, dass die Mitgliedstaaten eine(n) Datenschutzbeauftragte(n) benennen müssen, der/die u. a. folgende Aufgaben hat:

- Überwachung der Einhaltung der geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, einschließlich:

- Zuweisung von Zuständigkeiten;
- Sensibilisierung und Schulung der Mitarbeiter;
- Überprüfungen;

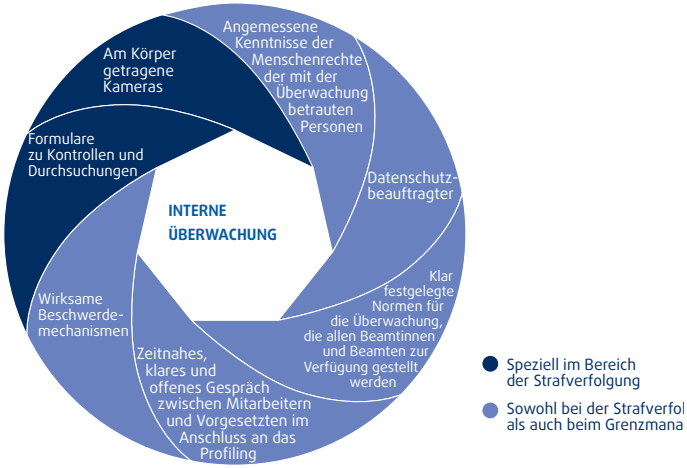
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Tätigkeit als Ansprechpartner(in) für die Aufsichtsbehörde.

Der/Die Datenschutzbeauftragte sollte vollständig und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden.

Siehe Artikel 32 bis 34 der Polizeirichtlinie.

Innerhalb der Polizei kann die interne Überwachung des Profilings im Rahmen einer Vielzahl weiterer Maßnahmen durchgeführt werden, die darauf abzielen, die Begegnungen zwischen Behörden und der Bevölkerung zu protokollieren (siehe Abbildung 10). Dazu gehört auch der Einsatz von:

Abbildung 10: Elemente der internen Überwachung



Quelle: *FRA, 2018*

- **Formularen zu Kontrollen und Durchsuchungen**: Diese sind ein nützliches und praktisches Instrument, mit dem die Beamtinnen und Beamten ermutigt werden, begründete Kontrollen durchzuführen, und die gleichzeitig die Offenheit und Rechenschaftspflicht gegenüber der Öffentlichkeit fördern (siehe Abschnitt 2.2.5);

- **am Körper getragenen Kameras**: Vorbehaltlich der erforderlichen Garantien können diese Kameras das Vertrauen zwischen den Gemeinschaften und der Polizei stärken und eine abschreckende Wirkung in Bezug auf den Missbrauch von Befugnissen sowie Diskriminierung haben (siehe Abschnitt 2.3.2).

Bei den internen Überwachungsaktivitäten in Grenzschutzorganisationen können diese Maßnahmen ebenfalls zum Einsatz kommen. Der Schengen-Katalog beispielsweise empfiehlt, die Anzahl und die Gründe für die Weiterleitung an eine Kontrolle in der zweiten Kontrolllinie zu protokollieren. Darüber hinaus schaffen verschiedene Umfelder bei den Grenzkontrollen, die Infrastruktur an den Grenzübergangsstellen und die Anwesenheit von Vorgesetzten vor Ort weitere Möglichkeiten der internen Überwachung. So können beispielsweise zusätzliche technische Geräte wie ein Videoüberwachungssystem vorhanden sein.

Mit den erforderlichen Garantien kann Videomaterial als Nachweis zur Beurteilung des Profilings dienen und bei spezifischen Beschwerden in diesem Zusammenhang herangezogen werden. Es könnte beispielsweise überprüft werden, ob das Verhalten einer Person während des Wartens auf die Erstkontrolle einen ausreichenden Grund dafür bot, sie einer Kontrolle in der zweiten Kontrolllinie zu unterziehen.

Anders als bei Kontrollen und Durchsuchungen erwarten und fordern die meisten Reisenden an den Grenzübergangsstellen aufgrund des öffentlichen Charakters und aus Sicherheitsgründen den Einsatz von Videoüberwachung. Dennoch müssen bei der Verwendung solcher Instrumente das Recht auf Privatsphäre und die geltenden Datenschutzbestimmungen beachtet werden.

Das Führen von Aufzeichnungen kann sowohl kurz- als auch langfristige Vorteile mit sich bringen. Dies wird am Beispiel der Formulare zu Kontrollen und Durchsuchungen deutlich:

- **Kurzfristig** können die Formulare zu Kontrollen und Durchsuchungen dazu beitragen, die Rechenschaftspflicht gegenüber der Öffentlichkeit vor Ort zu erfüllen. Im Vereinigten Königreich erhält jede angehaltene Person ein Protokoll der

Kontrolle oder eine Bescheinigung, aus der hervorgeht, wo eine Kopie des Protokolls angefordert werden kann. Darin enthalten sind detaillierte Angaben zum Grund der Kontrolle sowie Informationen darüber, wo und wie eine Beschwerde eingelegt werden kann. Die Person kann so den Grund für die Kontrolle einsehen und ggf. Einspruch einlegen, wenn sie die Kontrolle für nicht gerechtfertigt hält.

- **Langfristig** kann die Polizei anhand der Analyse der Aufzeichnungen feststellen, ob unverhältnismäßig viele Mitglieder einer Minderheitengruppe angehalten und durchsucht wurden; die Leitlinien für die Beamtinnen und Beamten können dann entsprechend angepasst werden. Diese Aufzeichnungen können veröffentlicht werden, um die Transparenz zu erhöhen und das Vertrauen der Öffentlichkeit in die Ausübung der Kontroll- und Durchsuchungsbefugnisse zu steigern.

Aufzeichnungen führen Wie ist die Rechtslage?

Um die Rechtmäßigkeit der Datenverarbeitung sicherzustellen, schreibt die Polizeirichtlinie vor, dass die Strafverfolgungsbehörden ein Verzeichnis aller Kategorien von Tätigkeiten der Verarbeitung führen, die ihrer Zuständigkeit unterliegen. Darüber hinaus müssen sie in automatisierten Verarbeitungssystemen Protokolle führen, anhand derer festgestellt werden kann, wer die personenbezogenen Daten abgefragt oder offengelegt hat und wann dies geschehen ist, wer die Daten erhalten hat und warum die Datenverarbeitung erfolgt ist (siehe Abschnitt 3.1.3).

Artikel 24 und 25 der Polizeirichtlinie

Fallstudie

Nutzung von Aufzeichnungen zur Aufdeckung von Unverhältnismäßigkeiten bei Kontrollen und Durchsuchungen (Vereinigtes Königreich)

Gemäß dem in England und Wales (Vereinigtes Königreich) ausgearbeiteten Verhaltenskodex im Rahmen des Police and Criminal Evidence Act (PACE, Polizei- und Beweismittelgesetz) sind die Polizeikräfte verpflichtet, die Ausübung der Befugnis zu Kontrollen und Durchsuchungen zu überwachen, um festzustellen, ob Personen aufgrund stereotyper Bilder oder unangemessener Verallgemeinerungen angehalten wurden. Jede

offensichtlich unverhältnismäßige Ausübung der Befugnisse durch bestimmte Beamtinnen und Beamte oder Gruppen von Beamtinnen und Beamten oder in Bezug auf bestimmte Teile der Gesellschaft sollte festgestellt und untersucht werden, und es sollten geeignete Abhilfemaßnahmen ergriffen werden. Darüber hinaus muss die Polizei dafür sorgen, dass die Aufzeichnungen von Vertreterinnen und Vertretern der Gemeinschaft eingesehen werden können, und die Ausübung der Befugnisse zu Kontrollen und Durchsuchungen auf lokaler Ebene erläutern.

Weitere Informationen: siehe Vereinigtes Königreich, Home Office (2014a).

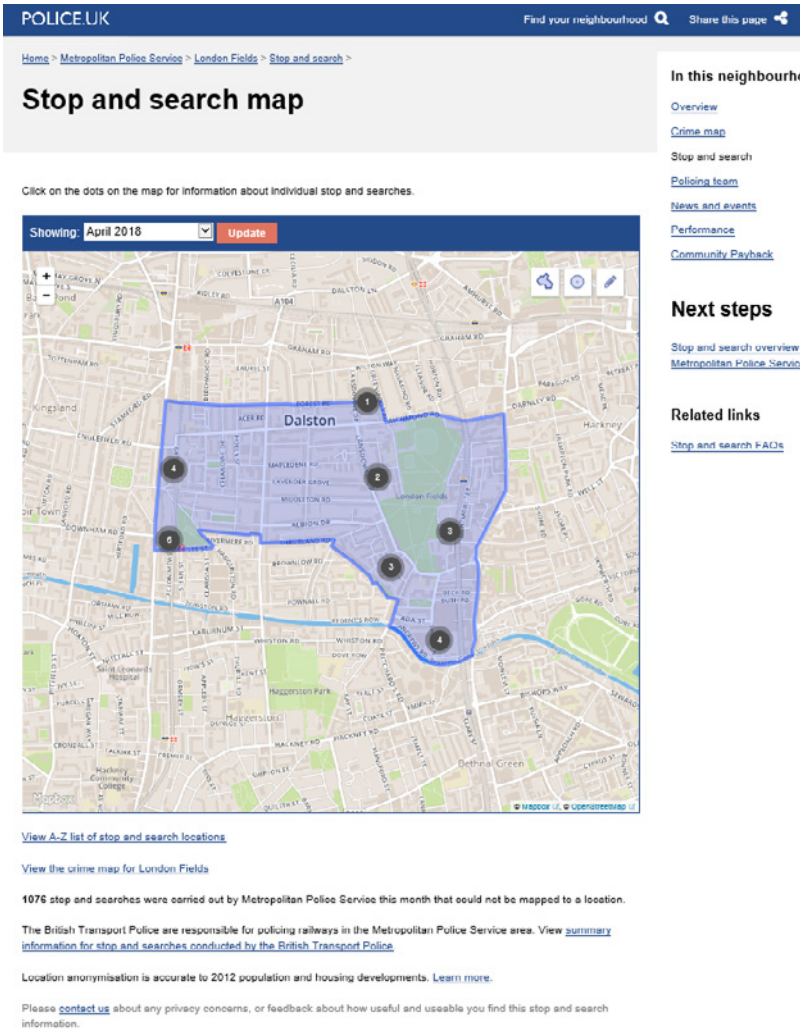
Zur Erhöhung der Transparenz hat die Polizei im Vereinigten Königreich mehrere Instrumente entwickelt, die die Daten zu Kontrollen und Durchsuchungen leichter zugänglich machen. Auf der Website www.police.uk können die Benutzerinnen und Benutzer durch Eingabe ihrer Postleitzahl ausführliche Informationen zur Anzahl und Art der in ihrer Umgebung durchgeführten Kontrollen abrufen. Die dort veröffentlichten Informationen basieren auf den ausgefüllten Formularen zu Kontrollen und Durchsuchungen. Die Datenbank der Metropolitan Police, das sogenannte Stop and search dashboard, enthält Daten zu allen Kontrollen und Durchsuchungen, die in London durchgeführt wurden, einschließlich Angaben zum Anteil der Angehörigen ethnischer Minderheiten im Verhältnis zur Gesamtbevölkerung. Die Benutzerinnen und Benutzer können sich die Daten in unterschiedlicher Form anzeigen lassen, z. B.

- als Karte, auf der der genaue Ort der Kontroll- und Durchsuchungsmaßnahmen, sortiert nach Monat, ersichtlich ist. Das Instrument liefert auch detaillierte Informationen über die Kontroll- und Durchsuchungsmaßnahme (Objekt, Art, Ergebnis, Angabe, ob die Maßnahme Teil eines Polizeieinsatzes war), über die Person (Geschlecht, Altersgruppe, Selbstauskunft zur ethnischen Zugehörigkeit, Angabe der Beamtin/des Beamten zur ethnischen Zugehörigkeit) sowie Angaben zur Gesetzgebung, auf die die Rechtmäßigkeit der Kontroll- und Durchsuchungsmaßnahme gestützt wurde (siehe Abbildung 11); sowie

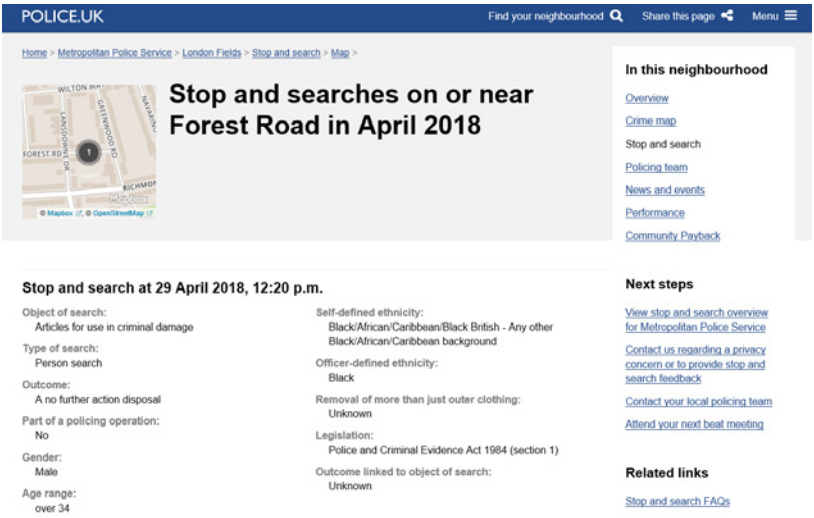
- als statistische Übersicht mit Diagrammen, die die Kontroll- und Durchsuchungsmaßnahmen der Polizei verdeutlichen. Die Informationen können aggregiert und heruntergeladen werden.

Diese Praxis fördert zwar die Transparenz und das Vertrauen, könnte sich jedoch nachteilig auf die Rechte auf Privatsphäre und Datenschutz der betroffenen

Abbildung 11: Online-Instrument mit Details zu Kontroll- und Durchsuchungsmaßnahmen in London



Quelle: *Vereinigtes Königreich, Home Office, Webseite mit Übersichtskarte zu Kontrollen und Durchsuchungen*



Quelle: Vereinigtes Königreich, Home Office, Webseite zu spezifischen Kontrollen

Personen auswirken. Die Identität einer Person könnte möglicherweise aus einer Kombination von Daten, die in diesem oder einem anderen Online-Instrument gespeichert sind, abgeleitet werden. Derlei Risiken müssen bewertet und gegebenenfalls berücksichtigt werden.

