SSOAR

Open Access Repository
www.ssoar.info

Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung

Töpfer, Eric

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Deutsches Institut für Menschenrechte

Empfohlene Zitierung / Suggested Citation:
Töpfer, E. (2024). *Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung.* (Analyse / Deutsches Institut für Menschenrechte). Berlin: Deutsches Institut für Menschenrechte. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-94580-2

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Terms of use:
This document is made available under a CC BY-NC-ND Licence (Attribution-Non Comercial-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nc-nd/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Deutsches Institut
für Menschenrechte

Analyse

Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung

Eric Töpfer

Das Institut

Das **Deutsche Institut für Menschenrechte** ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands (§ 1 DIMR-Gesetz). Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, anwendungsorientierte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit internationalen Organisationen. Es wird vom Deutschen Bundestag finanziert. Das Institut ist zudem mit dem Monitoring der Umsetzung von UN-Behindertenrechtskonvention und UN-Kinderrechtskonvention sowie der Berichterstattung zu den Konventionen des Europarats zu Menschenhandel und zu Gewalt gegen Frauen und häuslicher Gewalt betraut worden. Hierfür hat es entsprechende Monitoring- und Berichterstattungsstellen eingerichtet.

Der Autor

Eric Töpfer ist Politikwissenschaftler und seit 2012 Wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte, wo er zu Menschenrechtsthemen im Feld der Inneren Sicherheit arbeitet. Seine Schwerpunkte dabei sind die Kontrolle von Polizei und Geheimdiensten, Datenschutzfragen und Digitalisierungsthemen sowie die Achtung von Menschenrechten bei der Terrorismusbekämpfung.

Die vorliegende Analyse gibt die Auffassung des Deutschen Instituts für Menschenrechte wieder.

Deutsches Institut
für Menschenrechte

Analyse

Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung

Eric Töpfer

Vorwort

Das Sammeln, Speichern und Verarbeiten von Daten ist seit jeher ein zentraler Aspekt polizeilicher Arbeit. Dabei ist der Computer heute nicht mehr wegzudenken. Auch für die automatisierte Datenverarbeitung der Polizei gilt das menschenrechtliche Verbot rassistischer Diskriminierung. Daher sind Daten, aus denen – wie es im Datenschutzrecht heißt – eine „rassische oder ethnische Herkunft" hervorgeht, als besondere Kategorien personenbezogener Daten („sensible Daten") besonders geschützt.

Das Institut arbeitet bereits seit vielen Jahren zu polizeilichen Personenkontrollen und Racial Profiling und mahnt den Schutz vor rassistischer Diskriminierung im direkten Kontakt der Polizei zur Bevölkerung an. Angesichts der fortschreitenden Digitalisierung, die auch vor der Polizeiarbeit nicht haltmacht, wirft die vorliegende Analyse nun einen Blick hinter die Kulissen und thematisiert die polizeiliche Verarbeitung sensibler Daten.

Das Thema führt bislang eher ein Schattendasein in der Diskussion um institutionellen Rassismus, obwohl die Bürgerrechtsbewegung der Sinti*zze und Rom*nja mit ihrer Kritik an der jahrzehntelangen Sondererfassung seit Langem gegen diskriminierende Praktiken polizeilicher Datenverarbeitung kämpft. Daher soll die Analyse dazu beitragen, die Aufmerksamkeit für Diskriminierungsrisiken in einem Feld zu erhöhen, das polizeiliches Handeln zunehmend prägt, das in der Regel aber für Betroffene unsichtbar bleibt und dessen Wirkungen ob seiner wachsenden Komplexität auch für die Politik und einzelne Polizist*innen immer schwerer zu durchschauen sind.

Untersucht wird hierzu zum einen, welche grund-, menschen- und europarechtlichen Vorgaben zum Schutz vor den Risiken rassistischer Diskriminierung, die mit der Verarbeitung der genannten Daten einhergehen, bestehen und wie diese im deutschen Datenschutz- und Polizeirecht umgesetzt wurden. Zum anderen wird der Frage nachgegangen, was über die polizeiliche Praxis bekannt ist.

Das Institut bedankt sich bei allen, die die Erstellung der Analyse durch Hintergrundgespräche oder Interviews ermöglicht haben. Dies waren Expert*innen aus Datenschutzaufsichtsbehörden, Polizei, Zivilgesellschaft und Wissenschaft. Außerdem danken wir den Innenministerien aller Länder, die unseren Fragebogen zum Thema ausnahmslos beantwortet haben. Wir hoffen, dass die Analyse einen Anstoß für eine systematische Untersuchung der polizeilichen Praxis durch Polizei und Wissenschaft gibt, um Diskriminierungsrisiken in der Verarbeitung sensibler Daten zu identifizieren und auszuräumen.

Professorin Dr. Beate Rudolf
Direktorin des Deutschen Instituts
für Menschenrechte

Inhalt

Zusammenfassung

- Das grund- und menschenrechtliche Diskriminierungsverbot umfasst das Verbot rassistischer Diskriminierung. Es verbietet staatlichen Hoheitsträgern wie der Polizei bei allem Handeln auch die Unterscheidung aufgrund von physischen Merkmalen wie Hautfarbe, tatsächlicher oder vermeintlicher (nationaler) Herkunft oder Religionszugehörigkeit. Das Verbot umfasst auch das Differenzierungsmerkmal „Ethnie". Vom Verbot sind Ausnahmen nur zulässig, wenn damit keine rassistische Zuschreibung verbunden ist, sondern ein schwerwiegender sachlicher Grund vorliegt. Das Verbot gilt auch für die polizeiliche Datenverarbeitung.

- Gemäß der EU-Richtlinie zum Datenschutz bei Polizei und Strafjustiz („JI-Richtlinie") ist eine Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten"), „aus denen die rassische oder ethnische Herkunft [...] hervorgeht", nur dann erlaubt, wenn sie unbedingt erforderlich ist, der Schutz der Rechte und Freiheiten Betroffener durch geeignete Maßnahmen garantiert wird und wenn die Verarbeitung gesetzlich normiert ist, sie lebenswichtigen Interessen dient oder sich auf Daten bezieht, die Betroffene öffentlich gemacht haben.

- Die Umsetzung der JI-Richtlinie in deutsches Recht garantiert kein ausreichend hohes Schutzniveau für die Verarbeitung sensibler Daten. § 48 des Bundesdatenschutzgesetzes sowie die einschlägigen landesrechtlichen Regelungen zur polizeilichen Datenverarbeitung übernehmen regelmäßig mehr oder weniger nur den Wortlaut der JI-Richtlinie. Es fehlen jedoch eine Präzisierung der tatbestandlichen Voraussetzung für die Verarbeitung sensibler Daten und verbindliche Vorgaben für deren Schutz.

- In Deutschland werden Daten, aus denen eine vermeintliche „rassische oder ethnische Herkunft" Betroffener gelesen werden kann, in regional unterschiedlichem, aber erheblichem Ausmaß durch die Polizeien von Bund und Ländern erfasst. In zahlreichen polizeilichen Datenbanken werden Angaben über zugeschriebene „Phänotypen" oder „Volkszugehörigkeiten" von Beschuldigten, Tatverdächtigen und sogenannten Anlasspersonen standardisiert gespeichert. Regelmäßig werden die Vor- und Nachnamen, Staatsangehörigkeiten oder Geburtsorte gespeichert, dies gilt auch für Geschädigte oder Zeug*innen. Unter Umständen werden solche Daten als „proxy data" stellvertretend für eine zugeschriebene „rassische oder ethnische Herkunft" gelesen und sind dann ebenfalls als sensible Daten zu schützen.

- Angestoßen durch die Kritik an der jahrzehntelangen Sondererfassung von Sinti*zze und Rom*nja wird bis heute etwa polizeiintern kontrovers diskutiert, unter welchen Umständen die polizeiliche Verarbeitung des Merkmals „Volkszugehörigkeit" erforderlich ist. Ministerialerlasse zu seiner Vermeidung in der polizeiinternen Kommunikation geben keine konkreten Hinweise für die Praxis, sondern stellen die Entscheidung ins polizeiliche Ermessen. In Einzelfällen haben Datenschutzaufsichtsbehörden die Erfassungspraxis beanstandet. Eine systematische Überprüfung der Speicherung sensibler Daten zu vermeintlicher „rassischer oder ethnischer Herkunft" erfolgte aber bislang nicht.

- Fraglich ist, ob die Garantien zum besonderen Schutz sensibler Daten bei der Polizei ausreichen. Zwar sollen Datenschutzfolgeabschätzungen helfen, Risiken für die Rechte Betroffener zu erkennen und zu minimieren. Ob solche Risiken bestehen und ob es überhaupt eine Folgeabschätzung braucht, wird jedoch allein polizeiintern und ohne Anhörung von Betroffenen entschieden. Mit wenigen Ausnahmen herrscht dabei ein enges Verständnis vor, was sensible Daten zu „rassischer oder ethnischer Herkunft" sind, sodass sie in der Regel kaum anders behandelt werden als sonstige Daten.