2.3.2. Am Körper getragene Kameras

Die Polizei verwendet zunehmend am Körper getragene Kameras, auch Körperkameras oder Bodycams genannt. Sie können eine wesentliche Rolle spielen, wenn es darum geht, die Rechenschaftspflicht sicherzustellen, die Qualität der Begegnungen zu verbessern und vorurteilsbehaftete Verhaltensmuster zu ändern. Sie können außerdem dazu beitragen, gefährliche Situationen zu entschärfen. Zusätzlich zu den Videoaufzeichnungen der Polizei filmen auch die Bürgerinnen und Bürger zunehmend Kontrollen und andere Interaktionen mit der Polizei. Dieses Material kann ebenfalls dazu verwendet werden, die polizeiliche Praxis zu überprüfen.

Fallstudie

Die Wirksamkeit von am Körper getragenen Kameras

Im Vereinigten Königreich zeigte eine im Jahr 2015 durchgeführte Studie über die Verwendung von 500 Kameras durch 814 Beamtinnen und Beamte der Metropolitan Police keine Gesamtwirkung auf Anzahl oder Art der Kontrollen und Durchsuchungen, keine Auswirkungen auf den Anteil der Festnahmen wegen Gewaltverbrechen und keine Anzeichen dafür, dass die Kameras den Umgang der Beamtinnen und Beamten mit Opfern und Verdächtigen verändert haben. Berichte, in denen die Auswirkungen ähnlicher Versuche durch andere Polizeikräfte bewertet wurden, zeigen wenig oder gar keine Anzeichen dafür, dass der Einsatz von Kameras einen positiven Effekt auf die Verringerung der Kriminalität, Beschwerden gegenüber Polizeibeamtinnen und -beamten oder die Anwendung von Gewalt hatte.

Weitere Informationen: siehe Big Brother Watch (2017).

In Frankreich wurden im Rahmen eines zwei Jahre dauernden Pilotprojekts Polizeibeamtinnen und -beamte in 300 Orten mit am Körper getragenen Kameras ausgestattet. Eine vom Innenministerium durchgeführte Überprüfung aus dem Juni 2018 zeigte die positiven Auswirkungen und Ergebnisse dieses Tests auf. Der Bericht betonte vor allem die abschreckende Wirkung, die solche Kameras auf die angehaltenen Personen hatten – die Beamtinnen und Beamten wurden in der Folge deutlich seltener beleidigt oder tätlich angegriffen. Andere Berichte aus verschiedenen Gemeinden wiesen darauf hin, dass der Einsatz von Körperkameras das aggressive und beleidigende Verhalten gegenüber Polizeibeamten und -beamten verringert hat. Einige Gemeinden gaben an, dass Situationen, die andernfalls wohl einen Angriff gegen die Polizeibeamtinnen/beamten zur Folge gehabt hätten, durch die Verwendung von Körperkameras deeskaliert werden konnten. Den Berichten zufolge liegt der Hauptzweck von am Körper getragenen Kameras zwar vor allem in der abschreckenden Wirkung, in Gerichtsverfahren wurden jedoch bereits Aufnahmen als Beweismittel zur Identifizierung von Täterinnen und Tätern zugelassen. Darüber hinaus betonten mehrere Gemeinden den pädagogischen Nutzern solcher Kameras, da einige Polizeibeamtinnen und beamte in Interventionsverfahren und techniken geschult wurden, indem sie sich die während der Interventionen gemachten Aufzeichnungen ansahen. Im Anschluss an das Pilotprojekt wurde dem französischen Parlament ein Gesetzentwurf vorgelegt, der darauf abzielt, den Einsatz von Körperkameras

bei allen Polizeikräften zu harmonisieren und auch auf Feuerwehrkräfte und Justizvollzugsbeamtinnen/beamte auszudehnen.

Weitere Informationen: siehe Frankreich, Innenministerium (2018).

2012 und 2013 wurde im Rahmen eines groß angelegten 12-monatigen Testlaufs in Rialto (USA) untersucht, ob das Tragen von Körperkameras ein gesellschaftlich erwünschtes Verhalten der mit ihnen ausgestatteten Beamtinnen und Beamten zur Folge hat. Im Vergleich zum Jahr 2011 ging der Einsatz von Gewalt während des 12-monatigen Testlaufs von 60 auf 25 Fälle zurück, und Beschwerden gegen die Polizei verringerten sich von 28 Fällen auf 3 Fälle.

Weitere Informationen: siehe Farrar, T. (2018).

Der Einsatz von Körperkameras durch die Polizei führt jedoch auch zu Bedenken im Hinblick auf einige wesentliche Grundrechte und Polizeioperationen. Klare Garantien und Vorgaben bezüglich der Verwendung solcher Kameras sind erforderlich, um die folgenden Probleme anzugehen:

- Die **Rolle von Körperkameras bei der Aufdeckung und Verhinderung von unrechtmäßigem Profiling** ist nicht eindeutig festgelegt. Die Kameras zeichnen einzelne Vorfälle auf und gestatten keine Erhebung statistischer Daten, die der Feststellung dienen können, ob Kontrollen und Durchsuchungen eine Diskriminierung darstellen. Sie können aber dazu verwendet werden, einzelne Begegnungen zu überprüfen, um deren Qualität zu verbessern.

- Der Einsatz von Körperkameras könnte sich **negativ auf die Beziehungen zu Minderheiten auswirken**, wenn diese den Eindruck gewinnen, dass die Maßnahmen speziell auf sie abzielen. Die Schaffung von Garantien und geeigneten Maßnahmen in Absprache mit den lokalen Gemeinschaften kann dazu beitragen, dass Körperkameras stärker als Instrument zur Verbesserung der Rechenschaftspflicht wahrgenommen werden und weniger als Mittel zur Stigmatisierung von Minderheiten.

- Das Tragen von Körperkameras hat **Folgen für die Rechte auf Privatsphäre und Datenschutz** sowie andere grundlegende Menschenrechte. Beispielsweise könnte die Versammlungsfreiheit eingeschränkt werden, wenn die Kameras zur

Überwachung öffentlicher Demonstrationen eingesetzt werden. Es ist häufig unklar, wann die Kameras ein- bzw. ausgeschaltet werden sollten und was passiert, wenn eine Beamtin oder ein Beamter vergisst oder sich dagegen entscheidet, die Kamera einzuschalten: In diesem Bereich müssen eindeutige Vorgaben erlassen werden. Privatunternehmen, die diesen Service anbieten, müssen sich darüber im Klaren sein, dass sie die Aufzeichnungen nicht für ihre eigenen Zwecke verwenden dürfen. Der Einsatz von Körperkameras sollte gesetzlich geregelt sein, damit die Vereinbarkeit mit den Grundrechten sichergestellt ist.

Im Fokus: Der wirksame Einsatz von Körperkameras

Drei wichtige Grundsätze können dazu beitragen, den wirksamen Einsatz von Körperkameras sicherzustellen:

- **Authentizität**: Die Bilder müssen eindeutig mit dem Vorfall in Verbindung stehen. Datum und Zeit (z. B. durch einen Zeitstempel) und der genaue Ort (z. B. per GPS) des Vorfalls sollten aufgezeichnet werden;
- **Zuverlässigkeit**: Die Bilder sollten ausnahmslos, sicher und vertraulich in ein zentrales System hochgeladen werden. Die Bilder sollten die Grundsätze des Datenschutzes und der Achtung des Privatlebens wahren und daher nicht länger gespeichert werden als gesetzlich vorgeschrieben;
- **Zulässigkeit**: Die Aufzeichnungen müssen vor Gericht zulässig sein, damit sie in Strafverfahren von Nutzen sind. Hierfür sind u. a. folgende Aspekte zu beachten:
  - Vermeiden dauerhafter Videoaufzeichnungen, da dies sowohl für die Polizeibeamtinnen/beamten als auch für die gefilmten Personen einen nicht hinnehmbaren Eingriff in das Recht auf Privatsphäre darstellt;
  - Unterrichten derjenigen Personen, die gefilmt werden könnten, und ggf. Einholen ihres Einverständnisses;
  - Speichern der Bilder mit einem entsprechenden Maß an Sicherheit sowie Verfolgen des Zugriffs auf die Bilder sowohl durch die Polizeibeamtinnen/beamten als auch durch die Bürgerinnen und Bürger.

Weitere Informationen: siehe Coudert et al. (2015), S. 8.

Weitere technologische Entwicklungen erfordern die Ausarbeitung neuer Garantien, um sicherzustellen, dass der Einsatz von Körperkameras rechtmäßig ist. Kameras, die das Gesicht einer Person durch den Abgleich mit früheren Einträgen in einer Datenbank automatisch erkennen können, bringen beispielsweise neue Herausforderungen für die Rechte auf Privatsphäre und Datenschutz mit sich.

Fallstudie

Körperkameras der Polizei: Eine Scorecard mit Richtlinien (USA)

Zur Verbesserung der Transparenz und Rechenschaftspflicht durch den Einsatz von Körperkameras wurde auf der Leadership Conference on Civil and Human Rights & Upturn in den Vereinigten Staaten ein Instrument zur Bewertung und Strukturierung der Informationen entwickelt, die aus den Aufzeichnungen der Körperkameras gewonnen werden können. Das Instrument schlägt zur Bewertung des Videomaterials acht Kriterien vor:

1. Hat die Polizei das Material veröffentlicht, und ist es leicht zugänglich?
2. Ist die Ermessensfreiheit der Beamtinnen und Beamten bezüglich der Aufzeichnung eindeutig geregelt?
3. Werden Datenschutzbedenken berücksichtigt?
4. Müssen die Beamtinnen und Beamten das Videomaterial überprüfen, bevor sie den ersten schriftlichen Bericht verfassen?
5. Muss Videomaterial, das nicht als relevant gekennzeichnet wurde, nach einer festgelegten Zeit gelöscht werden?
6. Ist das Videomaterial vor Manipulation und Missbrauch geschützt?
7. Wird das Videomaterial Personen zugänglich gemacht, die eine Beschwerde eingelegt haben?
8. Ist der Einsatz biometrischer Methoden zur Identifizierung von Personen in den Aufzeichnungen eingeschränkt?

Durch die Festlegung gewisser Standards und die Einführung von Mechanismen zur Bewertung der Frage, ob das Material rechtmäßig erstellt und verwendet wird, können solche Initiativen zur Stärkung der Rechenschaftspflicht beitragen.

Weitere Informationen hierzu siehe die Website zur Richtlinien-Scorecard, die im Rahmen der Leadership Conference on Civil and Human Rights & Upturn erarbeitet wurde.

2.3.3. Beschwerdemechanismen

Wirksame Beschwerdemechanismen können Machtmissbrauch verhindern und dazu beitragen, das Vertrauen der Öffentlichkeit in die Tätigkeit der Polizei- und Grenzschutzbehörden wiederherzustellen bzw. zu stärken. Sie existieren in der Regel zusätzlich zu den formalen Rechtswegen, die es Einzelpersonen ermöglichen, eine Maßnahme oder Entscheidung einer Behörde vor einem unabhängigen und unparteiischen Gericht anzufechten.

Damit die Wirksamkeit einer solchen Beschwerde gewährleistet ist, müssen folgende Voraussetzungen erfüllt sein:

- **Beschwerdemechanismen sind für Einzelpersonen leicht zugänglich**: Untersuchungen zeigen immer wieder, dass Menschen zögern, eine Beschwerde einzulegen, weil beispielsweise das Verfahren langwierig oder teuer ist oder weil sie negative Konsequenzen befürchten. Durch die erleichterte Zugänglichkeit von Beschwerdemechanismen, z. B. über Online-Plattformen oder Apps, können mehr Menschen zur Nutzung dieser Möglichkeit ermutigt werden. Darüber hinaus können Organisationen Einzelpersonen bei der Einreichung von Beschwerden unterstützen, indem sie gemäß Artikel 80 Absatz 2 DSGVO entweder Beschwerde in ihrem Namen einlegen oder ein kollektives Beschwerdeverfahren auf den Weg bringen;

- **Beschwerden werden transparent behandelt**: Das trägt dazu bei, das Vertrauen in die Beschwerdemechanismen zu stärken;

- **Beschwerdestellen sind unabhängig** von der Organisation oder dem Teil der Organisation, gegen die bzw. den die Beschwerde gerichtet ist.

Abbildung 12: Überblick über die Beschwerdemechanismen in den EU-Mitgliedstaaten

Quelle: *FRA, 2018*

Es gibt eine Vielzahl von verschiedenen Mechanismen für unterschiedliche Arten von Beschwerden. Abbildung 12 gibt einen Überblick über einige der in den EU-Mitgliedstaaten und auf EU-Ebene verfügbaren Beschwerdemechanismen.

Mechanismen, die vorsehen, dass die Polizeibeamtinnen und -beamten mit Mitgliedern der Öffentlichkeit zusammenkommen, um sich ihre Beschwerden anzuhören, das Vorgehen beim Profiling zu diskutieren und Rückmeldungen zu ihren Einsätzen einzuholen, geben ihnen Gelegenheit, wichtige Erkenntnisse zur Verbesserung der Prozesse zu gewinnen, die dem Profiling zugrunde liegen. Darüber hinaus bieten sie die Möglichkeit, die Öffentlichkeit in die Strafverfolgung einzubeziehen (siehe Fallstudie).

Fallstudie

Öffentliche Beschwerdemechanismen in der Strafverfolgung

Öffentliche Kontrollgremien (West Midlands Police, Vereinigtes Königreich)

Jeder der acht Polizeibezirke der West Midlands Police (WMP) hält alle zwei Monate eine Sitzung des Kontrollgremiums, dem sogenannten Scrutiny Panel, zu Kontrollen und Durchsuchungen ab, die von Mitgliedern der Öffentlichkeit geleitet wird. Diese Gremien bewerten die Aufzeichnungen zu Kontrollen und Durchsuchungen, stellen sicher, dass die WMP dabei rechtmäßig handelt, und bieten den Gemeinden eine Möglichkeit, Beschwerden einzureichen und Probleme anzusprechen. Die Tagesordnungen und Protokolle dieser Sitzungen sind online verfügbar. Die WMP hat eine Reihe zusätzlicher Praktiken im Zusammenhang mit der Einbindung der Gemeinschaft eingeführt, um Kontrollen auf der Straße fairer und gezielter zu gestalten und die Verantwortlichkeit der Beamtinnen und Beamten zu erhöhen.

Weitere Informationen: siehe West Midlands Police, Webseite zu Kontrollen und Durchsuchungen, sowie Her Majesty's Inspectorate of Constabulary (2016).

Gremien zur Prüfung der Rechtmäßigkeit (Northamptonshire Police, Vereinigtes Königreich)

Die Northamptonshire Police hat Gremien zur Prüfung der Rechtsmäßigkeit von Kontrollen, die sogenannten Reasonable Grounds Panels, eingeführt, um die Öffentlichkeit aktiv in die Verbesserung ihrer Kontroll- und Durchsuchungsmaßnahmen einzubeziehen. Diese Gremien bieten eine Plattform für Diskussionen über die Ausübung der Kontroll- und Durchsuchungsbefugnisse der Polizei und deren Auswirkungen auf die Gemeinschaften. Ihnen steht ein Chief Inspector vor, die weiteren Teilnehmer(innen) sind ein Polizeivollzugsbeamter sowie zwei Mitglieder der Gemeinschaft, bei denen es sich auch um Straftäter(innen) oder ehemalige Straftäter(innen) handeln kann. Neben der Verbesserung der Kommunikation zwischen der Polizei und der Öffentlichkeit kann dieses Gremium den Beamtinnen und Beamten Befugnisse entziehen und zusätzliche Schulungen anordnen, um die Fähigkeiten der Beamtinnen und Beamten bei Kontrollen und Durchsuchungen zu verbessern.

Weitere Informationen: siehe Gremium-Webseite der Northamptonshire Police sowie Open Society Justice Initiative (2018a).

Informelles Netzwerk polizeilicher Beschwerdemechanismen

Das Netzwerk unabhängiger Behörden für Beschwerden über die Polizei (IPCAN) ist ein informelles Netzwerk für den Austausch und die Zusammenarbeit zwischen unabhängigen Strukturen, die für die externe Kontrolle von Sicherheitskräften zuständig sind. Es wurde 2013 eingerichtet und vereint Beschwerdestellen aus rund 20 Ländern. Diese Stellen, die hauptsächlich aus den EU-Mitgliedstaaten stammen, nehmen Beschwerden gegen öffentliche und manchmal auch gegen private Sicherheitskräfte entgegen und bearbeiten sie.

Weitere Informationen finden Sie auf der Website des IPCAN.

Im Grenzmanagement können öffentliche Beschwerdemechanismen durch Möglichkeiten zur Einreichung einer Beschwerde vor Ort oder im Rahmen eines *Ex-post*-Verfahrens umgesetzt werden. Die Möglichkeit, auf solche Mechanismen zurückgreifen zu können, erhöht die Transparenz und Rechenschaftspflicht und fördert den gegenseitigen Respekt und die guten Beziehungen zwischen den Grenzschutzbeamtinnen und -beamten und der Öffentlichkeit. Die Möglichkeit, eine

Beschwerde nachträglich (*ex post*) bei einer übergeordneten Stelle und nicht (nur) direkt an der Grenzübergangsstelle einreichen zu können, schafft ein gewisses Maß an Übersicht und kann die Bereitschaft der Reisenden, mögliche Vorfälle zu melden, positiv beeinflussen.[36]

Fallstudie

Öffentliche Beschwerdemechanismen im Grenzmanagement

Interner Beschwerdemechanismus am Flughafen Manchester (Vereinigtes Königreich)

Das zentrale Drehkreuz am Flughafen Manchester – der „Central Allocation Hub" – ist die Hauptanlaufstelle für alle Passagiere, die eine Beschwerde einreichen möchten. Die Beschwerden können per E-Mail, Brief, Telefon oder Fax sowie persönlich auf Englisch oder auf Walisisch eingereicht werden. Die Leitlinien der britischen Border Force zeigen mögliche Wege zur Lösung von Beschwerden auf. Geringfügiges Fehlverhalten wie Unhöflichkeit, Schroffheit oder eine negative Einstellung können in der Regel vor Ort behoben werden. Geeignete Möglichkeiten sind hierbei beispielsweise die Klärung der Probleme mit dem Reisenden, die Erläuterung der Abläufe im Rahmen des Einsatzes, die Vereinbarung weiterer Maßnahmen und ggf. eine Entschuldigung. Beschwerden über schwerwiegendes Fehlverhalten werden in der Regel an die Professional Standards Unit (PSU) weitergeleitet. Die Leitlinien der Border Force umfassen einen Test zum Bestimmen von Anzeichen einer möglichen Diskriminierung, die ein schwerwiegendes Fehlverhalten darstellen würde. Wenn es erste deutliche Hinweise darauf gibt, dass die Behandlung einer oder eines Reisenden durch andere Faktoren als die Rasse erklärt werden kann, wird der Fall in der Regel vor Ort gelöst.

Weitere Informationen: siehe FRA (2014a), S. 74.

Frontex: Individueller Beschwerdemechanismus (EU)

Nach der Annahme der neuen Verordnung der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) im Jahr 2016 hat Frontex einen individuellen Beschwerdemechanismus eingerichtet, um zu überwachen, ob die Grundrechte bei den Tätigkeiten der Agentur gewahrt werden.

36 FRA (2014b).

Hierzu zählen Pilotprojekte, Rückführungsaktionen, gemeinsame Aktionen, Soforteinsätze für Grenzsicherungszwecke sowie Einsätze der Teams zur Unterstützung von Migrationsverwaltung und Rückführungsaktionen. Jede Person, deren Rechte direkt durch die Handlungen der an Frontex-Aktivitäten beteiligten Mitarbeiter beschränkt wurden, darunter auch Mitarbeiter der nationalen Behörden, kann bei dem/der Grundrechtsbeauftragten von Frontex eine Beschwerde einreichen. Er oder sie entscheidet über die Zulässigkeit der Beschwerde und übermittelt sie an den Exekutivdirektor von Frontex sowie an die Behörden des betroffenen Mitgliedstaats, wenn nationale Mitarbeiter an der mutmaßlichen Rechteverletzung beteiligt waren. Die Beschwerde kann in einer beliebigen Sprache per E-Mail, Brief oder über ein Online-Beschwerdeformular eingereicht werden, das auf der Frontex-Website verfügbar ist: http://frontex.europa.eu/complaints/.

Im Fokus: Die Rechte von Strafverfolgungsbeamtinnen und -beamten

Polizeibedienstete haben die gleichen Rechte und Freiheiten wie andere Personen auch und fallen bei der Ausübung ihrer Arbeit unter den Schutz der Menschenrechte. Sie können sich dabei auf verschiedene internationale Menschenrechtsdokumente stützen, wie die Europäische Menschenrechtskonvention (EMRK) und den Internationalen Pakt über bürgerliche und politische Rechte (ICCPR). Dem Europäischen Kodex für die Polizeiethik zufolge muss „[d]as Polizeipersonal [...] in der Regel die gleichen zivilen und politischen Rechte wie andere Bürgerinnen und Bürger genießen. Einschränkungen dieser Rechte sind nur möglich, wenn sie zur Ausübung der Funktionen der Polizei in einer demokratischen Gesellschaft gemäß Gesetz und Europäischer Menschenrechtskonvention notwendig sind." Eine Ausnahme von dieser Auffassung findet sich in Artikel 11 EMRK zur Versammlungs- und Vereinigungsfreiheit.

Bei der Ausübung polizeilicher Aufgaben, insbesondere bei der Ausübung von Polizeibefugnissen, handelt eine Polizeibedienstete(r) nicht als Privatperson, sondern als Staatsorgan. Die staatliche Verpflichtung, die Menschenrechte zu achten und zu schützen, wirkt sich daher unmittelbar auf die Möglichkeiten einer bzw. eines Polizeibediensteten aus, auf Aggression zu reagieren. Die Rechte des/der Polizeibediensteten, der bei Ausübung ihrer bzw. seiner Pflichten Verletzungen oder gar den Tod riskiert, sind ebenfalls zu achten und zu schützen, beispielsweise durch die Bereitstellung von Schutzausrüstung, sorgfältige Einsatzplanung und die Umsetzung von

Präventivmaßnahmen. Einschränkungen dieser Rechte sind möglicherweise für die Ausübung der Funktionen der Polizei notwendig, dabei ist jedoch der Grundsatz der Verhältnismäßigkeit zu beachten. Aufgrund ihrer besonderen Rolle als Staatsorgan können die Rechte von Polizeibediensteten stärker eingeschränkt sein als jene „normaler Bürgerinnen und Bürger". So kann eine „normale Bürgerin" bei einer Demonstration, die in Gewalt ausartet, zum Beispiel weglaufen oder Hilfe holen, während ein Polizeibediensteter verpflichtet ist, die Menschenrechte anderer zu schützen und die öffentliche Ordnung wiederherzustellen.

Weitere Informationen: siehe FRA (2013).

3 Algorithmisches Profiling

Das algorithmische Profiling umfasst alle computergestützten Techniken, die Schritt für Schritt Daten analysieren, um Trends, Muster oder Zusammenhänge zu erkennen.[37] Durch das Profiling werden Einzelpersonen per Algorithmus auf der Grundlage ihrer Beziehungen zu anderen identifiziert und nicht durch ihr tatsächliches Verhalten; die Entscheidungen von Einzelpersonen werden anhand von Informationen über die Gruppe strukturiert und nicht nach ihren eigenen persönlichen Entscheidungen.[38]

Das algorithmische Profiling kann für Grenzschutz- und Strafverfolgungsbehörden eine effiziente Möglichkeit sein, Daten zur Prävention, Aufdeckung und Untersuchung von Straftaten zu nutzen. Die Erhebung und Verarbeitung großer Datensätze wirft jedoch eine Reihe von Grundrechtsfragen auf. Abgesehen davon, dass Diskriminierung unbedingt zu vermeiden ist, bringt das algorithmische Profiling aber auch neue Risiken mit sich, insbesondere hinsichtlich der Rechte auf Privatsphäre und Datenschutz. Der folgende Abschnitt konzentriert sich zunächst auf diese neuen Risiken. Anschließend werden die Grundrechtsprobleme veranschaulicht, die mit der Nutzung des algorithmischen Profilings in umfangreichen Datenbanken für Grenzmanagement- und Sicherheitszwecke einhergehen, und es werden einige Möglichkeiten zur Minimierung dieser Risiken vorgeschlagen.

37 Weitere Informationen zu Algorithmen finden Sie in FRA (2018b), S. 4.

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

Im Fokus: Vorhersagende Polizeiarbeit

Strafverfolgungsbehörden setzen verschiedene Softwareanwendungen ein, mit deren Hilfe vorhergesagt werden soll, wann und wo eine Straftat begangen wird. Beispiele dafür sind: PredPol im Vereinigten Königreich und den USA, das Criminality Awareness System (CAS) in den Niederlanden sowie Precobs in Deutschland und der Schweiz. Die Wirksamkeit dieser Vorhersagemethoden zur Verhütung von Straftaten wurde jedoch noch nicht ausreichend untersucht. Die bisherigen Erkenntnisse sind widersprüchlich, wie die folgenden Beispiele zeigen.

Feldversuch zu vorhersagender Polizeiarbeit in Kent (Vereinigtes Königreich) und Los Angeles (USA)

Die Polizei in Großbritannien und den USA erprobte – im Vergleich mit einem eher traditionellen Ansatz – einen vollständig automatisierten Algorithmus zur Identifizierung von Kriminalitätsschwerpunkten und der darauf folgenden Einsatzplanung für Polizeistreifen.

Die Ergebnisse zeigten, dass der automatisierte Algorithmus besser in der Lage war, mögliche künftige Straftaten zu erkennen. Im Vergleich zu einer Auswertung durch einen kriminalpolizeilichen Analytiker, der sich traditioneller kriminaltechnischer Erkenntnisse und Informationen aus der computergestützten geographischen Kriminalitätsanalyse („Crime mapping") bediente, konnten mithilfe des Algorithmus 1,4- bis 2,2mal mehr Straftaten vorhergesagt werden. Zudem sind Streifeneinsätze, die anhand dieses Prognoseinstruments geplant werden, deutlich effektiver, was zu einem Rückgang der Straftaten um durchschnittlich 7,4 % führte.

Weitere Informationen: siehe Mohler, G. O. et al. (2016).

Programm „PILOT" (Predictive Intelligence Led Operational Targeting) in Shreveport (USA)

Dieses Programm stützt sich auf ein Vorhersagemodell, mit dem begrenzte Gebiete identifiziert werden sollen, in denen das Risiko von Eigentumsdelikten erhöht ist. Ziel ist es, in diesen Gebieten ein Interventionsmodell zur Prävention von Eigentumskriminalität einzuführen. Die Ergebnisse aus drei Distrikten, die PILOT einsetzten, wurden mit drei Distrikten verglichen, in

denen traditionelle Polizeiarbeit geleistet wurde. In den drei untersuchten PILOT-Distrikten gab es keine statistischen Belege für einen stärkeren Rückgang der Eigentumsdelikte.

Weitere Informationen: siehe Hunt, P. et al (2014).

Software „Beware" (USA)

Mit der Softwareanwendung „Beware" werden den Einsatzkräften, die Notrufe entgegennehmen, farbige Markierungen (rot, gelb und grün) angezeigt, anhand derer sie die Gefährdungsstufe der betroffenen Person oder des Standorts erkennen können. Die Software durchsucht Datenbanken mit Festnahmeberichten, Eigentumsnachweise, kommerzielle Datenbanken, detaillierte Websuchen, Posts in den sozialen Medien sowie andere öffentlich zugängliche Datenbanken nach Informationen.

Die Stärken und Schwächen dieses Systems wurden nicht näher untersucht. Die mangelnde Übersicht bei der Entscheidungsfindung und die hohe Geheimhaltungsstufe bei der Verwendung des Algorithmus, der bestimmten Geschäftsgeheimnissen unterliegt, haben jedoch Bedenken hinsichtlich der Rechenschaftspflicht aufgeworfen. Darüber hinaus können mögliche Ungenauigkeiten bei den erhobenen Daten und/oder den aus der Analyse abgeleiteten Informationen die Gesamtwirksamkeit des Instruments beeinträchtigen.

Weitere Informationen: siehe American Civil Liberties Union (2016).