- Die polizeiliche Nutzung einmal rechtmäßig erhobener und gespeicherter Daten ist einfachgesetzlich bislang wenig reguliert. Dies gilt auch für die Nutzung sensibler Daten. So sind aus der polizeilichen Praxis Fälle bekannt, in denen ursprünglich für Identifizierungszwecke erhobene Daten als „proxy data“ für rassifizierende Zuschreibung genutzt werden, um Einsätze zu planen, Lagebilder zu erstellen oder Analyseprojekte durchzuführen. In der Folge erfahren Menschen etwa aufgrund ihres Nachnamens oder ihrer Staatsangehörigkeit eine andere polizeiliche Behandlung als der Rest der Bevölkerung.

- Mit dem aktuell laufenden Umbau der polizeilichen Informationsarchitektur im Rahmen des Projektes „P20“, das die Zusammenlegung der polizeilichen Datenbestände in einem gemeinsamen „Datenhaus“ und den verstärkten Einsatz „intelligenter“ algorithmengestützter Analysen anstrebt, wachsen die Diskriminierungsrisiken bei der Nutzung sensibler Daten.

- Der Schutz Betroffener vor rassistischer Diskriminierung bei der Verarbeitung sensibler Daten muss dringend gestärkt werden. Gesetzgeber in Bund und Ländern müssen die gesetzlichen Vorschriften anpassen, um die tatbestandlichen Voraussetzungen eng gefasst zu präzisieren und verbindliche Regeln für Schutzmaßnahmen zu normieren.

- Zudem sollte die Polizei Transparenz über die Konzepte, den Umfang und die Praxis der polizeilichen Verarbeitung solcher Daten herstellen, sich einer kritischen Diskussion stellen und ihre Routinen hinterfragen. Dafür braucht es ein Verständnis für die Entstehung und Wirkungsweise von Rassismus, insbesondere für die soziale Konstruktion von „Rasse“. Besonderes Gewicht ist dabei der Stimme rassifizierter Menschen zu geben.

1 Einleitung

Seit einigen Jahren hat die Diskussion über Rassismus in der deutschen Gesellschaft auch die Polizei erreicht.[1] In der Folge wurden durch Politik, Zivilgesellschaft, Polizei und Wissenschaft zahlreiche Projekte angestoßen, um Rassismus in der Polizei zu beforschen und diskriminierungsfreie Polizeiarbeit sicherzustellen.[2]

Bisher spielt die polizeiliche Datenverarbeitung dabei keine Rolle – und dies, obwohl Polizeiarbeit inzwischen viel Computerarbeit ist und insbesondere die Bürgerrechtsbewegung der Sinti*zze und Rom*nja die Bedeutung polizeilicher Datenverarbeitung für die Reproduktion rassistischer Stereotype immer wieder problematisiert hat.[3] Aktuell in der Diskussion sind insbesondere Auswertungen nach Namen, die stellvertretend für eine vermeintliche „ethnische Zugehörigkeit“ gelesen werden und Betroffene als Angehörige krimineller Milieus einstufen und stigmatisieren.[4]

Dabei bestehen Diskriminierungsrisiken in allen Phasen der polizeilichen Datenverarbeitung – von der Erhebung über die Speicherung und Nutzung bis zur Übermittlung und Löschung (vgl. Abbildung 1): Sehen sich etwa Menschen aufgrund ihres Äußeren verstärkt polizeilichen Personenkontrollen ausgesetzt, bedeutet dies nicht nur, dass ihre Daten im Rahmen einer Identitätsfeststellung erhoben werden. Es bedeutet oft auch, dass ihre Daten im Zusammenhang mit Folgemaßnahmen in polizeilichen Datenbanken gespeichert werden, weil zum Beispiel Anhaltemeldungen geschrieben oder erkennungsdienstliche Maßnahmen durchgeführt werden. Im Ergebnis werden betroffene Gruppen nicht nur häufiger kontrolliert, sondern auch registriert. Dies erhöht, anders als für die nicht polizeilich registrierte Bevölkerung, die Wahrscheinlichkeit, dass die Betroffenen erneut zum Ziel polizeilicher Maßnahmen werden, etwa weil ein Datenabgleich anlässlich einer Identitätsfeststellung einen „Treffer“ mit ihren Daten erzeugt.

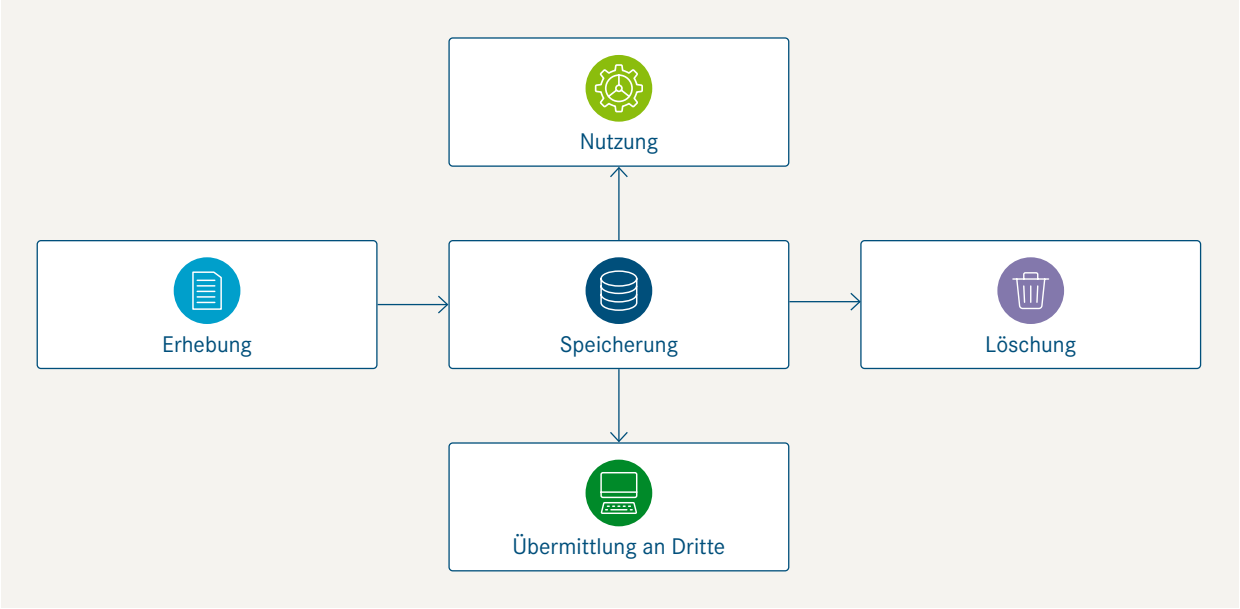
Im Rahmen der weiteren Verarbeitung ist rassistische Diskriminierung möglich, wenn etwa an Herkunft anknüpfende Profile zur Rasterung von Datenbeständen genutzt, einschlägige Diskriminierungsmerkmale als Gefahrenindikator kommuniziert oder als Prognosemaßstab herangezogen werden, oder um zu entscheiden, ob Daten zu löschen oder weiterhin zu speichern sind.

Eine (Re-)Produktion rassistischer Diskriminierung droht zudem, wenn Menschen informationstechnisch klassifiziert, sortiert und bestimmten Kategorien zugeordnet werden und diese Informationen aggregiert und für polizeiliche oder kriminalpolitische Zwecke zu Lagebildern oder Statistiken etwa über „Ausländerkriminalität“ aufbereitet werden, obwohl Nationalität kein kriminogener Faktor ist.[5]

Seit dem 19. Jahrhundert sammelt und verarbeitet die Polizei zur Erfüllung ihrer Aufgaben in erheblichem Umfang personenbezogene Daten.[6] Mit dem Siegeszug der Informations- und Kommunikationstechnologien wird die polizeiliche Informationsverarbeitung seit den späten 1960er-Jahren in wachsendem Maße digitalisiert. Anfänglich ging es dabei primär um den Aufbau von elektronischen Datenbanken, die bestehende

1 Dengler / Foroutan (2017); Bosch (2020).
2 Eine Übersicht in: Die Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration / Die Beauftragte der Bundesregierung für Antirassismus (2023), S. 46 ff.
3 Rose (2000); Reuss (2023); Deutscher Bundestag (21.05.2021), S. 366 ff.
4 Wegner (2023).
5 Zur Kritik an der Erfassung von „Ausländerkriminalität“ sowie ihrer rassistischen Traditionen siehe u. a.: Feltes / Weingärtner / Weigert (2016); Fischer (20.04.2023).
6 Heinrich (2007), S. 121 ff.