Fallstudie

Bewertung der Auswirkungen und des Risikos vorhersagender Polizeiarbeit – das Bewertungsinstrument ALGO-CARE

Mögliche negative Auswirkungen der vorhersagenden Polizeiarbeit müssen berücksichtigt werden, um einen ausgeglichenen und transparenten Überblick über ihre Wirkung auf die Gesellschaft zu gewährleisten. Eine Gruppe, der auch Akademikerinnen und Akademiker und Polizeibeamtinnen und -beamte angehörten, führte eine Analyse durch. Diese ergab, dass sich die vorhersagende Polizeiarbeit im Vereinigten Königreich momentan noch

im Versuchsstadium befindet und daher ausführliche Bewertungen ihrer Auswirkungen auf die Gesellschaft und den Einzelnen erforderlich sind. Die Untersuchung legt nahe, dass einige Entscheidungen zu große Auswirkungen auf die Gesellschaft und den einzelnen Menschen haben könnten, als dass sie von einer neuen Technologie beeinflusst werden könnten; diese Fälle sollten aus dem Einflussbereich der algorithmischen Entscheidungsfindung herausgenommen werden.

Die Gruppe hat den Entscheidungsrahmen ALGO-CARE für den Einsatz von algorithmischen Bewertungsinstrumenten im Polizeikontext erarbeitet. Dieser Rahmen dient dazu, Polizeibeamtinnen und -beamte bei der Bewertung der potenziellen Risiken der vorhersagenden Polizeiarbeit zu unterstützen. Darüber hinaus soll auch versucht werden, die wichtigsten Grundsätze des öffentlichen Rechts und der Menschenrechte in praktische Überlegungen und Leitlinien umzusetzen, die von öffentlichen Stellen aufgegriffen werden können.

Das Bewertungsinstrument ermutigt die Polizeibeamtinnen und -beamten, den Einsatz der vorhersagenden Polizeiarbeit mittels acht einander ergänzender Schritte zu bewerten:

- **Beratung:** Beurteilung des Umfangs der menschlichen Intervention;
- **Rechtmäßigkeit:** Beurteilung der rechtlichen Begründung für die Anwendung des Algorithmus;
- **Granularität:** Beurteilung, ob der Algorithmus in einem konkreten Fall einen ausreichenden Detaillierungsgrad erreichen kann;
- **Eigentum:** Gewährleistung, dass die Polizei das rechtliche Eigentum an den Quelltexten hat und über die technische Fähigkeit verfügt, regelmäßig auf den Quelltext zuzugreifen, ihn zu pflegen, zu aktualisieren und zu korrigieren;
- **Anfechtbarkeit:** Gewährleistung, dass Aufsichts- und Prüfmechanismen vorhanden sind;
- **Genauigkeit:** Beurteilung, ob der Algorithmus mit der Zielsetzung der Polizeiarbeit übereinstimmt und regelmäßig überprüft werden kann und ob die Wahrscheinlichkeit und die Auswirkungen von Ungenauigkeiten ein akzeptables Risiko darstellen;

- **Verantwortlichkeit:** Beurteilung der Fairness, Rechenschaftspflicht und Transparenz des Algorithmus;
- **Erklärbarkeit:** Beurteilung der Zugänglichkeit von Informationen sowohl über die Entscheidungsfindungsregeln als auch über die Auswirkungen der einzelnen Faktoren auf das Endergebnis

Weitere Informationen: siehe Oswald, M. et al. (2017).

3.1. Der Datenschutzrahmen für das algorithmische Profiling

Die Entwicklung und der zunehmende Einsatz neuer Technologien, einschließlich der steigenden Verwendung großer Datensätze zur Unterstützung der Entscheidungsfindung, haben die EU veranlasst, ihre Vorschriften bezüglich der Verarbeitung personenbezogener Daten im Jahr 2016 umfassend zu überarbeiten. Die beiden daraus hervorgegangenen neuen Instrumente, nämlich die Datenschutz-Grundverordnung (DSGVO) und die Polizeirichtlinie, enthalten wichtige Grundsätze und Standards für alle Entscheidungen, die auf computergestützten Entscheidungsverfahren, einschließlich algorithmischem Profiling, beruhen.

Die DSGVO und die Polizeirichtlinie sind im Mai 2018 in Kraft getreten. Zum Zeitpunkt der Erstellung dieses Handbuchs lagen daher nur wenige praktische Beispiele für die Umsetzung vor. Abschnitt 1.2.2 enthält eine Beschreibung der rechtlichen Standards bezüglich des Rechts auf Privatsphäre und des Rechts auf Datenschutz und erläutert einige der wichtigsten Unterschiede zwischen der DSGVO und der Polizeirichtlinie (siehe Tabelle 2). Das vorliegende Kapitel stützt sich auf diese Informationen, um die gesetzlichen Anforderungen an das algorithmische Profiling zu beschreiben und zu erklären, die durch die DSGVO und die Polizeirichtlinie eingeführt wurden. Hierzu zählen:

- Die Datenverarbeitung muss für einen bestimmten Zweck auf einer bestimmten Rechtsgrundlage erfolgen;
- die betroffenen Personen müssen über die Verarbeitung ihrer personenbezogenen Daten unterrichtet werden;
- die Daten müssen sicher aufbewahrt werden;

- die unrechtmäßige Verarbeitung von Daten muss aufgedeckt und verhindert werden.

Polizei- und Grenzschutzbeamtinnen und -beamte, die weitere Informationen zu den in diesem Kapitel beschriebenen gesetzlichen Anforderungen benötigen, wenden sich bitte an die Datenschutzbeauftragten in ihren jeweiligen Behörden. Das gemeinsam von der FRA, dem EDSB und dem Europarat erarbeitete Handbuch zum Europäischen Datenschutzrecht (*Handbook on European Data Protection Law*, bisher nur auf Englisch verfügbar) enthält weitere Hinweise und Leitlinien zur Anwendung der Polizeirichtlinie und der DSGVO.[39]

Kernpunkte

- Das algorithmische Profiling muss **rechtmäßig, notwendig** und **verhältnismäßig** sein.
- Die Datenverarbeitung muss **für einen bestimmten Zweck auf einer bestimmten Rechtsgrundlage** erfolgen.
- Die betroffenen Personen haben spezifische Rechte, die in den Bestimmungen der DSGVO und der Polizeirichtlinie detailliert beschrieben werden, darunter:
  - das Recht **auf Information,** einschließlich des Anspruchs auf aussagekräftige Informationen über die Logik des Algorithmus,
  - das Recht **auf Auskunft über die personenbezogenen Daten**,
  - das Recht **auf Beschwerde** bei einer Aufsichtsbehörde sowie
  - das Recht **auf einen wirksamen gerichtlichen Rechtsbehelf**.
- Die Daten sollten **sicher** erfasst, verarbeitet und gespeichert werden.
- Die unrechtmäßige Verarbeitung von Daten muss **verhindert** und **aufgedeckt** werden.

3.1.1. Die Datenverarbeitung muss für einen bestimmten Zweck erfolgen

Jegliche Verarbeitung personenbezogener Daten muss sich auf eine rechtliche Grundlage stützen. Das bedeutet, dass sie zur Erreichung eines **bestimmten, gesetzlich festgelegten Zwecks** durchgeführt werden muss.

39 FRA, EDSB und Europarat (2018).

Bevor er oder sie mit der Datenverarbeitung beginnt, muss sich die Beamtin bzw. der Beamte über den jeweiligen Zweck im Klaren sein. Dieser könnte sich u. a. auf die folgenden Aspekte beziehen:

- Werden die Daten zur Aufdeckung einer Straftat verarbeitet?
- Werden sie zur Aufrechterhaltung der öffentlichen Sicherheit verarbeitet?
- Werden sie zur Terrorismusbekämpfung verarbeitet?

Sobald der Zweck der Verarbeitung korrekt ermittelt wurde, wissen die Beamtinnen und Beamten, welcher Rechtsrahmen anzuwenden ist und welche rechtlichen Verpflichtungen bestehen. Tabelle 4 zeigt, wie der anzuwendende Rechtsrahmen ermittelt wird.

3.1.2. Betroffene Personen müssen unterrichtet werden

Gemäß Artikel 13 der Polizeirichtlinie sowie Artikel 13 und 14 der DSGVO müssen die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Aus Tabelle 5 geht hervor, wie und wann die Person, deren Daten verarbeitet werden, zu unterrichten ist.

Tabelle 4: Ermitteln des korrekten Rechtsrahmens je nach Zweck der Datenverarbeitung

1. Zu welchem Zweck erfolgt die Datenverarbeitung?

- **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten;**
- **Strafvollstreckung;**
- **Schutz der öffentlichen Sicherheit.**

- sonstiger Zweck

2. Es gilt die Polizeirichtlinie.

2. Es gilt die Datenschutz-Grundverordnung.

3. Unionsrecht oder nationales Recht legt fest:*

- **welche personenbezogenen Daten verarbeitet werden dürfen;**
- **die spezifischen Zwecke der Datenverarbeitung.**

3. Die Datenverarbeitung ist nur unter folgenden Voraussetzungen zulässig:

- **Zustimmung** der von der Datenverarbeitung betroffenen Person liegt vor;
- erforderlich zur Erfüllung eines **Vertrags**;
- erforderlich zur Erfüllung **rechtlicher Verpflichtungen;**
- erforderlich zum Schutz **lebenswichtiger Interessen** einer Person oder
- erforderlich zur Wahrung des öffentlichen Interesses.

4. Ist der Zweck des Profilings aus der Polizeirichtlinie ausgenommen?	4. Ist der Zweck des Profilings aus der DSGVO ausgenommen?
Das Recht auf Information, das Recht auf Auskunft über die personenbezogenen Daten und das Recht auf Änderung oder Löschung personenbezogener Daten kann in den folgenden Fällen (teilweise oder vollständig) eingeschränkt werden: • zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden; • zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden; • zum Schutz der öffentlichen Sicherheit; • zum Schutz der nationalen Sicherheit; • zum Schutz der Rechte und Freiheiten anderer.	Die in der DSGVO festgelegten Verpflichtungen (Transparenz, Information und Meldung von Verletzungen des Schutzes personenbezogener Daten) und Rechte (Recht auf Auskunft, Berichtigung und Löschung von Daten, Recht auf Widerspruch und Recht, keiner automatisierten Entscheidungsfindung unterworfen zu werden) können zur Gewährleistung der folgenden Aspekte durch nationales oder EU-Recht **eingeschränkt werden**: • die nationale Sicherheit, die Landesverteidigung oder die öffentliche Sicherheit; • die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; • den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit; • den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren; • die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe; • Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt in spezifischen Fällen verbunden sind; • den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; • die Durchsetzung zivilrechtlicher Ansprüche.

Anmerkung: **Die nationalen Rechtsakte zur Umsetzung der Polizeirichtlinie sind auf der EUR-Lex-Website abrufbar.*

Quelle: *FRA, 2018*

Tabelle 5: Verpflichtung, Einzelpersonen Profiling-Informationen zur Verfügung zu stellen: Art der Daten, Kommunikationsmittel und Ausnahmen

Meldepflicht – Checkliste	
An wen?	Person, deren Daten verarbeitet werden
Wie?	• klare und verständliche Sprache, • leicht zugängliches Formular, • in der gleichen Form wie die Anfrage – *elektronische Mittel sind zu bevorzugen.*
Was?	**In Bezug auf die Verarbeitung**: • Name und Kontaktdaten Ihrer Behörde, • Kontaktdaten Ihres Datenschutzbeauftragten, • Zwecke der Verarbeitung, • Rechtsgrundlage der Verarbeitung, • maximale Dauer der Datenspeicherung, • Arten der Personen/Organisationen, die die Daten erhalten. **In Bezug auf die Rechte der Person**: • das Recht auf **Beschwerde** bei einer Aufsichtsbehörde sowie die Kontaktdaten dieser Aufsichtsbehörde, • das Recht auf **Auskunft** über die eigenen personenbezogenen Daten, • das Recht auf **Berichtigung** und/oder **Löschung** der personenbezogenen Daten, • das Recht auf **Einschränkung** der Verarbeitung.
Ausnahmen	• Es werden exzessive (d. h. wiederholte) oder offenkundig unbegründete Anfragen gestellt; • die Identität der antragstellenden Person kann nicht eindeutig bestätigt werden; • die Bereitstellung von Informationen würde Ermittlungen behindern; • die Bereitstellung von Informationen würde die Verhütung/Ermittlung von Straftaten beeinträchtigen; • zum Schutz der öffentlichen oder nationalen Sicherheit; • zum Schutz der Rechte anderer.

Quelle: *FRA, 2018*

Im Fokus: Das „Recht auf Erläuterung“

Die DSGVO sieht vor, dass im Rahmen des Profilings der betroffenen Person „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ der Datenverarbeitung mitgeteilt werden müssen. Diese Informationen sollten sowohl zum Zeitpunkt der Datenerhebung (Meldung) als auch im Zuge eines Antrags der betroffenen Person auf weitere Informationen (Auskunftsrecht) bereitgestellt werden. Dieses Recht wird in der Polizeirichtlinie nicht ausdrücklich erwähnt. In Erwägungsgrund 38 heißt es jedoch, dass eine „[automatisierte Verarbeitung] mit geeigneten Garantien verbunden sein [sollte], einschließlich der spezifischen Unterrichtung der betroffenen Person und des Rechts [...] insbesondere auf [...] Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung“.

Dieses „Recht auf Erläuterung“ ist in der Praxis aber möglicherweise nicht problemlos umsetzbar. Während einige Personen sicher über die nötige digitale Kompetenz verfügen, um den Code eines Algorithmus zu verstehen, sind für andere vereinfachte Informationen über den Zweck der Verarbeitung und die Zusammenhänge der verwendeten Daten ausreichend. Das angestrebte Ziel ist der Schlüssel zur Beurteilung der Aussagekraft der Erläuterung. Die betroffene Person sollte ausreichende Informationen erhalten, um den Zweck der Verarbeitung sowie die Begründung und die Kriterien zu verstehen, die zu einer Entscheidung geführt haben.

Das Recht auf Erläuterung ist kein absolutes Recht (siehe Schritt 4 in Tabelle 4). Die Mitgliedstaaten können dieses Recht in bestimmten Fällen gesetzlich einschränken, unter anderem zur Gewährleistung der folgenden Aspekte: Schutz der nationalen Sicherheit; Landesverteidigung; Schutz der öffentlichen Sicherheit; Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten; Strafvollstreckung; Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; Durchsetzung zivilrechtlicher Ansprüche.

Die Bereitstellung angemessener Informationen über den Zweck und die voraussichtlichen Folgen der Verarbeitung ist dennoch eine empfehlenswerte bewährte Vorgehensweise. Die Entwicklung einfacher Möglichkeiten, die

angewendete Logik und die Kriterien für eine Entscheidung zu erläutern, wird letztlich die Transparenz und Rechenschaftspflicht erhöhen.