Abbildung 1: Phasen/Formen der Datenverarbeitung



Papierarchive ablösten und auf die nur eine sehr begrenzte Zahl von Nutzer*innen unmittelbaren Zugriff hatte. Heute werden immer mehr Polizeibeamt*innen mit mobilen Geräten zur Erfassung und Abfrage der Daten ausgestattet und so auch die Kräfte in der Fläche mit den digitalen Informationssystemen vernetzt.[7]

Aktuell treiben Innenministerien und Polizeibehörden in Bund und Ländern im Rahmen des Projektes „P20“ (früher „Polizei 2020“) die Zusammenführung der polizeilichen Datenbestände in einem zentralen „Datenhaus“ voran. Das Ziel ist, die Informationen künftig allen Polizist*innen schneller bereitstellen zu können und die Möglichkeiten ihrer (automatisierten) Auswertung zu verbessern. Ähnliche Pläne werden auf europäischer Ebene durch die Initiative zur Interoperabilität[8] der großen IT-Systeme der Europäischen Union (EU) im Bereich Asyl, Migration und Sicherheit verfolgt. Mit der zunehmenden Digitalisierung und der Schaffung großer „Datenhäuser“ wächst die Bedeutung der Datenverarbeitung für das polizeiliche Management von Wissen und seine Übersetzung in praktische Maßnahmen.

Vor diesem Hintergrund hat sich das Deutsche Institut für Menschenrechte mit der Frage befasst, inwiefern Risiken einer rassistischen Diskriminierung bei der polizeilichen Datenverarbeitung in Deutschland bestehen. Denn auch für die Verarbeitung personenbezogener Daten durch die Polizei gilt nicht nur das Grund- und Menschenrecht auf informationelle Selbstbestimmung, Datenschutz und Privatsphäre,[9] sondern ebenso das Verbot rassistischer Diskriminierung.[10] Dementsprechend gilt, dass die Verarbeitung personenbezogener Daten durch die Polizei weder willkürlich und unverhältnismäßig erfolgen noch rassistische Diskriminierung bezwecken oder bewirken darf.

Im Einzelnen werden folgende Fragen untersucht:

- Welche Bedeutung hat das menschenrechtliche Diskriminierungsverbot für die polizeiliche Datenverarbeitung?
- Wie wird die staatliche Pflicht zur Achtung des Diskriminierungsverbotes im Recht der polizeilichen Datenverarbeitung umgesetzt?
- Wie wird die Pflichterfüllung in der polizeilichen Praxis gewährleistet?

7 So waren bereits 2021 bei der Bundespolizei rund 9.100 Mobiltelefone mit Zugriff auf polizeiliche Datenbanken, mobiler Vorgangsbearbeitung und Fast-ID im Testbetrieb im Einsatz. Siehe: Deutscher Bundestag (07.05.2021), S. 14.

8 Der Begriff „Interoperabilität“ meint in diesem Zusammenhang die Möglichkeit, dass IT-Systeme Daten miteinander austauschen und auf diese Weise Informationen leichter genutzt werden können, die zuvor getrennt vorgehalten wurden.

9 Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, Art. 7 und 8 Grundrechtecharta der EU, Art. 8 EMRK, Art. 17 UN-Zivilpakt.

10 Art. 3 Abs. 3, S. 1 GG, Art. 14 EMRK, Art. 21 EU-Grundrechtecharta, Art. 2 Abs. 1 UN-Zivilpakt, Art. 2 Abs. 1 ICERD.

Dafür werden die grund- und menschenrechtlichen Vorgaben beschrieben (Kapitel 1.2.1 und 1.2.2) und ihre Umsetzung in das Recht der polizeilichen Datenverarbeitung untersucht (Kapitel 1.2.3). Anschließend wird der Frage nachgegangen, wie die Polizei sogenannte besondere Kategorien personenbezogener Daten zu „rassischer oder ethnischer Herkunft" verarbeitet und dabei den Schutz vor Risiken rassistischer Diskriminierung sicherstellt (Kapitel 1.3). Dabei geht es nicht um die Phase der Datenerhebung zum Beispiel bei Personenkontrollen. Die Untersuchung fokussiert auf die Speicherung und weitere Datennutzung durch die Polizei.

Dafür hat das Deutsche Institut für Menschenrechte einen standardisierten Fragebogen an die Innenministerien und -senator*innen aller 16 Bundesländer geschickt. Erfragt wurden Informationen zu Art und Umfang der polizeilichen Verarbeitung personenbezogener, sensibler Daten sowie zu internen Verarbeitungsvorschriften und Schutzmaßnahmen. Der Fragebogen wurde von allen 16 Bundesländer beantwortet.[11] Zusätzlich wurden Gespräche mit 17 Expert*innen aus Polizei, Datenschutzaufsicht und von zivilgesellschaftlichen Organisationen zu Risiken und Problemen sowie der Wirksamkeit oder Reformbedürftigkeit von Schutzmechanismen geführt und öffentlich verfügbare Informationen, Studien und Parlamentsdrucksachen aus Bund und Ländern ausgewertet.

Die Studie erlaubt keine umfassenden Aussagen dazu, ob es bei oder durch die polizeiliche Datenverarbeitung tatsächlich zu rassistischer Diskriminierung kommt. Ob oder in welchem Ausmaß dies unter den dargestellten Rahmenbedingungen tatsächlich passiert, entscheidet sich jeweils in konkreten, lokalen Situationen, die hier lediglich exemplarisch dargestellt werden können. Die Studie zeigt aber sehr deutlich, dass die rechtlichen Vorgaben zum Schutz sensibler Daten Betroffener mangelhaft umgesetzt wurden. Sie verdeutlicht außerdem, welche Risiken rassistischer Diskriminierung bei der polizeilichen Datenverarbeitung bestehen.

Forschungsstand: Rassismus, Polizei und Datenverarbeitung

Obwohl in der Forschung kein einheitlicher Rassismus-Begriff existiert und häufiger im Plural von Rassismen gesprochen wird, um die Vielschichtigkeit des Phänomens zu markieren, besteht in den Sozialwissenschaften inzwischen weitgehend Konsens, dass Rassismus ein System von Diskursen und Praktiken zur Rechtfertigung und Durchsetzung gesellschaftlicher Machtverhältnisse ist. Rassismus imaginiert Menschen aufgrund (vermeintlicher) biologischer oder kultureller Merkmale als homogene Gruppen, schreibt diesen Gruppen bestimmte Eigenschaften zu und hierarchisiert sie. Auf diese Weise wird systematisch die Benachteiligung und Exklusion der abgewerteten Gruppen reproduziert und zur selbstverständlichen Routine. Dabei tritt Rassismus nicht nur als offener Rechtsextremismus zutage, sondern auch in Form unbewusster Vorurteile und Mikroaggressionen. Dieser sogenannte Alltagsrassismus steht in Wechselbeziehung mit den Strukturen einer Gesellschaft. Daher reicht es für die Analyse nicht, nur individuelle Einstellungen und das Handeln Einzelner zu untersuchen. Vielmehr müssen auch die Institutionen, welche die Reproduktion rassistischer Wissensbestände und Praktiken bedingen, in den Blick genommen werden.[12]

Dabei kommt der Polizei eine besondere Rolle zu, welche inzwischen auch in Deutschland verstärkt Forschungsthema ist. Der Anstoß dazu kam unter anderem von der Europäischen Kommission gegen Rassismus und Intoleranz (ECRI), die den Polizeien von Bund und Ländern im Frühjahr 2020 empfohlen hatte, eine Studie zu „Racial Profiling" in Auftrag zu geben.[13] Unterscheiden lassen sich in der Forschung zu Rassismus und Polizei drei Perspektiven: 1) Forschung zu individuellen Einstellungsmustern und Erfahrungen von Polizist*innen, 2) Studien zur Handlungspraxis und institutionalisierten Handlungsmustern und 3) Analysen der Rahmenbedingungen des polizeilichen Handelns auf organisationaler oder politisch-rechtlicher Ebene.[14] Bereits Mitte der 1990er-Jahre wurden erstmals Einstellungsmuster untersucht, die bis heute ein

11 Der Fragebogen enthielt sechs Fragen. Diese wurden von den Innenministerien und -senator*innen zwischen März und September 2023 unterschiedlich detailliert und zum Teil mit Verweis auf technische Hürden oder Geheimschutzbelange gar nicht beantwortet.

12 Siehe etwa: Rommelspacher (2009); Tsianos / Karakayali (2014); Danielzik (2018); Foroutan (2020).

13 Europäische Kommission gegen Rassismus und Intoleranz (2020), Ziff. 109.

14 Bergmann / Jacobsen (2021); Fink / Kretschmann (2022).

Schwerpunkt der Forschung sind. Inzwischen kommen, teilweise finanziert durch Innenministerien einiger Bundesländer, auch Studien zur Erforschung lokaler Handlungspraktiken und Wissensbestände durch ethnografische Beobachtung oder Interviews hinzu.[15] In ihrer Summe zeigt die bisherige Forschung, dass Rassismus auch innerhalb der deutschen Polizeien existiert sowohl auf der Ebene individueller Einstellungen als auch in der polizeilichen Praxis; allerdings sind die Forschungslücken groß, da die Studien in der Regel nur regionale Ausschnitte beleuchten und meist auf die Schutzpolizei fokussieren.[16] Arbeiten zur Bedeutung der strukturellen Rahmenbedingungen für das polizeiliche Handeln finden sich bislang wenige; in den Blick genommen wurden rechtliche Rahmenbedingungen und diskursive Muster.[17] Insgesamt dominiert die Perspektive, dass Polizeiarbeit durch einen erheblichen individuellen Ermessensspielraum gekennzeichnet ist und Diskriminierung primär das Ergebnis der Reproduktion rassistischer Wissensbestände ist, die lokal in einzelnen Dienststellen tradiert werden.[18]

Seit etwa 30 Jahren gibt es insbesondere im angelsächsischen Raum sozialwissenschaftliche Forschung zu den Auswirkungen der Computerisierung und Informatisierung auf die Polizei.[19] Diese kommt zu dem Ergebnis, dass polizeiliches Handeln zunehmend durch die Formate und Standards von IT-Systemen vorstrukturiert wird und lokales Wissen angesichts der neuen Bedeutung der Daten und ihrer Analyst*innen an Bedeutung verliert und sich Praktiken der Verdachtsgewinnung ändern.[20] Die Forschung zur Informatisierung der Polizei konstatiert außerdem, dass die polizeiliche Informationstechnik sich ob ihrer Komplexität in wachsendem Maße nicht nur der politischen Kontrolle entzieht, sondern auch der bürokratischen Steuerung und damit unerwünschte Nebeneffekte drohen.[21] Allerdings gilt auch hier, dass die Forschungslücken groß sind und Differenzierung geboten ist, da die Handlungslogiken, die Techniknutzung und ihre Konsequenzen für die betroffene Bevölkerung je nach räumlicher Verortung und entsprechend den vielfältigen polizeilichen Arbeitsfeldern sehr unterschiedlich ausfallen dürften.[22] Kaum Beachtung hat dabei bislang die Frage gefunden, welche Rolle die Strukturen der polizeilichen Informationstechnik für die Reproduktion rassistischer Wissensbestände in der Polizei spielen.[23]

Vor diesem Hintergrund will die vorliegende Studie an der Schnittstelle der Forschung zu Rassismus und der Forschung zur polizeilichen Nutzung von Informationstechnik einen Beitrag leisten zum Verständnis von Diskriminierungsrisiken durch die Verarbeitung von besonderen Kategorien personenbezogener Daten.

15 Siehe für Berlin: Howe u. a. (2022) und für Niedersachsen: Jacobsen / Bergmann (2022).
16 Hunold / Wegner (2020); Hunold / Singelnstein (2022).
17 Siehe etwa: Cremer (2013); End (2019).
18 Kritisch zum Stand der Forschung zu Polizei und Rassismus: Atali-Timmer / Fereidooni / Schroth (2022).
19 Siehe etwa: Ericson / Haggerty (1997); Chan (2001); Haggerty (2004); Ericson (2007).
20 So auch Ergebnisse aus Deutschland: Reichertz / Wilz (2022); Creemers / Guagnin (2014).
21 Heinrich (2007).
22 Nogala (2019).
23 Ausnahmen finden sich etwa bei Herrnkind (2014), der Methoden der Rasterfahndung und gruppenbezogene Sondererfassungen als Praktiken des Racial Profiling problematisiert.

2 Rechtliche Grundlagen

Welche Bedeutung hat das menschenrechtliche Verbot rassistischer Diskriminierung für die polizeiliche Datenverarbeitung? Zur Klärung dieser Frage erläutert das Kapitel in einem ersten Schritt, was der Begriff rassistische Diskriminierung meint. Anschließend wird dargestellt, wie das Konzept besonders schutzwürdiger Kategorien personenbezogener Daten („sensible Daten"), durch welche eine „rassische oder ethnische Herkunft"[24] zugeschrieben werden kann, Diskriminierungsrisiken minimieren soll. Abschließend erläutert das Kapitel die rechtlichen Vorgaben zum besonderen Schutz sensibler Daten, insbesondere die Richtlinie (EU) 2016/680 über den Datenschutz in Polizei und Strafjustiz („JI-Richtlinie"), sowie ihre unzureichende Umsetzung in nationales Recht.

Die Begriffe „Rasse", „rassische oder ethnische Herkunft"

Das Deutsche Institut für Menschenrechte lehnt die Verwendung des Begriffs „Rasse" ab, um zu vermeiden, dass Vorstellungen von unterschiedlichen „Rassen" durch Normen zum Diskriminierungsschutz oder bei ihrer Anwendung reproduziert werden. Das Institut empfiehlt deshalb auch, den Begriff aus Artikel 3 Absatz 3 Grundgesetz zu streichen und durch „rassistisch" zu ersetzen.

Da der Begriff jedoch rechtlich etabliert ist, wird er hier in Anführungszeichen verwendet, wenn einschlägige Normen zitiert werden. Dies gilt auch für den Begriff der „rassischen oder ethnischen Herkunft", der im Datenschutzrecht eine besonders geschützte Kategorie personenbezogener Daten markiert.[25]

Die Nutzung dieser Begriffe ist jedoch nicht in dem Sinne zu verstehen, dass es tatsächlich „Rassen" oder eine „rassische oder ethnische Herkunft" gebe. Sie sind vielmehr als Kategorien zu begreifen, die durch Fremd- oder Selbstzuschreibungen sozial konstruiert werden.

2.1 Das Verbot rassistischer Diskriminierung

So wie alle staatlichen Behörden ist auch die Polizei an das grund- und menschenrechtliche Verbot rassistischer Diskriminierung gebunden.[26] Verfassungsrechtlich ergibt sich das Verbot aus Artikel 3 Absatz 3 Satz 1 Grundgesetz, wonach niemand wegen seiner „Rasse" benachteiligt oder bevorzugt werden darf. Europarechtlich sind Diskriminierungen wegen „Rasse" durch Artikel 21 der EU-Grundrechtecharta verboten. Völkerrechtlich bekennt sich Deutschland zur Einhaltung des Verbots unter anderem durch die Ratifikation der UN-Konvention gegen rassistische Diskriminierung (ICERD) und der Europäischen Menschenrechtskonvention (EMRK). Nach Artikel 2 Absatz 1 ICERD verpflichtet sich jeder Vertragsstaat, Handlungen oder Praktiken der „Rassendiskriminierung" gegenüber Personen, Personengruppen oder Einrichtungen zu unterlassen und dafür zu sorgen, dass alle staatlichen sowie kommunalen Behörden und öffentlichen Einrichtungen im Einklang mit dieser Verpflichtung handeln. Ergänzend stellt Artikel 5 ICERD ausdrücklich fest, dass sich das Verbot auch auf die Praxis aller Organe der Rechtspflege und damit auch auf die Polizei bezieht. Artikel 14 EMRK gewährleistet den Genuss der Konventionsrechte und -freiheiten ohne Diskriminierung wegen der „Rasse".

24 So der Wortlaut von Artikel 10 der JI-Richtlinie (EU) 2016/680.

25 Die deutsche Fassung von ICERD übersetzt „ethnic origin" mit „Volkstum". Daneben und synonym dazu existiert der (rechtliche) Begriff „Volkszugehörigkeit", so etwa in § 3 Antiterrordateigesetz, wo er eine polizeiliche Datenart beschreibt.

26 Barskanmaz (2022); Ruch (2022).

Umstritten ist dabei, wie der Begriff „Rasse“ auszulegen ist.[27] Traditionell dominieren im juristischen Schrifttum biologistische Positionen, die „Rasse“ als Gruppe von Menschen mit tatsächlich oder vermeintlich vererbbaren Eigenschaften verstehen.[28] Ihnen liegt immer noch die Vorstellung zugrunde, dass es „Rassen“ im biologistischen Sinne geben könnte. Andere Stimmen verstehen „Rasse“ dagegen als sozial konstruierte Kategorie, die auch anknüpft an (zugeschriebene,) angeblich kulturell bedingte Eigenschaften, denen sich die Mitglieder einer so konstruierten Gruppe nicht entziehen können.[29] Das Deutsche Institut für Menschenrechte[30] sowie zahlreiche weitere Stimmen aus Wissenschaft[31] und Selbstvertretungsorganisationen[32] empfehlen hingegen, den Begriff „Rasse“ aus dem Grundgesetz zu streichen und durch „rassistisch“ zu ersetzen, um dem Dilemma zu entkommen, Vorstellungen von „Rasse“ durch Normen zum Diskriminierungsschutz zu reproduzieren.