Weitere Informationen: siehe DSGVO, Artikel 13 bis 15 (Recht auf Information und Auskunftsrecht), Artikel 22 (automatisierte Entscheidungsfindung im Einzelfall, einschließlich Profiling) und Artikel 23 (Beschränkungen) sowie Polizeirichtlinie, Artikel 11 (automatisierte Entscheidungsfindung im Einzelfall, einschließlich Profiling) und Artikel 13 bis 15 (Recht auf Information und Auskunftsrecht). Siehe auch Artikel29-Datenschutzgruppe (2018a).

3.1.3. Daten sicher aufbewahren: Aufzeichnungen, Protokolle und Speichervorgaben

Behörden, die personenbezogene Daten zum Zwecke des Profilings erheben und verarbeiten, sind nicht nur zur gesetzeskonformen Verarbeitung dieser Daten verpflichtet, sondern müssen auch sicherstellen, dass die Daten nicht:

- von unbefugten Personen eingesehen werden;
- für einen anderen als den ursprünglich vorgesehenen Zweck verwendet werden;
- länger als erforderlich aufbewahrt werden.

Hierzu müssen die Behörden wie auch die Beamtinnen und Beamten im Bereich der Strafverfolgung und des Grenzmanagements sicherstellen, dass geeignete Maßnahmen zum Schutz der Integrität und Sicherheit der Daten ergriffen werden. Sie müssen jeden Zugriff auf die Daten und deren Verwendung nachverfolgen, indem sie Aufzeichnungen über alle Verarbeitungstätigkeiten oder Kategorien von Verarbeitungstätigkeiten führen und verwalten (Artikel 30 DSGVO und Artikel 24 der Polizeirichtlinie). Diese Verzeichnisse müssen folgende Angaben enthalten:

- den **Namen** und die **Kontaktdaten** der Behörden und der/des Datenschutzbeauftragten;
- den **Zweck** der Verarbeitung;

- die **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;

- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

- den **Verwendungszweck des Profilings**;

- eine Angabe der **Rechtsgrundlage** für den Verarbeitungsvorgang;

- wenn möglich, die vorgesehenen **Fristen** für die Löschung der verschiedenen Kategorien personenbezogener Daten;

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO oder Artikel 29 Absatz 1 der Polizeirichtlinie.

Wenn computergestütztes Profiling für in der Polizeirichtlinie festgelegte Zwecke (siehe Abschnitt 3.2) durchgeführt wird, müssen die Behörden darüber hinaus Protokolle über folgende Tätigkeiten führen: Erhebung, Änderung, Abfrage, Offenlegung, einschließlich der Übermittlung, Zusammenführung und Löschung von Daten.

Diese Aufzeichnungen und Protokolle unterstützen die Beamtinnen und Beamten dabei, die Einhaltung der gesetzlichen Anforderungen bei der internen und externen Überwachung nachzuweisen. Wenn beispielsweise eine Person eine Beschwerde einreicht, sind die Strafverfolgungs- und Grenzschutzbehörden verpflichtet, den nationalen Datenschutzbehörden diese Aufzeichnungen und Protokolle zur Verfügung zu stellen.

Die personenbezogenen Daten sollten nicht länger aufbewahrt werden, als es zum Erreichen des festgelegten rechtmäßigen Zwecks erforderlich ist. Die Aufbewahrung über einen darüber hinausgehenden Zeitraum muss hinreichend begründet werden. In solchen Fällen sollten die Behörden sicherstellen, dass die Datenspeicherung regelmäßig überprüft wird, um die Integrität und Sicherheit der Daten zu gewährleisten.

3.1.4. Die unrechtmäßige Verarbeitung von Daten muss aufgedeckt und verhindert werden

Die Aufdeckung und Verhinderung der unrechtmäßigen Verarbeitung personenbezogener Daten ist eine große Herausforderung. Die zum Verständnis komplexer Algorithmen und großer Datenbanken erforderlichen Fachkenntnisse erschweren die Sicherstellung ordnungsgemäßer Kontrollen.

Um dieses Problem anzugehen, wurden in die DSGVO und die Polizeirichtlinie bestimmte Garantien aufgenommen, die die Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten vor, während und nach der Datenverarbeitung leiten sollen. Diese beziehen sich auf:

- Datenschutz-Folgenabschätzungen sowie
- Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen.

Folgenabschätzungen

Gemäß dem Rechtsrahmen der EU müssen die Polizei- und Grenzschutzbehörden vorab eine Folgenabschätzung durchführen, wenn die Form der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte des Einzelnen zur Folge hat (Artikel 35 DSGVO und Artikel 27 der Polizeirichtlinie). Das bedeutet, dass Folgenabschätzungen nicht nur dann durchzuführen sind, wenn das Ergebnis der Datenverarbeitung einen Verstoß gegen Datenschutzstandards oder Standards zum Schutz der Privatsphäre darstellen könnte, sondern in jeder Situation, in der eine Verletzung *eines Grundrechts* vorliegen kann. Dies kann die folgenden Rechte betreffen: Recht auf Gleichbehandlung und Nichtdiskriminierung; Meinungs- und Informationsfreiheit; Gedanken-, Gewissens- und Religionsfreiheit; Recht auf medizinische Versorgung; Recht auf Asyl; Schutz bei Abschiebung, Ausweisung und Auslieferung.

Folgenabschätzungen sind besonders wichtig, wenn das Profiling rechtliche Folgen für die betreffende(n) Person(en) haben könnte. In diesen Fällen schreiben die DSGVO und die Polizeirichtlinie die Durchführung von Folgenabschätzungen vor.

Die Folgenabschätzungen müssen vor der automatischen Datenverarbeitung durchgeführt werden. Dabei werden jedoch, je nach Situation, unterschiedliche Ziele verfolgt:

- *a priori*: Eine Folgenabschätzung, die vor Beginn der Datenverarbeitung durchgeführt wird, gibt Auskunft über die Qualität der Daten und/oder den Algorithmus, der dem Verarbeitungsvorgang zugrunde liegt, und trägt dazu bei, mögliche Grundrechtsverletzungen aufzudecken und gegebenenfalls zu beheben.

- *a posteriori*: Wenn die Daten verarbeitet wurden, kann der Beamtin bzw. dem Beamten der Nachweis abverlangt werden, dass sie/er rechtmäßig gehandelt hat. Die Folgenabschätzung kann ihr/ihm dabei als Beleg dienen, dass alle notwendigen Maßnahmen ergriffen wurden, um die Einhaltung der gesetzlichen Vorgaben zu gewährleisten.

Darüber hinaus unterstützen Folgenabschätzungen die Beamtinnen und Beamten auch dabei, versteckte Vorurteile aufzudecken, die das Recht auf Datenschutz und Nichtdiskriminierung verletzen und sich auf die Qualität des Profilings auswirken können (siehe Abschnitt 1.3.2).

Im Fokus: Risiken im Zusammenhang mit dem Einsatz „dynamischer Algorithmen"

Dynamische Algorithmen sind Algorithmen, die auf Basis von Feedbackschleifen ständig neu definiert und verbessert werden. Diese Schleifen werden von den algorithmischen Systemen selbst erzeugt und können nicht vollständig verstanden oder gar in einfacher Sprache ausgedrückt werden (siehe Artikel 35 DSGVO und Artikel 27 der Polizeirichtlinie). Anders als statische Algorithmen, die auf vorgegebenen Kriterien basieren, erzeugen die dynamischen Algorithmen **neue Korrelationen**, indem sie sich ständig neu definieren.

Dynamische Algorithmen bergen das Risiko, dass selbst erfahrene Programmiererinnen und Programmierer irgendwann die Logik hinter dem Algorithmus nicht mehr kennen. Dadurch besteht große **Gefahr, dass bestehende Vorurteile unfreiwillig reproduziert werden** und soziale Ungleichheiten und die Stigmatisierung bestimmter Gruppen aufrechterhalten werden. In solchen Fällen ist es sehr schwierig, die Rechenschaftspflicht und den Rechtsschutz für die betroffenen Personen zu gewährleisten.

Die Verwendung dynamischer Algorithmen sollte daher **vermieden oder begrenzt** werden, um so das Risiko, den Überblick über die

Bewertungskriterien zu verlieren, möglichst gering zu halten. Interne wie auch externe Prüferinnen und Prüfer können dadurch die Algorithmen bewerten und, wenn sie sich als unrechtmäßig erweisen, auch ändern. Wenn die Verwendung dynamischer Algorithmen begründet werden kann, sind die Risikoindikatoren zu überprüfen und zu testen, damit sichergestellt ist, dass sie nicht zu einem unrechtmäßigen Profiling führen.

Weitere Informationen: siehe Gandy, O. (2010) und Korff, D. (2015).

Folgenabschätzungen können je nach Art und Umfang der verarbeiteten personenbezogenen Daten sowie Art und Zweck der Verarbeitung erheblich variieren. Sie können beispielsweise eine Überprüfung der Qualität der Daten, technische Kontrollen der bei der Verarbeitung eingesetzten Algorithmen und/oder eine vollständige Überprüfung der Ziele der Datenverarbeitung umfassen. In Abbildung 13 sind die Mindestkriterien ersichtlich, die in diesem Zusammenhang bewertet werden sollten.

Die Artikel29-Datenschutzgruppe (nun abgelöst durch den Europäischen Datenschutzausschuss), in der die nationalen Datenschutzbehörden aus den EU-Mitgliedstaaten vertreten sind, hat Leitlinien mit weiteren Informationen in Bezug auf Datenschutz-Folgenabschätzungen entwickelt. Diese Leitlinien enthalten eine detaillierte Darstellung der Kriterien, die bei der Durchführung von Folgenabschätzungen zu berücksichtigen sind.[40]

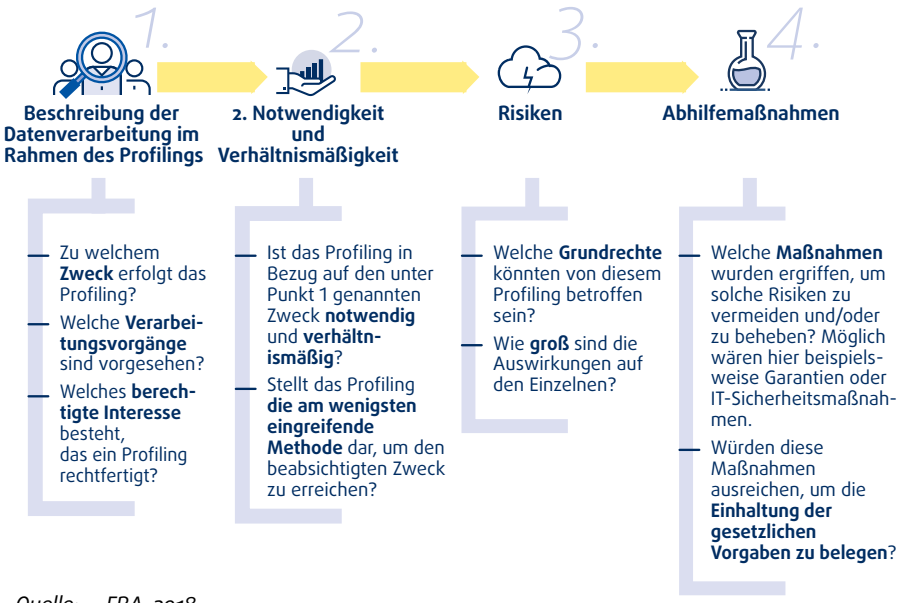
Einbettung der Rechtmäßigkeit durch Technikgestaltung oder durch datenschutzfreundliche Voreinstellungen

Unabhängig davon, ob im Rahmen einer Folgenabschätzung die Möglichkeit einer Grundrechtsverletzung festgestellt wurde, können Maßnahmen ergriffen werden, um das Risiko einer Rechtswidrigkeit zu verhindern. Diese Maßnahmen werden als Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen bezeichnet (Artikel 25 DSGVO und Artikel 20 der Polizeirichtlinie).

Mit dem Datenschutz durch Technikgestaltung soll sichergestellt werden, dass sowohl *vor* als auch *während* der Datenverarbeitung technische und organisatorische Maßnahmen zur Gewährleistung der Datenschutzgrundsätze ergriffen werden.

40 Artikel29-Datenschutzgruppe (2017a).

Abbildung 13: Mindestanforderungen bei Folgenabschätzungen



Quelle: FRA, 2018

So könnten beispielsweise personenbezogene Daten, soweit möglich, „pseudonymisiert" werden. Die Pseudonymisierung ist eine Maßnahme, durch die personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen, die gesondert aufbewahrt werden, nicht mehr einer einzelnen Person zugeordnet werden können. Der „Schlüssel", der die erneute Identifizierung der Personen ermöglicht, ist gesondert und sicher aufzubewahren.[41] Im Gegensatz zu anonymisierten Daten sind pseudonymisierte Daten nach wie vor personenbezogene Daten und unterliegen daher den Datenschutzbestimmungen und grundsätzen.

Beim Datenschutz durch datenschutzfreundliche Voreinstellungen ist sichergestellt, dass „grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden".[42] Dies hat Auswirkungen auf:

- die Menge der erhobenen und gespeicherten personenbezogenen Daten;

41 FRA, EDSB und Europarat (2018), S. 83.

42 Datenschutz-Grundverordnung (DSGVO), Artikel 25.

- die Arten der Verarbeitung im Zusammenhang mit personenbezogenen Daten;
- die maximale Speicherdauer;
- die Anzahl der Personen, die Zugang zu diesen personenbezogenen Daten erhalten.

Im Fokus: Rechenschaftspflicht

Das primäre Ziel des Datenschutzes durch Technikgestaltung und des Datenschutzes durch datenschutzfreundliche Voreinstellungen ist es, Strafverfolgungs- und Grenzschutzbehörden und -beamte bei der Entwicklung von Programmen für das algorithmische Profiling zu unterstützen, die den Grundrechtsanforderungen, insbesondere den Grundsätzen der **Rechtmäßigkeit**, **Transparenz** und **Sicherheit**, genügen.

Solche Maßnahmen können jedoch auch verdeutlichen, wie die Behörden die rechtliche Anforderung der **Rechenschaftspflicht** erfüllen. Behörden, die Daten verarbeiten, sind gesetzlich dazu verpflichtet, „geeignete technische und organisatorische Maßnahmen" durchzuführen, die im Einklang mit dem EU-Recht stehen. Ein Beispiel: Wenn eine Person eine Beschwerde einreicht, können die nationalen Justiz- und Datenschutzbehörden die betreffenden Behörden ersuchen, jeden der folgenden Punkte nachzuweisen:

- die Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit des computergestützten Profiling;
- die Rechtmäßigkeit des Zwecks;
- die Informationen, die einzelnen Personen zur Verfügung gestellt werden;
- die Integrität und Sicherheit der Daten;
- die Qualitätsmaßnahmen und kontrollen, die vor und während des Profilings durchgeführt werden.