Eine Legaldefinition rassistischer Diskriminierung findet sich in Artikel 1 Absatz 1 ICERD, wonach der „Ausdruck ‚Rassendiskriminierung‘ jede auf der Rasse, der Hautfarbe, der Abstammung, dem nationalen Ursprung oder dem Volkstum beruhende Unterscheidung, Ausschließung, Beschränkung oder Bevorzugung umfasst, die zum Ziel oder zur Folge hat, dass dadurch ein gleichberechtigtes Anerkennen, Genießen oder Ausüben von Menschenrechten und Grundfreiheiten im politischen, wirtschaftlichen, sozialen, kulturellen oder jedem sonstigen Bereich des öffentlichen Lebens vereitelt oder beeinträchtigt wird“.[33] Die Definition bringt zum Ausdruck, dass rassistische Diskriminierung auf dem (biologistischen oder kulturalistischen) Konstrukt „Rasse“ beruht, und sie benennt weitere Kriterien, die – je nach Staat und Gesellschaft – typischerweise Anknüpfungspunkte für rassistische Diskriminierung waren und sind.[34] Diese weiteren Kriterien sind deshalb „verdächtige“ Kategorien, ihrer Nutzung wohnt ein hohes Diskriminierungsrisiko inne. Andere Menschenrechtsverträge und das Grundgesetz nennen aus demselben Grund noch die Kategorien Religion und Sprache, und der Vertragsausschuss zu ICERD wertet dementsprechend unter bestimmten Bedingungen auch eine Benachteiligung aufgrund von Sprache oder Religion als rassistische Diskriminierung, etwa wenn hieran anknüpfende Regelungen Angehörige einer nationalen, ethnischen oder religiösen Minderheit diskriminieren.[35]

Während bei biologistisch oder kulturalistisch begründetem Rassismus die Diskriminierung offenkundig ist, ist bei der Anknüpfung an die genannten Kategorien mit hohem Diskriminierungsrisiko zu überprüfen, ob sie zu einer rassistischen Diskriminierung führt. Nach Rechtsprechung des Bundesverfassungsgerichts kann eine Ungleichbehandlung nur in Ausnahmefällen und lediglich durch kollidierendes Verfassungsrecht gerechtfertigt werden. Dabei sind die Anforderungen sehr hoch; in jedem Fall muss eine Unterscheidung zwingend erforderlich sein und auf hinreichend sachlichen Gründen beruhen, die nichts mit einer bestehenden gesellschaftlichen Marginalisierung der Gruppe zu tun haben.[36] Auch für den Europäischen Gerichtshof für Menschenrechte (EGMR) ist jede Ungleichbehandlung ohne sachliche oder vernünftige Begründung eine verbotene Diskriminierung; in keinem Fall lässt sich eine Ungleichbehandlung in demokratischen und pluralistischen Gesellschaften rechtfertigen, die sich ausschließlich oder in entscheidendem Ausmaß auf eines der Merkmale stützt.[37]

27 Die Diskussion kurz zusammenfassend: Liebscher (10.01.2023).
28 Stellvertretend für viele Kischel (2022).
29 U. a. Baer / Markard (2018), Rn. 470; Barskanmaz (2020); Kaneza (2020).
30 Cremer (2020).
31 U. a. Tabbara (2021).
32 U. a. Bundeskonferenz der Migrantenorganisationen (27.02.2020); Zentralrat Deutscher Sinti und Roma (15.06.2020).
33 Offizielle deutsche ICERD-Übersetzung nach Bundesgesetzblatt 1969 II, S. 961.
34 Siehe auch: Payandeh (2022), S. 220 f.
35 Barskanmaz (2019), S. 204–210; Payandeh (2022), S. 226 f.
36 Baer / Markard (2018), Rn. 432 f.
37 Europäischer Gerichtshof für Menschenrechte (2005): Timishev v. Russia, Urteil vom 13.12.2005, Beschwerde Nr. 55762/00 und 55974/00, Ziff. 56-58.

Unter Umständen kann auch die Ungleichbehandlung aufgrund von Staatsangehörigkeit eine rassistische Diskriminierung darstellen. Zwar erlaubt Artikel 1 Absatz 2 ICERD Unterscheidungen, Ausschließungen, Beschränkungen oder Bevorzugungen zwischen eigenen und fremden Staatsangehörigen. Dies bedeutet jedoch keinen Freibrief für die Diskriminierung von Nicht-Staatsbürger*innen. Vielmehr ist die Ausnahme eng auszulegen. Eine Ungleichbehandlung aufgrund von Staatsangehörigkeit oder Einwanderungsstatus stellt demnach eine rassistische Diskriminierung im Sinne von ICERD dar, „wenn die Kriterien für die unterschiedliche Behandlung, beurteilt im Lichte der Ziele und Zwecke des Übereinkommens, nicht zur Erreichung eines rechtmäßigen Ziels angewandt werden oder im Hinblick auf die Erreichung dieses Ziels unverhältnismäßig sind.“[38] Auch verfassungsrechtlich unterliegen Unterscheidungen, die an die Staatsangehörigkeit anknüpfen, aufgrund der Nähe zu Merkmalen wie Heimat oder Sprache und zu rassistischen Konstruktionen von Kollektiven strengen Rechtfertigungsanforderungen.[39]

Mit Blick auf die polizeiliche Datenverarbeitung lässt sich zusammenfassend feststellen: Die Polizei ist bei der Erhebung, Speicherung, Nutzung, Übermittlung und Löschung von personenbezogenen Daten sowohl an das Recht auf Privatsphäre und Datenschutz als auch an das Verbot der rassistischen Diskriminierung gebunden. Kategorien, die nach weltweiter Erfahrung im Kontext rassistischer Diskriminierung verwendet wurden und werden, wie Hautfarbe, Abstammung, nationale oder ethnische Herkunft, Sprache, Religion oder Staatsangehörigkeit, sind grund- und menschenrechtlich nur zulässig, wenn ihre Verwendung einem strengen Maßstab standhält. Die Ungleichbehandlung der Angehörigen einer marginalisierten Gruppe anhand dieser Kriterien bedarf eines rechtmäßigen Sachgrunds, muss zwingend erforderlich sein und darf nicht außer Verhältnis zum verfolgten Ziel stehen.

2.2 Die besondere Schutzwürdigkeit sensibler Daten

Aufgrund der erheblichen Diskriminierungsrisiken, die mit der Verarbeitung von Daten über Hautfarbe, Abstammung, nationale oder ethnische Herkunft, Sprache, Religion, Staatsangehörigkeit verbunden sind, gilt für diese Daten ein erhöhter Schutz. Dieser ist für den Bereich der polizeilichen Datenverarbeitung jedoch erst seit 2016 durch Artikel 10 der EU-Richtlinie (EU) 2016/680 über den Datenschutz bei Polizei und Strafjustiz („JI-Richtlinie“) ausdrücklich normiert. Die Richtlinie betrifft polizeiliche Datenverarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung.[40]

Grund- und menschenrechtlicher Rahmen
Seinen Ursprung hat das Konzept besonders schützenswerter Daten in Artikel 6 der Konvention 108 des Europarates (Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) aus dem Jahr 1981. Demnach dürfen personenbezogene Daten, „welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen“, nur automatisch verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet. Die besondere Schutzwürdigkeit ergibt sich dabei aus dem höchstpersönlichen Charakter der Daten, die für Betroffene

38 UN, Committee on the Elimination of Racial Discrimination (05.08.2004): General recommendation No. 30 on discrimination against non-citizens, UN-Doc CERD/C/64/Misc.11/rev.3, Ziff. 4. Deutsche Übersetzung der Allgemeinen Empfehlung in: Bundesministerium der Justiz und für Verbraucherschutz (2017), S. 43–47 (44).

39 Baer / Markard (2018), Rn. 483.

40 Die vollständige Bezeichnung der JI-Richtlinie lautet: 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. Die Richtlinie gilt nicht für jede Datenverarbeitung durch die Polizei, sondern nur für jene zu den aufgezählten Zwecken, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Datenschutzrechtliche Fragen betreffend die innere Organisation der Polizei etwa im Rahmen der Personalverwaltung, zur allgemeinen Gefahrenprävention und -aufklärung, zur Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat und Ähnliches fallen in den Anwendungsbereich der Datenschutz-Grundverordnung (EU) 2016/679. Siehe: Johannes / Weinhold (2018), Rn. 47.

identitätsprägend sind und deren Missbrauch ein hohes Schadenspotenzial hat.[41]

Ursprünglich war das Konzept besonders schützenswerter Daten dem deutschen Regelungsansatz fremd, weil dieser davon ausging, dass in Zeiten moderner Datenverarbeitung nicht die Art eines Datums entscheidend sei, sondern dessen Nutzbarkeit und Verwendungsmöglichkeiten und es somit keine Daten von mehr oder weniger Belang gebe.[42] Jedoch betonte auch das Bundesverfassungsgericht in seinen Entscheidungen zur Rasterfahndung und dem Antiterrordateigesetz die erhöhte Schutzwürdigkeit bestimmter Datenkategorien: In seinem Beschluss zur bundesweiten Rasterfahndung nach 9/11[43] stellte das Gericht die besondere Persönlichkeitsrelevanz von Informationen fest, die sich auf etwa in Artikel 3 Absatz 3 Grundgesetz oder in Artikel 140 Grundgesetz in Verbindung mit Artikel 136 Absatz 3 der Weimarer Reichsverfassung verfassungsrechtlich geschützte Bereiche beziehen.[44] Zusätzlich erhöht sah das Gericht die Intensität der Grundrechtseingriffe und damit auch die Anforderungen an ihre Rechtfertigung durch das Risiko, dass die Verarbeitung solch sensibler Daten – im konkreten Fall die Rasterung nach islamischer Religionszugehörigkeit und der Herkunft aus Ländern mit überwiegend muslimischer Bevölkerung – Vorurteile reproduziert und ganze Bevölkerungsgruppen stigmatisiert.[45] In seinem Urteil zum Antiterrordateigesetz von 2013 betonte das Gericht erneut, dass für die Verarbeitung sensibler Daten – hier die durch das Antiterrordateigesetz vorgegebenen Datenkategorien Volks- und Religionszugehörigkeit – besonders hohe Anforderungen gelten, da für sie gemäß Artikel 3 Absatz 3 Grundgesetz ein besonderer verfassungsrechtlicher Diskriminierungsschutz besteht.[46]

Auch der EGMR misst dem Schutz sensibler Daten eine besondere Rolle zu. So sah er sich im Fall Catt gegen das Vereinigte Königreich sogar dazu veranlasst, die Erforderlichkeit einer polizeilichen Datenspeicherung trotz des Einschätzungsspielraums („margin of appreciation"), der Staaten üblicherweise in Sicherheitsfragen eingeräumt wird, erneut zu prüfen, weil die britischen Gerichte den Aspekt der besonderen Schutzwürdigkeit der infrage stehenden Daten außer Acht gelassen hatten.[47]

Der Schutz sensibler Daten bei der Polizei und die „JI-Richtlinie"

Gleichwohl war lange unklar, wie der gebotene besondere Schutz sensibler Daten in der polizeilichen Datenverarbeitung umzusetzen sei. Nachdem Deutschland die Konvention 108 des Europarates (Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) im Jahr 1985 ratifiziert hatte, blieb eine entsprechende Anpassung des nationalen Rechts der polizeilichen Datenverarbeitung aus. Vor dem Hintergrund von Artikel 9 der Konvention, die Ausnahmen für die Datenverarbeitung zum Schutz der öffentlichen Sicherheit erlaubte, und der bereits erwähnten Tatsache, dass das Konzept besonders schützenswerter Daten der deutschen Datenschutztradition fremd war, gingen die deutschen Gesetzgeber damals davon aus, dass das Recht der polizeilichen Datenverarbeitung innerstaatlich einen geeigneten Schutz sicherstellte. Sie sahen weder Änderungsbedarf bei den Polizei- noch bei den Datenschutzgesetzen in Bund und Ländern.

Einen ersten Standard zum Schutz sensibler Daten, der sich ausdrücklich auf die polizeiliche Datenverarbeitung bezog, setzte die 1987 verabschiedete Empfehlung R (87) 15 des Ministerkomitees

41 Weichert (2017).

42 Albers (2005), S. 328.

43 In der Entscheidung ging es um die bundesweite Rasterfahndung, die nach dem 11. September 2001 zur Suche nach sogenannten „Schläfern" durchgeführt wurde. Dafür wurden unter anderem Daten zur Religion und nationalen Herkunft von Einwohnermeldeämtern, Universitäten und aus dem Ausländerzentralregister erhoben und anschließend nach bestimmten Kriterien gerastert.

44 Bundesverfassungsgericht (2006): Rasterfahndung II. Beschluss vom 04.04.2006, 1 BvR 518/02, Rn. 99.

45 Ebd., Rn. 111 f.

46 Bundesverfassungsgericht (2013): Antiterrordateigesetz. Urteil vom 24.04.2013, 1 BvR 1215/07, Rn. 189. Eine Konsequenz aus der Entscheidung war der Erlass einer öffentlich zugänglichen Verwaltungsvorschrift zum sogenannten Katalogmanual unter anderem zu den Datenarten „Volks- und Religionszugehörigkeit" durch das Bundeskriminalamt (2015).

47 Europäischer Gerichtshof für Menschenrechte (2019): Catt v. United Kingdom, Urteil vom 24.01.2019, Beschwerde Nr. 43514/15, Ziff. 109–112.

des Europarates. Demnach sollte die Erhebung von Daten über Personen allein aufgrund ihrer „rassischen Herkunft", ihrer religiösen Überzeugungen, ihres Sexualverhaltens, ihrer politischen Überzeugungen oder ihrer Zugehörigkeit zu legalen Gruppen oder Organisationen verboten werden und eine Erhebung von Daten über diese Merkmale nur erfolgen dürfen, wenn dies für die Zwecke einer bestimmten Untersuchung unbedingt erforderlich ist.[48] Damit sollte zum einen die Errichtung von Dateien zur Sondererfassung von Minderheiten ausgeschlossen und zum anderen sichergestellt werden, dass die Erhebung und Weiterverwendung sensibler Daten durch die Polizei nur ausnahmsweise erfolgt. Allerdings handelte es sich bei den Vorgaben lediglich um rechtlich unverbindliche Empfehlungen.

Als das Konzept sensibler Daten durch die Umsetzung der europäischen Datenschutz-Richtlinie 95/46/EG[49] in den 1990er-Jahren auch Einzug ins deutsche Datenschutzrecht hielt, blieb die polizeiliche Datenverarbeitung davon weitgehend unberührt. So bestimmte etwa die alte Fassung des Bundeskriminalamtgesetzes (BKAG) ausdrücklich, dass die Regeln des Bundesdatenschutzgesetzes (BDSG) zur Erhebung und Verarbeitung von „besonderen Arten personenbezogener Daten" durch öffentliche Stellen keine Anwendung bei der Erfüllung von Aufgaben durch das Bundeskriminalamt (BKA) finden.[50] Somit blieb die oben genannte Empfehlung R (87) 15 des Europarates von 1987 über viele Jahre der einzige, jedoch rechtlich unverbindliche Standard zum Schutz sensibler Daten bei der Polizei.[51]

Dies änderte sich erst mit der Verabschiedung der Richtlinie (EU) 2016/680 über den Datenschutz bei Polizei und Strafjustiz („JI-Richtlinie"), die bis Mai 2018 in nationales Recht umgesetzt werden musste. Laut Artikel 10 der JI-Richtlinie ist die „Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, [...] nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt".[52] Außerdem muss die Verarbeitung nach nationalem oder EU-Recht zulässig sein, der Wahrung lebenswichtiger Interessen von natürlichen Personen dienen oder sich auf Daten beziehen, die Betroffene bereits öffentlich gemacht haben.

Der Begriff Daten „aus denen die rassische oder ethnische Herkunft [...] hervorgeht", wird in der Richtlinie nicht definiert. Zur Bedeutung und Reichweite des Begriffs können aber die Erwägungsgründe sowie Literatur zur Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) beziehungsweise zum BDSG herangezogen werden: Erwägungsgrund 37 der JI-Richtlinie betont, dass die „Verwendung des Begriffs ‚rassische Herkunft' [...] nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt".[53]

48 Council of Europe (1987): Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, Principle 2.4. Eigene Übersetzung, eine Übersetzung in deutscher Sprache liegt nicht vor.

49 Art. 8 Abs. 1 der Richtlinie bestimmte ein grundsätzliches Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten", unter anderem zu „rassischer und ethnischer Herkunft". Umgesetzt wurden die europarechtlichen Vorgaben im alten BDSG mit leicht abweichender Terminologie („besondere Arten personenbezogener Daten") unter anderem durch die Begriffsbestimmung in § 3 Abs. 9 sowie die Regeln zur Erhebung, Verarbeitung und Übermittlung solcher Daten durch öffentliche Stellen in §§ 13, 14 und 16.

50 § 37 BKAG alte Fassung.

51 Dies gilt jedoch nicht für die polizeiliche Datenverarbeitung zur inneren Organisation, etwa zur Personalverwaltung, die bereits zuvor in den Anwendungsbereich der EU-Datenschutzrichtlinie 95/EG/46 fiel (und inzwischen durch die Datenschutzschutzgrundverordnung (EU) 2016/679 reguliert wird), und den Informationsaustausch im Rahmen der innereuropäischen Polizeikooperation, für den seit 2009 der EU-Rahmenbeschluss 2008/977/JI gilt. Sowohl die EU-Datenschutzrichtlinie als auch der Rahmenbeschluss kannten mit Art. 8 beziehungsweise Art. 6 Normen zum Schutz sensitiver Daten.

52 Art. 10 JI-Richtlinie nennt außerdem genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung als besondere Kategorien personenbezogener Daten.

53 In ähnlicher Form heißt es im sechsten Erwägungsgrund der Antirassismus-Richtlinie 2000/43/EG wörtlich: „Die Europäische Union weist Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, zurück. Die Verwendung des Begriffs ‚Rasse' in dieser Richtlinie impliziert nicht die Akzeptanz solcher Theorien." In der deutschen Fassung von Art. 2 der Antirassismus-Richtlinie wird der Begriff „Rasse" genutzt, wohingegen es in der englischen Fassung „racial [...] origin" heißt. Ausführlich zur Bedeutung des Begriffs „racial or ethnic origin" in der Antirassismus-Richtlinie: Farkas (2017).