3.2. Umfangreiche Datenbanken für Grenzmanagement- und Sicherheitszwecke

Die EU hat mehrere IT-Großsysteme oder Mechanismen für die Erhebung und Verarbeitung von Daten entwickelt, die für das Grenzmanagement und die Migrationsverwaltung und bis zu einem gewissen Grad auch für Strafverfolgungszwecke genutzt werden können. Sie dienen als Beispiele zur Veranschaulichung einiger der gängigsten Herausforderungen im Zusammenhang mit dem Einsatz von algorithmischem Profiling sowie möglichen Garantien.

Tabelle 6 stellt diese IT-Systeme und -Mechanismen der EU kurz vor. Der Anhang bietet einen ausführlichen Überblick über die vorhandenen und geplanten IT-Großsysteme der EU (Stand: März 2018).

Die IT-Großsysteme der EU kommen in einer Reihe von Verfahren im Zusammenhang mit der Migration zum Einsatz, u. a. bei der Bewertung des Vorabrisikos vor der Einreise, bei Asylverfahren, bei Visumantragsverfahren, während der Grenzkontrollen, bei der Ausgabe von Aufenthaltstiteln, bei der Festnahme von Migrantinnen und Migranten in einer irregulären Situation, bei Rückführungsverfahren und bei der Verhängung von Einreiseverboten. Die von der EU eingerichteten IT-Systeme, einschließlich jener, die ursprünglich für Asyl- und Migrationsverwaltungszwecke geschaffen wurden, werden zunehmend auch im Kontext der inneren Sicherheit eingesetzt, beispielsweise bei Polizeikontrollen und bei der Bekämpfung von schwerer Kriminalität und Terrorismus.

Die meisten der nach EU-Recht eingerichteten Systeme konzentrieren sich auf die Identifizierung einer bestimmten Person durch den Abgleich alphanumerischer oder biometrischer Daten (derzeit Fingerabdrücke) mit bereits im System vorhandenen Informationen. Mit einigen Ausnahmen (siehe „Im Fokus: Algorithmisches Profiling in EU-Instrumenten") enthalten sie selbst keinen eigenen Algorithmus, der es ermöglichen würde, eine Person anhand eines Profils zu ermitteln. Sie können jedoch zur Erstellung anonymisierter Statistiken verwendet werden, einschließlich solcher über sogenannte Schutzmerkmale, wie das Geschlecht oder das Alter (siehe Abschnitt 1.2.1).

Solche Statistiken könnten herangezogen werden, um Risikoprofile zu erstellen, die bei künftigen Grenzschutz- oder Polizeientscheidungen angewendet werden. Im

Tabelle 6: Ausgewählte EU-Instrumente für die Verarbeitung großer Datenmengen im Grenzmanagement und in der Strafverfolgung

Datenbank	Akronym	Hauptzweck
Schengener Informationssystem	*SIS II*	Erfassung und Bearbeitung von Ausschreibungen von gesuchten oder vermissten Personen zur Gewährleistung der Sicherheit; Erfassung und Bearbeitung von Ausschreibungen von Drittstaatsangehörigen zur Einreise- oder Aufenthaltsverweigerung; Erfassung und Bearbeitung von Ausschreibungen von Drittstaatsangehörigen, gegen die eine Rückführungsentscheidung ergangen ist
Visa-Informationssystem	*VIS*	Erleichterung des Datenaustauschs zu Visumanträgen zwischen den Schengen-Mitgliedstaaten
Europäisches System für den Abgleich von Fingerabdruckdaten	*Eurodac*	Bestimmung des für die Prüfung des Antrags auf internationalen Schutz zuständigen Mitgliedstaats und Unterstützung bei der Bekämpfung der irregulären Zuwanderung und Sekundärmigration
Einreise-/Ausreisesystem	*EES*	Berechnung und Überwachung der Dauer des zulässigen Aufenthalts von Drittstaatsangehörigen und Ermittlung von Aufenthaltsüberziehern
Fluggastdatensätze	*PNR*	Erhebung, Verarbeitung und Austausch von Fluggastdaten bei Flügen aus Drittländern („Drittstaatsflüge").* Kommen streng genommen nur für Strafverfolgungszwecke zum Einsatz.
Vorab übermittelte Fluggastdaten	*API*	Erhebung und Verarbeitung von Fluggastdaten bei Flügen aus Drittländern („Drittstaatsflüge") zu Grenzmanagement- und Strafverfolgungszwecken
Europäisches Reiseinformations- und genehmigungssystem	*ETIAS*	•berprüfung, ob ein Drittstaatsangehöriger ohne Visum ein Sicherheitsrisiko, ein Risiko in Bezug auf irreguläre Migration oder ein Risiko für die öffentliche Gesundheit darstellt
Europäisches Strafregisterinformationssystem für Drittstaatsangehörige	*ECRIS-TCN*	Austausch von Informationen über frühere Verurteilungen von Drittstaatsangehörigen

*Anmerkung: * Darüber hinaus haben die Mitgliedstaaten gemäß Artikel 2 der Verordnung (EU) 2016/681 die Möglichkeit, auch Daten aus Flügen innerhalb der Europäischen Union (EU-Flüge) zu verarbeiten.*

Quelle: FRA, 2018

Rahmen des umfassenderen Programms für die Interoperabilität der IT-Systeme der EU wird die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) für die Verwaltung des zentralen Speichers für Berichte und Statistiken (Central Repository for Reporting and Statistics, CRRS) zuständig sein. Dieser Speicher stützt sich auf Daten aus bestehenden EU-Datenbanken (Einreise-/Ausreisesystem, ETIAS, Schengener Informationssystem und Visa-Informationssystem), um Statistiken und Analyseberichte für EU- und nationale Stellen zu generieren.[43]

Im Fokus: Algorithmisches Profiling in EU-Instrumenten

Einige bestehende EU-Instrumente sehen für die Erstellung von Risikoprofilen die Verwendung von aus ihren Daten abgeleiteten Statistiken vor. Neben der Identifizierung „bekannter" spezifischer Verdächtiger enthalten sie eine Funktion für algorithmisches Profiling, um auch „unbekannte" Personen zu identifizieren, die für Strafverfolgungs- und Grenzschutzbehörden von Interesse sein könnten.

Das im September 2018 verabschiedete, aber zum Zeitpunkt der Erstellung dieses Handbuchs noch nicht in Kraft getretene **Europäische Reiseinformations- und genehmigungssystem (ETIAS)**[44] prüft vor Erteilung der Reisegenehmigung, ob von der Visumpflicht befreite Drittstaatsangehörige ein Risiko in Bezug auf irreguläre Migration, die Sicherheit oder die öffentliche Gesundheit darstellen. Die von den Reisenden während des Antragsverfahrens gemachten Angaben werden automatisch mit den einschlägigen EU- und internationalen Datenbanken sowie einer Reihe von Risikoindikatoren („Überprüfungsvorschriften") abgeglichen, die im ETIAS-System selbst hinterlegt sind. Ein von Frontex entwickelter

43 Europäische Kommission (2017), *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226*, COM(2017) 793 final, Straßburg, 12. Dezember 2017; Europäische Kommission (2017), *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)*, COM(2017) 794 final, Brüssel, 12. Dezember 2017.

44 Europäische Kommission (2018), *Verordnung(EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226,* COM(2016) 731 final, Brüssel, 16. November 2016, Artikel 33 Absatz 5.

Algorithmus vergleicht das individuelle Profil der oder des Reisenden (basierend auf Indikatoren wie Alter, Geschlecht, Staatsangehörigkeit, Wohnort, Bildungsabschluss und Beruf) mit diesen Risikoindikatoren, um zu bestimmen, ob der Antrag manuell überprüft werden sollte.

Fluggastdatensätze (PNR-Daten) werden von den Fluggesellschaften erhoben. Die Grundlage bilden Informationen, die von den Passagieren über die Flugreservierungssysteme zur Verfügung gestellt werden, beispielsweise Reisedaten und routen, Kontakt- und Zahlungsdaten, Gepäckinformationen und andere „allgemeine Hinweise" wie z. B. Ernährungspräferenzen. Diese Daten werden nicht in einer zentralen EU-Datenbank erhoben. Gemäß der EU-Richtlinie über die Verwendung von Fluggastdatensätzen (PNR-Daten)[45] sind die Fluggesellschaften jedoch verpflichtet, die Daten an eine sogenannte PNR-Zentralstelle zu übermitteln, die die erhaltenen Informationen dann zum Zwecke der Bekämpfung von terroristischen Straftaten und schwerer Kriminalität analysiert. Neben der Erkennung von Grenzübertritten bekannter Personen können diese Daten auch mit spezifischen Risikoindikatoren („im Voraus festgelegte Kriterien") abgeglichen werden, um bis dato noch unbekannte Bedrohungen zu identifizieren. Diese Kriterien werden von den PNR-Zentralstellen festgelegt und auf der Grundlage neuer im System verfügbarer Daten und Muster aktualisiert.

3.2.1. Minimierung der mit der Verarbeitung von Daten in umfangreichen Datenbanken verbundenen Risiken für die Grundrechte

Die Daten von Reisenden, wie deren Staatsangehörigkeit, Geschlecht und Alter, werden heute beim Profiling, einschließlich des algorithmischen Profiling, in einer Größenordnung verwendet, die in der Vergangenheit nicht möglich war. Auch wenn diese Daten anonymisiert werden, ist ihre Verarbeitung dennoch mit Risiken verbunden. Eine bewusste oder unbewusste Voreingenommenheit bei der Auswahl der Risikoindikatoren, der Gestaltung der Algorithmen oder der Interpretation der

45 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119, Artikel 6 Absatz 4.

Ergebnisse könnte zu operativen Maßnahmen führen, die wiederum eine Diskriminierung bestimmter Personengruppen zur Folge haben könnten.[46]

Dieser Abschnitt befasst sich mit einigen dieser Risiken und unterbreitet verschiedene Möglichkeiten zu deren Minimierung. Er baut auf zwölf operativen Grundrechtsüberlegungen der FRA bei der Verarbeitung von PNR-Daten zu Strafverfolgungszwecken auf (siehe Fallstudie). Auch wenn diese Grundrechtsüberlegungen im spezifischen Kontext der PNR-Datenverarbeitung konzipiert wurden, sind einige von ihnen doch allgemeiner anwendbar und können als Garantien zur Minderung der Risiken im Zusammenhang mit dem algorithmischen Profiling betrachtet werden.

Fallstudie

Operative Leitlinien der FRA für den Aufbau nationaler PNR-Systeme

In Ermangelung einer Richtlinie zur Erhebung von PNR-Daten forderte die Europäische Kommission die FRA im Jahr 2014 auf, praktische Leitlinien für die Verarbeitung von PNR-Daten zu Strafverfolgungszwecken für diejenigen Mitgliedstaaten bereitzustellen, die vorhaben, eigene nationale PNR-Systeme einzurichten. Im Mittelpunkt dieser Leitlinien standen das Recht auf Achtung des Privatlebens (Artikel 7 der Charta), das Recht auf Schutz personenbezogener Daten (Artikel 8 der Charta) und das Recht auf Nichtdiskriminierung (Artikel 21 der Charta). Einige der vorgeschlagenen Garantien flossen später in die EU-Richtlinie über PNR-Daten ein.

Die zwölf Grundrechtsüberlegungen im Zusammenhang mit der Verarbeitung von PNR-Daten zu Strafverfolgungszwecken lauten:

- PNR-Daten werden nur zur Bekämpfung von Terrorismus und schwerer transnationaler Kriminalität verwendet;
- der Zugriff auf die PNR-Datenbank ist auf eine spezialisierte Einheit zu beschränken;
- ein direkter Zugriff auf die Datenbanken der Fluggesellschaften wird nicht angefordert;
- sensible PNR-Daten werden gelöscht;

46 Weitere Informationen: siehe FRA (2017e) und FRA (2018a).

- es sind strenge Sicherheits- und Rückverfolgbarkeitsgarantien gegen Missbrauch festzulegen;
- die Wahrscheinlichkeit von falsch positiven Treffern ist zu minimieren;
- die Transparenz gegenüber den Passagieren ist zu gewährleisten;
- Personen muss der Zugang zu ihren PNR-Daten und eine Korrektur dieser Daten ermöglicht werden;
- die Identifizierung der betroffenen Personen oder die Aufbewahrung von Daten ist nicht länger als nötig zuzulassen;
- die aus den PNR-Daten gewonnenen Informationen dürfen ausschließlich an die zuständigen nationalen Behörden übermittelt werden;
- die aus den PNR-Daten gewonnenen Informationen dürfen nur unter strengen Bedingungen an Drittländer übermittelt werden;
- das PNR-System ist objektiv und transparent zu bewerten.

Weitere Informationen: siehe FRA (2014c).

Die Verarbeitung von Daten, die geschützte Merkmale offenbaren, sollte notwendig und verhältnismäßig sein

Eine Besonderheit des algorithmischen Profilings liegt darin, dass die Berücksichtigung personenbezogener Merkmale, die im Zusammenhang mit geschützten Merkmalen stehen, ein besonders hohes Diskriminierungsrisiko birgt.[47] Im Kontext der EU verbieten sowohl die ETIAS- als auch die PNR-Gesetzgebung, dass die Risikoindikatoren auf Kriterien gestützt werden, die ein hohes Diskriminierungsrisiko mit sich bringen, einschließlich Rasse, ethnischer Herkunft oder religiöser Überzeugung. Aber auch wenn derlei Daten nicht vorliegen, können andere Arten von Daten eng mit diesen Merkmalen verbunden werden und so effektiv als Gründe vorgeschoben werden, die diese Schutzmerkmale widerspiegeln. So könnte z. B. die Kategorie „Allgemeine Hinweise" im Zusammenhang mit den PNR-Daten, in der möglicherweise Ernährungspräferenzen der Reisenden angegeben werden, bestimmte religiöse Überzeugungen offenbaren.

Ebenso könnten spezifische Kombinationen der vom Algorithmus verwendeten Daten bestimmte Kategorien von Personen benachteiligen. So können Personen

47 Europäischer Datenschutzbeauftragter (2018).

aufgrund ihrer ethnischen oder sozialen Herkunft oder der Zugehörigkeit zu einer nationalen Minderheit benachteiligt werden, also aus Gründen, bei denen es sich nach Artikel 21 der Charta um geschützte Merkmale handelt. Wenn z. B. in ETIAS ein Risikoprofil in Bezug auf das Risiko der irregulären Migration auf der Kombination einer bestimmten Staatsangehörigkeit und Berufsgruppe beruht, kann dies dazu führen, dass eine ethnische Gruppe oder Menschen mit einer bestimmten Staatsangehörigkeit, die in einem bestimmten Land in der Regel in einem bestimmten Wirtschaftszweig wie dem Baugewerbe oder der Landwirtschaft arbeiten, ins Visier genommen werden.[48]

- Die Verarbeitung von Daten, die Merkmale aufweisen, die durch Artikel 21 der Charta geschützt sind, sollte auf das absolut notwendige und angemessene Maß beschränkt sein und niemals zu Diskriminierung führen. Vor Beginn jeder Verarbeitung sollte die zuständige Behörde die Daten bewerten, um geschützte Merkmale zu identifizieren und Daten zu entfernen, deren Verarbeitung nicht rechtmäßig wäre. Als gute Praxis sollte diese Bewertung durch ein Programm ergänzt werden, bei dem die Daten mit einem regelmäßig aktualisierten Glossar „sensibler Begriffe" abgeglichen und ggf. entfernt werden.

Die Kriterien für das Profiling sollten spezifisch und zielgerichtet sein

Ein weiteres Risiko ergibt sich aus der Anwendung **weit gefasster Kriterien für das Profiling**. Die bestehenden EU-Instrumente lassen bei der Entwicklung von Algorithmen für das Profiling einen erheblichen Ermessensspielraum. Um das Risiko der irregulären Migration zu bewerten, sieht ETIAS die Verwendung von EU-weiten und nationalen Statistiken zum Anteil der Überziehungen und Einreiseverboten vor. Im Hinblick auf Sicherheitsrisiken bezieht ETIAS sich jedoch nur allgemein auf Informationen über spezifische Sicherheitsindikatoren und Bedrohungen. Die PNR-Richtlinie enthält allgemeine Hinweise für die Gestaltung von Algorithmen, gibt aber weder an, welche Kriterien für die Identifizierung von Personen zu verwenden sind, die möglicherweise an einer terroristischen Straftat oder einem schweren Verbrechen beteiligt sind, noch, wie ein bestimmtes Kriterium zu gewichten ist.

Zu weit gefasste Kriterien führen zu einer signifikanten Anzahl „falsch positiver Treffer", da Personen fälschlicherweise einem bestimmten Risikoprofil zugeordnet werden. Einige dieser falsch positiven Treffer können auch diskriminierender Natur sein. So bedeutet beispielsweise eine zu weit gefasste Definition des Kriteriums „frühere

48 Siehe auch FRA (2017a).

strafrechtliche Verurteilung", dass LGBT-Personen verpflichtet wären, Strafregistereinträge im Zusammenhang mit bestimmten sexuellen Handlungen, die in einigen Nicht-EU-Ländern unter Strafe gestellt sind, zu melden.

- Die Bewertungskriterien sollten vorab festgelegt, zielgerichtet, spezifisch, verhältnismäßig und faktenbasiert sein. Außerdem sollten sie an anonymisierten Stichproben getestet werden. Sie sollten regelmäßig von einem internen Prüfer darauf geprüft werden, ob sie durch ihre spezifischen Ziele nach wie vor gerechtfertigt sind.

- Bevor eine Ausschreibung auf der Grundlage einer automatisierten Verarbeitung für weitere Maßnahmen übermittelt wird, sollte die zuständige Behörde die Daten in Verbindung mit anderen Informationen manuell überprüfen, um festzustellen, ob die Person dem Risikoprofil entspricht, und mögliche falsch positive Treffer beseitigen. Die Datenempfänger sollten eine Rückmeldung über die aufgrund der Ausschreibung getroffenen Maßnahmen geben.

Die verarbeiteten Daten sollten genau und verlässlich sein

Die Untersuchungen der FRA bestätigen, dass die vorhandenen IT-Großsysteme eine erhebliche Menge an ungenauen Daten enthalten.[49] **Ungenaue oder unzuverlässige Daten** können im Rahmen des algorithmischen Profilings für Grenzmanagement- oder Strafverfolgungszwecke zahlreiche negative Auswirkungen haben. Ungenaue Daten können sich nachteilig auf den Einzelnen auswirken, aber auch zu falschen Zusammenhängen und einem verzerrten Bild führen, wodurch wiederum die Wirksamkeit der Arbeit von Polizei und Grenzschutz beeinträchtigt wird.

Dies gilt insbesondere für Daten, die von den Bürgern und Bürgerinnen eingegeben werden, beispielsweise bei den PNR-Daten und ETIAS-Anträgen, die anfälliger für Fehler sein können als offizielle Aufzeichnungen. Die Überprüfung von Social-Media-Konten, die von einigen Reisegenehmigungssystemen außerhalb der EU vorgesehen ist, birgt ein hohes Risiko, dass unzuverlässige Informationen in das Profiling einfließen. Darüber hinaus besteht dabei insbesondere das Risiko, dass Informationen erhoben werden, die Aufschluss über sensible, durch die Charta geschützte personenbezogene Daten geben, wie z. B. politische Meinungen oder Informationen über das Sexualleben der Personen.

49 Siehe FRA (2018c), S. 81-98.

- Stellen Sie Einzelpersonen genaue Informationen über die Erhebung, Speicherung und Verarbeitung ihrer Daten und über die geltenden Datenschutzgrundsätze zur Verfügung. Jede einzelne Person sollte über ihre Rechte aufgeklärt werden, einschließlich der ihr zur Verfügung stehenden Beschwerdeverfahren.

- Ermöglichen Sie es den Personen, sich um die Berichtigung ihrer Daten zu kümmern, wenn die Daten unrichtig sind, und darüber informiert zu werden, ob die Daten berichtigt oder gelöscht wurden.

- Sehen Sie wirksame administrative und gerichtliche Rechtsbehelfe für den Fall vor, dass gegen Datenschutzrechte verstoßen wird, einschließlich der Auskunftsverweigerung oder der Verweigerung, unrichtige Daten zu korrigieren oder zu löschen.

Schlussfolgerung

Profiling ist ein rechtmäßiges Verfahren, das von Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten zur Verhinderung, Ermittlung und Verfolgung von kriminellen Handlungen sowie zur Verhinderung und Aufdeckung irregulärer Zuwanderung eingesetzt wird.

Damit das Profiling rechtmäßig, fair und wirksam ist, muss es innerhalb der Grenzen des Gesetzes erfolgen. Insbesondere müssen dabei der Grundsatz der Gleichbehandlung und die Anforderungen in Bezug auf den Schutz personenbezogener Daten gewahrt werden.

Dies wird durch eine Kombination verschiedener Elemente erreicht. Beim Profiling sollte stets Folgendes beachtet werden:

- jede(r) Einzelne ist gleichberechtigt, mit Respekt und Würde zu behandeln;
- vermeiden Sie es, einzelne Personen aufgrund von Vorurteilen einem bestimmten Profil zuzuordnen;
- handeln Sie vernünftig, objektiv und erkenntnisorientiert;
- schützen Sie die personenbezogenen Daten und das Privatleben der betreffenden Person.

Den Polizei- und Grenzschutzbeamtinnen und -beamten stehen verschiedene Instrumente zur Verfügung, um sicherzustellen, dass diese Grundsätze bekannt sind, verstanden und in der Praxis eingehalten werden:

- vor dem Profiling sollten die Beamtinnen und Beamten entsprechende Anweisungen und Schulungen erhalten;
- während des Profilings sollten die Einzelheiten der Handlung aufgezeichnet und gespeichert werden;
- nach dem Profiling sollten die Maßnahmen der Beamtinnen und Beamten überprüft und bewertet werden, um einen möglichen Verbesserungsbedarf zu ermitteln.

Durch die Verhinderung eines unrechtmäßigen Profilings sind die Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten nicht nur gesetzlich geschützt, sondern es ist auch gewährleistet, dass ihre Handlungen von der breiten Öffentlichkeit verstanden und akzeptiert werden. Die Stärkung des Vertrauens in die Strafverfolgung und das Grenzmanagement verbessert die Wirksamkeit der Arbeit von Polizei und Grenzschutz und trägt somit dazu bei, die Sicherheit in der gesamten Gesellschaft zu erhöhen.

Anhang

Tabelle 7: Vorhandene und geplante IT-Großsysteme der EU

IT-System	Hauptzweck	Betroffene Personen	Geltungsbereich	Rechtsinstrument/ Vorschlag	Biometrische Identifikatoren
Europäisches System für den Abgleich von Fingerabdruckdaten (Eurodac)	Bestimmung des für die Prüfung des Antrags auf internationalen Schutz zuständigen Mitgliedstaats *Unterstützung bei der Bekämpfung der irregulären Zuwanderung und Sekundärmigration*	Antragsteller und Personen, die internationalen Schutz genießen, *Migranten in einer irregulären Situation*	28 EU-Mitgliedstaaten + SAC	Verordnung (EU) Nr. 603/2013 (Eurodac-Verordnung) *COM(2016) 272 final (Vorschlag für eine Neufassung der Eurodac-Verordnung)*	
Visa-Informationssystem (VIS)	Erleichterung des Datenaustauschs zu Visumanträgen zwischen den Schengen-Mitgliedstaaten	Antragsteller und Bürgen	24 EUMS (außer CY, HR, IE, UK)[1] + SAC	Verordnung (EG) Nr. 767/2008 (VIS-Verordnung)	
Schengener Informationssystem (SIS II) – Polizei	Gewährleistung der Sicherheit in der EU und den Schengen-Mitgliedstaaten	Vermisste oder gesuchte Personen	26 EUMS (außer CY, IE)[2] + SAC	Beschluss 2007/533/JI des Rates (Beschluss zu SIS II) *COM(2016) 883 final (Vorschlag für die SIS-II-Verordnung im Bereich der polizeilichen Zusammenarbeit)*	
Schengener Informationssystem (SIS II) – Grenzen	Ausschreibungen zum Zwecke des Verbots der Einreise oder des Aufenthalts in den Schengen-Mitgliedstaaten erfassen und bearbeiten	Migranten in einer irregulären Situation	25 EUMS (außer CY, IE, UK)[2] + SAC	Verordnung (EG) Nr. 1987/2006 (SIS-II-Verordnung) *COM(2016) 882 final (Vorschlag für die SIS-II-Verordnung im Bereich der Grenzkontrollen)*	

Schengener Informationssystem (SIS II) – Rückführungen	*Ausschreibungen von Drittstaatsangehörigen erfassen und bearbeiten, gegen die eine Rückführungsentscheidung ergangen ist*	*Migranten in einer irregulären Situation*	*25 EUMS (außer CY, IE, UK)[2] + SAC*	*COM(2016) 881 final (Vorschlag für die SIS-II-Verordnung in Bezug auf die Rückkehr illegal aufhältiger Drittstaatsangehöriger)*	
Einreise-/ Ausreisesystem (EES)	*Berechnung und Überwachung der Dauer des zulässigen Aufenthalts von Drittstaatsangehörigen und Ermittlung von Aufenthaltsüberziehern*	*Reisende, die für einen kurzfristigen Aufenthalt einreisen*	*22 EUMS (außer BG, CY, HR, IE, RO UK)[3] + SAC*	*Verordnung (EU) 2017/2226 (EES-Verordnung)*	
Europäisches Reiseinformations- und genehmigungssystem (ETIAS)	*Überprüfung, ob ein Drittstaatsangehöriger ohne Visum ein Sicherheitsrisiko, ein Risiko in Bezug auf irreguläre Migration oder ein Risiko für die öffentliche Gesundheit darstellt*	*Reisende ohne Visum*	*26 EUMS (außer IE, UK)[3] + SAC*	*COM(2016) 731 final (Vorschlag für eine Verordnung zu ETIAS)*	*Keine*
Europäisches Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN)	*Austausch von Informationen über frühere Verurteilungen von Drittstaatsangehörigen*	*Vorbestrafte Drittstaatsangehörige*	*27 EU-Mitgliedstaaten (außer DK)[4]*	*COM(2017) 344 final (Vorschlag für eine Verordnung zu ECRIS-TCN)*	
Interoperabilität – Gemeinsamer Speicher für Identitätsdaten (CIR)	*Errichtung eines Rahmens für die Interoperabilität zwischen EES, VIS, ETIAS, Eurodac, SIS II und ECRIS-TCN*	*Drittstaatsangehörige, die unter Eurodac, VIS, SIS II, EES, ETIAS und ECRIS-TCN fallen*	*28 EU-Mitgliedstaaten[5] + SAC*	*COM(2017) 793 final (Vorschlag für eine Verordnung zur Interoperabilität im Bereich Grenzen und Visa)* *COM(2017) 794 final (Vorschlag für eine Verordnung zur Interoperabilität im Bereich polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)*	

Anmerkung: Geplante Systeme und vorgesehene Änderungen innerhalb der Systeme sind kursiv gedruckt.

 *Fingerabdrücke;*  *Handabdrücke;*  *Gesichtsbild;*  *DNA-Profil.*

EUMS: EU-Mitgliedstaaten.

SAC: Schengen-assoziierte Länder (Island, Liechtenstein, Norwegen und die Schweiz).

1 *Irland und das Vereinigte Königreich beteiligen sich nicht am VIS. Dänemark ist nicht an die VIS-Verordnung gebunden, hat der Anwendung des VIS jedoch zugestimmt. Das VIS gilt bislang nicht für Kroatien und Zypern und gemäß Beschluss (EU) 2017/1908 des Rates vom 12. Oktober 2017 nur in Teilen für Bulgarien und Rumänien.*

2 *Irland und Zypern sind bisher nicht an das SIS angeschlossen. Dänemark ist nicht an die Verordnung oder den Beschluss des Rates gebunden, hat der Anwendung von SIS II jedoch zugestimmt und muss nach Annahme der Vorschläge zu SIS II erneut über die Zustimmung entscheiden. Das Vereinigte Königreich beteiligt sich am SIS, kann jedoch keine Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung im Schengen-Raum nutzen oder darauf zugreifen. Bulgarien, Rumänien und Kroatien können keine Schengen-weit geltenden Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung im Schengen-Raum ausgeben, da sie noch nicht Teil des Schengen-Raums sind.*

3 *Dänemark könnte der Anwendung von EES und ETIAS zustimmen.*

4 *ECRIS-TCN gilt nicht für Dänemark. Das Vereinigte Königreich und Irland könnten der Anwendung zustimmen.*

5 *Dänemark, Irland und das Vereinigte Königreich beteiligen sich, da sie auch an der Einführung eines Interoperabilitätsrahmens für die IT-Systeme beteiligt sind.*

Quelle: FRA, auf der Grundlage vorhandener und vorgeschlagener Rechtsinstrumente, 2018

Quellen

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A. und 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. Januar 2016.