Insofern soll die Formulierung kein biologistisches Verständnis von „rassischer Herkunft“ und „Rasse“ implizieren, sondern dem Schutz vor Rassismus dienen. Gleichwohl dominiert in der datenschutzrechtlichen Diskussion die Lesart, dass der Begriff auf biologische Abstammung und vererbbare Eigenschaften abstelle, womit – ähnlich wie durch die traditionell vorherrschende juristische Interpretation des „Rasse“-Begriffs – rassistische Vorstellungen reproduziert werden, obwohl das Datenschutzrecht vor Diskriminierung schützen soll.[54]

Als Beispiele für sensible Daten zur zugeschriebenen „rassischen oder ethnischen Herkunft“ (vgl. Kasten S. 15) gemäß Artikel 9 DSGVO nennt die Kommentarliteratur ethnische Zuschreibungen, aber auch Angaben zum äußeren Erscheinungsbild einer Person, etwa zur Hautfarbe, oder zu typischen, regional begrenzten Sprachen. Dabei müssen die verarbeiteten Daten nicht zwingend unmittelbar Informationen über ein Diskriminierungsmerkmal enthalten; vielmehr genügt es, wenn sich solche Hinweise mittelbar aus dem Gesamtzusammenhang der Verarbeitung ergeben.[55] So entschied der Europäische Gerichtshof im August 2022 anlässlich einer Vorlage aus Litauen, dass selbst die Veröffentlichung von Informationen, die „mittels gedanklicher Kombination“ nachteilige Hinweise auf besonders geschützte Daten geben könnten, durch Artikel 9 DSGVO geschützt seien.[56] Somit kann unter Umständen auch abgeleitet aus Namen oder anderen „Stellvertreterdaten“ („proxy data“) wie der Postleitzahl eines überwiegend von einer bestimmten Minderheit bewohnten Stadtviertels oder dem Wunsch eines Flugreisenden nach Essen ohne Schweinefleisch eine „rassische oder ethnische Herkunft“ zugeschrieben werden.[57] Als grundsätzlich nicht erfasst von der Kategorie sieht die datenschutzrechtliche Kommentarliteratur Nationalität oder Staatsangehörigkeit.[58] Dabei wird in einem verkürzten Verständnis des Schutzes vor rassistischer Diskriminierung verkannt, dass Unterscheidungen nach Nationalität oder Staatsbürgerschaft dann rassistisch sein können, wenn die oben genannten strengen Rechtfertigungsanforderungen verfehlt werden.[59] Insofern wird hier die Auffassung vertreten, dass im Falle solcher Verfehlungen eine Zuschreibung „rassischer oder ethnischer Herkunft“ auch mittels Nationalität oder Staatsangehörigkeit erfolgen kann und die Daten dann als sensibel zu werten sind.

Zur Frage, was geeignete Garantien zum Schutz sensibler Daten sind, notieren die Erwägungsgründe der JI-Richtlinie exemplarisch, „dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird“.[60]

Damit gelten zum Schutz vor Risiken rassistischer Diskriminierung für die polizeiliche Verarbeitung sensibler Daten besonders hohe Anforderungen. Europarechtlich erlaubt Artikel 10 JI-Richtlinie eine Verarbeitung solcher Daten nur dann, wenn sie unbedingt erforderlich ist, geeignete Schutzgarantien vorgesehen sind und sie – von in der Polizeipraxis seltenen Ausnahmen abgesehen – eine gesetzliche Grundlage hat. Welche Daten dabei das Risiko rassistischer Diskriminierung bergen und entsprechend zu schützen sind, ergibt sich allerdings erst im konkreten Verarbeitungskontext.

2.3 Unzureichende Umsetzung von Artikel 10 der JI-Richtlinie ins deutsche Recht

Für die polizeiliche Verarbeitung sensibler Daten gelten besonders hohe Anforderungen. Dieses Kapitel lenkt den Blick nun auf die Rechtslage in Deutschland und untersucht, welchen Schutz sensible Daten zu „rassischer oder ethnischer

54 Zum Datenschutz als Solidaritätsgebot siehe Bielefeldt (2011).
55 Petri (2019), Rn. 11–16; Weichert (2024), Rn. 25 f.
56 Europäischer Gerichtshof (2022): Urteil vom 01.08.2022, C-184/20, Ziff. 125. Siehe dazu auch Nabulsi (2024).
57 Siehe hierzu auch Europäische Kommission gegen Rassismus und Intoleranz (2020), Ziff. 32.
58 Siehe etwa Petri (2019), Rn. 16; Weichert (2024), Rn. 26.
59 Siehe die Ausführungen hierzu in Kapitel 2.1.
60 Erwägungsgrund 37 der JI-Richtlinie.

Herkunft“ (vgl. Kasten S. 15) genießen und wie Artikel 10 der JI-Richtlinie in nationales Recht umgesetzt wurde. Die Umsetzung der JI-Richtlinie in nationales Recht hätte gemäß Artikel 63 der Richtlinie bis 6. Mai 2018 erfolgen müssen. Die folgende Analyse zeigt, dass die Anpassung des Polizeirechts beziehungsweise des Rechts der polizeilichen Datenverarbeitung in Deutschland zumeist erst deutlich später und im Ergebnis unzureichend stattfand. In der Folge besteht kein hinreichender gesetzlicher Schutz vor Risiken rassistischer Diskriminierung bei der polizeilichen Verarbeitung sensibler Daten.

2.3.1 Umsetzung auf Bundesebene

Aus Sicht der Bundesregierung wurde die JI-Richtlinie für die Polizeien des Bundes bereits weitgehend durch Teil III des neu gefassten BDSG vom 30. Juni 2017 umgesetzt.[61] Teil III umfasst die Bestimmungen über die Datenverarbeitung durch öffentliche Stellen, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten sowie den Schutz und die Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind,[62] also im Wesentlichen für Polizei, Zoll, Steuerfahndung und Staatsanwaltschaft. Für Polizeibehörden und andere zuständige Stellen der Länder gelten die Regeln nur, soweit der Datenschutz nicht durch Landesrecht geregelt ist,[63] was inzwischen jedoch flächendeckend gegeben ist (siehe S. 24 ff. zu den Ländern).

Maßgeblich ist Teil III des BDSG somit für die Polizeien des Bundes, also Bundespolizei, Bundeskriminalamt und die Polizei des Deutschen Bundestages. Anders als für das Bundeskriminalamt (BKA), das mit der Neufassung des BKA-Gesetzes von 2017 auch die Verweise auf das neue BDSG aktualisierte, steht eine solche Neufassung des Gesetzes über die Bundespolizei weiterhin aus. Ein Anlauf zu seiner Novellierung war in der 19. Legislaturperiode gescheitert.[64] Somit ist auch fünf Jahre nach Fristablauf die Umsetzung der JI-Richtlinie für die Bundespolizei nicht erfolgt, weswegen die Europäische Kommission im April 2022 ein Vertragsverletzungsverfahren gegen Deutschland einleitete.[65] Mit der Neuauflage des Gesetzgebungsverfahrens, zu dessen Auftakt im Mai 2023 ein Referentenentwurf zur Neustrukturierung des Bundespolizeigesetzes vorgelegt wurde, könnte das Defizit nun beseitigt werden.

Das neu gefasste BDSG soll den polizeilichen Umgang mit sensiblen Daten regeln. § 46 Nr. 14 BDSG übernimmt für die Bestimmung des Begriffs der besonderen Kategorien personenbezogener Daten den Katalog aus Artikel 10 der JI-Richtlinie textgleich. Nach § 48 Absatz 1 BDSG ist die Verarbeitung besonderer Kategorien personenbezogener Daten nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Gemäß § 48 Absatz 2 BDSG sind bei einer Verarbeitung solcher Daten geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen, die in einem unabgeschlossenen Katalog exemplarisch aufgezählt werden: Genannt werden spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle, die Festlegung besonderer Fristen zur Überprüfung der Datenspeicherung (Aussonderungsprüffristen), die Sensibilisierung von datenverarbeitendem Personal, Beschränkungen des Zugangs zu den Daten, die von anderen Daten getrennte Verarbeitung, die Pseudonymisierung oder Verschlüsselung der Daten sowie spezifische Verfahrensregeln bei Übermittlungen oder Änderungen des Datenverarbeitungszwecks.

Allerdings ist juristisch umstritten, inwiefern § 48 BDSG überhaupt als Rechtsgrundlage für die Verarbeitung von sensiblen Daten dienen kann. Die Norm gilt als „unspezifische Generalklausel“ [66] oder „unvollständige Rechtsgrundlage“[67], welche die Voraussetzungen für die Datenverarbeitung nur

61 Siehe Deutscher Bundestag (09.02.2021), S. 2.
62 § 45 BDSG.
63 § 1 Abs. 1 BDSG.
64 Entsprechend verweist § 37 Bundespolizeigesetz weiterhin auf das BDSG in seiner alten Fassung vor der Umsetzung und Anpassung an die EU-Datenschutzreform.
65 Europäische Kommission (25.07.2022), S. 10.
66 Schwichtenberg (2020), Rn. 7.
67 Frenzel (2021), Rn. 4.