Amt des Hohen Kommissars der Vereinten Nationen für Menschenrechte (OHCHR) (2014), Recommended Principles and Guidelines on Human Rights at International Borders, 23. Juli 2014.

Artikel-29-Datenschutzgruppe (2014), *Stellungnahme 01/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung*, 536/14/DE, WP 211, Brüssel, 27. Februar 2014.

Artikel-29-Datenschutzgruppe (2017a), *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"*, WP 248 Rev. 01, 4. Oktober 2017.

Artikel-29-Datenschutzgruppe (2017b), *Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680)*, 7. Dezember 2017.

Artikel-29-Datenschutzgruppe (2018a), *Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679*, WP251rev.01, 6. Februar 2018.

Artikel-29-Datenschutzgruppe (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Brüssel, 23. April 2018.

Belgien, Unia, *Jahresbericht 2016*, Brüssel, September 2017.

Belgien, Unia, *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Brüssel, 2015.

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

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

Bovens et al. (2014), „Public accountability" in: Bovens, M., Schillermans, T. und Goodlin, R. E. (Hrsg.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), „Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment", *American Sociological Review*, Band 79, Nr. 3, S. 367-391.

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

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

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, Paris, La Documentation française, 2006.

Coudert, F, Butin, D. und Le Metayer, D. (2015), „*Body-worn cameras for police accountability: Opportunities and risks*", *Computer Law & Security Review*, Band 31, S. 749-762.

De Hert, P. und Lammerant, H. (2016), „Predictive profiling and its legal limits: effectiveness gone forever?" in: van der Sloot, B., Broeders, D. und Schrijvers, E. (Hrsg.), 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. und Rouvroy, A. (2008), *Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD),* Dok. T-PD 01, S. 3.

Europäische Agentur für die Grenz- und Küstenwache (Frontex) (2012), *Common Core Curriculum, EU Border Guard Basic Training*, März 2012.

Europäische Agentur für die Grenz- und Küstenwache (Frontex) (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Europäische Agentur für die Grenz- und Küstenwache (Frontex) (2015), *Twelve Seconds to Decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Europäische Agentur für die Grenz- und Küstenwache (Frontex) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Europäische Kommission (2017a), *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, Februar 2017.

Europäische Kommission (2017b), *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, Dezember 2017.

Europäische Kommission gegen Rassismus und Intoleranz (ECRI) (2007), *Allgemeine Politik-Empfehlung Nr. 11 der ECRI: Bekämpfung von Rassismus und Rassendiskriminierung in der Polizeiarbeit, verabschiedet am 29. Juni 2007*, Straßburg, 4. Oktober 2007.

Europäische Stelle zur Beobachtung von Rassismus und Fremdenfeindlichkeit (2016), Wahrnehmung von Diskriminierung und Islamfeindlichkeit – Stimmen von Mitgliedern muslimischer Gemeinschaften in der Europäischen Union, 2006.

Europäischer Datenschutzbeauftragter (EDSB) (2015), *Zweite Stellungnahme zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, Stellungnahme 5/2015*, Brüssel, 24. September 2015.

Europäischer Datenschutzbeauftragter (EDSB) (2018), *Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU*, Brüssel, 18. April 2018.

Europäisches Netz von Rechtsexperten für Gleichstellung und Nichtdiskriminierung (2016), *Links between migration and discrimination – A legal analysis of the situation in EU Member States*, Juli 2016.

Europarat, Ministerkomitee (2001), Empfehlung Rec(2001)10 des Ministerkomitees an die Mitgliedstaaten über den Europäischen Kodex für die Polizeiethik, 19. September 2001.

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 (Agentur der Europäischen Union für Grundrechte), Europäischer Datenschutzbeauftragter (EDSB) und Europarat (2018), *Handbook on European data protection law – Edition 2018*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Mai 2018.

FRA (Agentur der Europäischen Union für Grundrechte) (2013), *Polizeiliche Aus- und Fortbildung in Grundrechtsfragen – Handbuch für Trainer und Trainerinnen im Polizeidienst*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Dezember 2013.

FRA (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, 2014.

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

FRA (2016), *Fundamental Rights Report 2016*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, 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)*, Stellungnahme der FRA – 2/2017 [ETIAS], Juni 2017.

FRA (2017b), *Second European Union Minorities and Discrimination Survey – Main results*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Dezember 2017.

FRA (2017a), *Fundamental Rights Report 2017*, Luxemburg: Amt für Veröffentlichungen der Europäischen Union, Mai 2017.

FRA (2017d), *Zweite Erhebung der Europäischen Union zu Minderheiten und Diskriminierung: Muslime und Muslimas – ausgewählte Ergebnisse*, Luxemburg: Amt für Veröffentlichungen der Europäischen Union, September 2017.

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Mai 2017.

FRA (2018a), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, Stellungnahme der FRA – 1/2018 [Interoperabilität], April 2018.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, Fokuspapier der FRA, Mai 2018.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Februar 2018.

FRA (2018d), *Hate crime recording and data collection practice across the EU*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Juni 2018.

FRA (2018e), *Fundamental Rights Report 2018*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Juni 2018.

FRA und Europarat (2018), *Handbuch zum europäischen Antidiskriminierungsrecht – Ausgabe 2018*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Februar 2018.

Frankreich, Innenministerium (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7. Juni 2018.

Gandy, O. (2010), „Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems", *Ethics and Information Technology*, Band 12, Nr. 1, S. 29-42, 2010.

Gross, S. R. (2002), „*Racial Profiling under Attack*", D. Livingston, Ko-Autor. *Colum. L.* Rev. 102, No. 5, S. 1413-38.

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*, Band 71, 2004.

Harris, D. (2002), „*Flying While Arab: Lessons from the Racial Profiling Controversy*", *Civil Rights Journal*, Band 6, Nr. 1, Winter 2002.

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

Hildebrandt, M. und de Vries, K. (2013), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, New York, Routledge, 2013.

Hildebrandt, M. und Gutwirth, S. (Hrsg.) (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*, Band 13, Nr. 5, S. 573-589.

Hunt, P., Saunders, J. und 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*, Band 2, Nr. 4, S. 1287-1302.

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

Keskinen, S. et al (2018), *The Stopped – Ethnic Profiling in Finland*, Swedish School of Social Science, University of Helsinki, Helsinki, 3. April 2018.

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

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

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. und Floridi, L. (2016), *'The ethics of algorithms: Mapping the debate', Big Data & Society*, 1. Dezember 2016.

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. Januar 2016.

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

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

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

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

Rat der Europäischen Union (2009), Aktualisierter EU-Schengen-Katalog über Außengrenzkontrollen, Rückkehr und Rückübernahme, 19. März 2009.

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

Scheinin, M. (2007), United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/26, 29. Januar 2007.

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

Tóth, B. M. und Kádár, A. (2011), „Ethnic profiling in ID checks by the Hungarian police", *Policing and Society*, Band 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, März 2000.

Vereinigtes Königreich, Camden und London Prepared (2006), *Major Incident Procedures, What businesses and the voluntary sector need to know*, April 2006.

Vereinigtes Königreich, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29. September 2016.

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

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

Vereinigtes Königreich, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, Februar 2016.

Vereinigtes Königreich, Home Office (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, Februar 1999.

Vereinigtes Königreich, 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.

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

Vereinigtes Königreich, House of Commons Home Affairs Committee (2009), *The Macpherson Report – Ten Years On,* Twelfth Report of Session 2008–09, 22. Juli 2009.

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

Vereinigtes Königreich, London School of Economics (2011), *Reading the Riots*, Dezember 2011.

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

Vereinigtes Königreich, Northamptonshire Police (2018), *Get Involved – Reasonable Grounds Panel*, abgerufen im April 2018.

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

Vereinigtes Königreich, Stop Watch (2011), *"Carry on Recording" – Why police stops should still be recorded*, Mai 2011.

Vereinigtes Königreich, West Midlands Police (2012), *Stop and Search Policy*, November 2012.

Vereinigtes Königreich, West Midlands Police (2016), *Stop and Search Recommendations*, Juli 2015 (zuletzt geändert im Juni 2016).

Vereinigtes Königreich, West Midlands Police (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, April 2017.

Vereinigtes Königreich, West Midlands Police (2017b), *New "app' set to speed up Stop & Search process*, August 2017.

Vereinigtes Königreich, West Midlands Police (2018),,*Stop and Search Scrutiny Panels* abgerufen im April 2018.

Vereinigtes Königreich, West Midlands Police und Crime Commissioner (2014), *Stop and Search Action Plan – Outcome of Consultation*, Januar 2014.

Vereinte Nationen (UN) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29. Januar 2007.

Van Brakel, R. (2016), „Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing" in: van der Sloot, B., Broeders, D. und Schrijvers, E. (Hrsg.), 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*, Band 11, Nr. 2, S. 285-330.

EU-Rechtsvorschriften

Grundrechte

Charta der Grundrechte der Europäischen Union, 2012/C 326/02, ABl. C 326 vom 26.10.2012.

Erläuterungen (*) zur Charta der Grundrechte, 2007/C 303/02, ABl. C 303/17 vom 14.12.2007.

Nichtdiskriminierung

Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft.

Richtlinie 2000/78/EG des Rates vom 27. November 2000 zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf.

Datenschutz

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung

personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Grenzmanagement

Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205/63 vom 7.8.2007 *(SIS II)*.

Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119/132 vom 4.5.2016.

Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381/4 vom 28.12.2006.

Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, ABl. L 218/60 vom 13.8.2008 (*VIS-Verordnung*).

Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit

Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 180/1 vom 29.6.2013.

Verordnung (EU) 1624/2016 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG, ABl. L 251/1 vom 16.9.2016.

Verordnung (EU) Nr. 1052/2013 des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zur Errichtung eines Europäischen Grenzüberwachungssystems (EUROSUR), ABl. L 295/11 vom 6.11.2013.

Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex).

Rechtsprechung

Frankreich, Kassationshof (*Cour de Cassation*), *Décision 1245*, 9. November 2016.

Vereinigtes Königreich, House of Lords, *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.,* [2006] UKHL 12, 8. März 2006.

EuGH, C-524/06, *Heinz Huber gegen Bundesrepublik Deutschland*, 16. Dezember 2008.

EGMR, *B.S. v. Spain*, Nr. 47159/08, 24. Juli 2012.

ECtHR, *S. and Marper v. United Kingdom*, Nr. 30562/04 und 30566/04, 4. Dezember 2008.

EGMR, *Gillan and Quinton v. the United Kingdom*, Nr. 4158/05 2010, 12. Januar 2010.

UNHRC, *Rosalind Williams Lecraft v. Spain*, Mitteilung Nr. 1493/2006, 30. Juli 2009.

Die EU kontaktieren

Besuch

In der Europäischen Union gibt es Hunderte von „Europe-Direct"-Informationsbüros. Über diesen Link finden Sie ein Informationsbüro in Ihrer Nähe: https://europa.eu/european-union/contact_de

Telefon oder E-Mail

Der Europe-Direct-Dienst beantwortet Ihre Fragen zur Europäischen Union. Kontaktieren Sie Europe Direct

— über die gebührenfreie Rufnummer: 00 800 6 7 8 9 10 11 (manche Telefondienstanbieter berechnen allerdings Gebühren),
— über die Standardrufnummer: +32 22999696 oder
— per E-Mail über: https://europa.eu/european-union/contact_de

Informationen über die EU

Im Internet

Auf dem Europa-Portal finden Sie Informationen über die Europäische Union in allen Amtssprachen: https://europa.eu/european-union/index_de

EU-Veröffentlichungen

Sie können – zum Teil kostenlos – EU-Veröffentlichungen herunterladen oder bestellen unter https://publications.europa.eu/de/publications. Wünschen Sie mehrere Exemplare einer kostenlosen Veröffentlichung, wenden Sie sich an Europe Direct oder das Informationsbüro in Ihrer Nähe (siehe https://europa.eu/european-union/contact_de).

Informationen zum EU-Recht

Informationen zum EU-Recht, darunter alle EU-Rechtsvorschriften seit 1952 in sämtlichen Amtssprachen, finden Sie in EUR-Lex: http://eur-lex.europa.eu

Offene Daten der EU

Über ihr Offenes Datenportal (http://data.europa.eu/euodp/de) stellt die EU Datensätze zur Verfügung. Die Daten können zu gewerblichen und nichtgewerblichen Zwecken kostenfrei heruntergeladen werden.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Technologische Entwicklungen haben zu einem verstärkten Einsatz von Profiling in einer Vielzahl von Kontexten geführt, und die EU-Mitgliedstaaten haben der Nutzung von Profiling-Werkzeugen zur Unterstützung der Arbeit von Strafverfolgungs- und Grenzschutzbeamtinnen und -beamten in jüngster Zeit zunehmend Beachtung geschenkt. Profiling ist ein rechtmäßiges Verfahren, das zur Verhinderung, Ermittlung und Verfolgung von Straftaten sowie zur Verhinderung und Aufdeckung irregulärer Zuwanderung eingesetzt wird. Unrechtmäßiges Profiling kann jedoch das Vertrauen in die Behörden beeinträchtigen und bestimmte Gemeinschaften stigmatisieren.

In diesem Handbuch wird erläutert, was Profiling ist, welcher Rechtsrahmen ihm zugrunde liegt und weshalb Profiling von rechtlicher Seite nicht nur die Grundrechte wahren muss, sondern auch von entscheidender Bedeutung für eine wirksame Polizeiarbeit und ein wirksames Grenzmanagement ist. Das Handbuch enthält außerdem praktische Anweisungen zur Vermeidung von unrechtmäßigem Profiling bei Einsätzen von Polizei und Grenzmanagement.

FRA – AGENTUR DER EUROPÄISCHEN UNION FÜR GRUNDRECHTE
Schwarzenbergplatz 11, 1040 Wien – Österreich
Tel. +43 158030-0 – Fax +43 158030-699
@EURightsAgency

Amt für Veröffentlichungen
der Europäischen Union