„relativ abstrakt und vage“ bestimmt.[68] Insbesondere eingriffsintensive Maßnahmen müssen jedoch hinreichend bestimmt und normenklar geregelt sein. Somit lasse sich eine Verarbeitung sensibler Daten nicht pauschal auf § 48 BDSG stützen, da etwa die Speicherung sensibler Daten zur Dokumentation polizeilicher Vorgänge eine völlig andere Qualität habe als ihre Nutzung zur Rasterfahndung. Überwiegend wird daher die Auffassung vertreten, dass § 48 BDSG höchstens als Eingriffsbefugnis für Datenverarbeitungsprozesse dienen kann, von denen ein geringes Risiko für die Rechte Betroffener ausgehe.[69] Andere Stimmen argumentieren, dass die Verarbeitung sensibler Daten immer eine eingriffsintensive Maßnahme sei, und halten spezifische polizeirechtliche Befugnisnormen insbesondere zur Klarstellung der Zwecke daher grundsätzlich für geboten.[70]

Zudem hat der Gesetzgeber mit dem unverbindlichen, nicht abschließenden Katalog von Schutzmaßnahmen in § 48 Absatz 2 BDSG darauf verzichtet, Garantien explizit oder durch Verordnungsermächtigung festzulegen. Damit bleibt die Wahl der Mittel der datenverarbeitenden Stelle überlassen. Untergesetzliche Regelungen sind aber häufig nicht einsehbar und garantieren keinen Umsetzungsanspruch. Mindestens für eingriffsintensive Maßnahmen ist damit der Bestimmtheitsgrundsatz verletzt.[71] Außerdem beschränkt sich der Katalog auf technisch-organisatorische Maßnahmen, obwohl auch materiell-rechtliche Maßnahmen wie Richtervorbehalte, klare Vorgaben zur Kontrolle durch Aufsichtsbehörden oder weitergehende Betroffenenrechte zielführend sein könnten.[72]

Im Ergebnis ist festzuhalten, dass § 48 BDSG sein Ziel verfehlt. Er stellt keine hinreichend bestimmte Rechtsgrundlage für eine generelle Verarbeitung sensibler Daten durch die Polizeien des Bundes dar. Für einen wirksamen Schutz Betroffener im Sinne von Artikel 10 JI-Richtlinie fehlen Regelungen im Fachrecht, die spezifische Vorgaben zu Voraussetzungen und Schutzmaßnahmen machen. Entsprechende Einwände waren bereits 2021 im Zusammenhang mit der Evaluierung der gesetzlichen Umsetzung der EU-Datenschutzreform in Deutschland von der Konferenz der Datenschutzbeauftragten von Bund und Ländern vorgetragen worden.[73] Leider wurden sie damals vom Bundesinnenministerium verworfen, unter anderem mit dem Hinweis, dass eine offene Formulierung geboten sei, da für den Gesetzgeber nicht alle Gesichtspunkte vorhersehbar seien, unter denen eine Verarbeitung sensibler Daten durch Sicherheitsbehörden erforderlich sein könnte.[74]

2.3.2 Umsetzung auf Landesebene

Mit teilweise deutlicher Verspätung haben mittlerweile auch alle Bundesländer die JI-Richtlinie in Landesrecht umgesetzt. Für die Regelung der polizeilichen Verarbeitung sensibler Daten lassen sich dabei drei Modelle der Umsetzung unterscheiden:[75]

- Allgemeines Datenschutzrecht: Sieben Bundesländer setzen die europarechtlichen Vorgaben überwiegend im allgemeinen Datenschutzrecht um, das heißt in den jeweiligen Landesdatenschutzgesetzen. Diese beinhalten, vergleichbar dem BDSG, ein gesondertes Kapitel zum Datenschutz im Anwendungsbereich der JI-Richtlinie und entsprechende Vorgaben für die polizeiliche Verarbeitung sensibler Daten. Teilweise wurden allerdings auch Vorschriften des Polizeirechts angepasst und mit den Datenschutzgesetzen verknüpft, was der Verständlichkeit der Regeln wenig zuträglich ist. Bei den Ländern handelt es sich um Berlin, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Schleswig-Holstein und Thüringen.

68 Albers / Schimke (2023), Rn. 9.
69 So etwa: Schwichtenberg (2020), Rn. 7; Braun (2022), Rn. 3 ff.; Kampert (2022), Rn. 18; Albers / Schimke (2023), Rn. 12.
70 Johannes / Weinhold (2018), Rn. 149.
71 Siehe hierzu: Braun (2022), Rn. 15; Albers / Schimke (2023), Rn. 33.
72 Schwichtenberg (2020), Rn. 6; Braun (2022), Rn. 13.
73 Datenschutzkonferenz (2021), S. 13 f.
74 Bundesministerium des Innern, für Bau und Heimat (2021), S. 90 ff.
75 Die folgenden Ausführungen stützen sich auf ein vom Deutschen Institut für Menschenrechte beauftragtes Rechtsgutachten aus dem Jahr 2022. Die Ergebnisse sind teilweise nachzulesen in: Arzt (2023).

- Besonderes Datenschutzrecht: Fünf Bundesländer normieren die polizeiliche Verarbeitung sensibler Daten im besonderen Datenschutzrecht, also in Spezialgesetzen über die polizeiliche Datenverarbeitung, ebenfalls teilweise verknüpft mit dem Polizeirecht. Diesen Weg gewählt haben Brandenburg, Hamburg, das Saarland, Sachsen und Sachsen-Anhalt.

- Landespolizeigesetze: Nur in vier Bundesländern wird die polizeiliche Verarbeitung sensibler Daten im Wesentlichen durch die Landespolizeigesetze geregelt und ist damit sowohl für Rechtsanwender*innen als auch Betroffene leicht nachvollziehbar. Dies ist der Fall in Baden-Württemberg, Bayern, Bremen und Mecklenburg-Vorpommern.

Die Regelungen unterscheiden sich nicht nur in der Gesetzgebungstechnik, sondern auch inhaltlich teilweise deutlich. So wird in Mecklenburg-Vorpommern in der Legaldefinition besonderer Kategorien personenbezogener Daten bewusst auf den Begriff der „rassischen Herkunft“ verzichtet und lediglich auf „ethnische Herkunft“ abgestellt.[76] In Bremen nennt die Definition Daten, aus denen eine „zugeschriebene rassische Herkunft“ hervorgeht, und weicht damit ebenfalls bewusst von der Terminologie der JI-Richtlinie ab.[77]

Auch hinsichtlich der Voraussetzungen für die Verarbeitung sensibler Daten haben einige Landesgesetzgeber andere Begrifflichkeiten gewählt. Teilweise soll so der strengere Verarbeitungsmaßstab deutlicher markiert werden: In Niedersachsen[78] und Brandenburg[79] ist die polizeiliche Verarbeitung sensibler Daten grundsätzlich nur zulässig, wenn sie – wie in manchen Datenschutzkommentaren empfohlen[80] – für die Aufgabenerfüllung „unerlässlich“ (statt „unbedingt erforderlich“) ist. Teilweise werden durch andere Begrifflichkeiten aber auch die Standards der JI-Richtlinie unterschritten: In Bayern ist die Datenverarbeitung bereits zulässig, wenn „andernfalls die Erfüllung polizeilicher Aufgaben, insbesondere die Verhütung oder Unterbindung von Straftaten, gefährdet oder wesentlich erschwert“ wäre.[81]

Vereinzelt finden sich begrüßenswerte Ansätze für Maßnahmen, die einen besonderen Schutz versprechen. So sehen etwa die Polizeigesetze in Bayern[82] und Mecklenburg[83] – mit Einschränkungen – Pflichten zur Kennzeichnung sensibler Daten vor, sodass entsprechend zum Beispiel Zugriffsrechte oder die Datenübermittlung beschränkt werden könnten.[84] In Bayern sollen sensible Daten außerdem bei der Festlegung von Fristen zur Löschung oder Prüfung besonders berücksichtigt werden.[85] In Bremen ist sogar vorgesehen, dass bei sensiblen Daten spätestens nach zwei Jahren geprüft werden muss, ob die Speicherung der Daten weiterhin erforderlich ist.[86]

In der Regel aber erfolgte die Umsetzung der Vorgaben der JI-Richtlinie in den Ländern lediglich schematisch, indem Artikel 10 der Richtlinie oder § 48 BDSG mehr oder weniger im Wortlaut übernommen wurde. Die tatbestandlichen Voraussetzungen für die Datenverarbeitung werden in keinem Bundesland präzisiert und verbindliche Vorgaben für konkrete Schutzmaßnahmen sind seltene Ausnahmen. Damit gilt grundsätzlich auch für die Länder, dass die polizeiliche Verarbeitung sensibler Daten nur unzureichend geregelt ist.

76 § 3 Abs. 5 Nr. 3 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern.
77 § 21 Nummer 21 Bremisches Polizeigesetz.
78 § 25 Absatz 3 Niedersächsisches Datenschutzgesetz.
79 § 9 Abs. 1 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz.
80 Braun (2022), Rn. 9.
81 Art. 30 Abs. 2 Bayerisches Polizeiaufgabengesetz.
82 Art. 53 Abs. 5 Bayerisches Polizeiaufgabengesetz.
83 § 46g Abs. 1 Nr. 9 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern.
84 Grundsätzlich zur Kennzeichnung sensibler Daten als Voraussetzung für die Einhaltung spezifischer Verfahrensregelungen bei deren Weiternutzung und Übermittlung: Weichert (2022), S. 847 f.
85 Art. 53 Abs. 5 Bayerisches Polizeiaufgabengesetz.
86 § 58 Abs. 6 Bremisches Polizeigesetz.

3 Sensible Daten in der polizeilichen Praxis

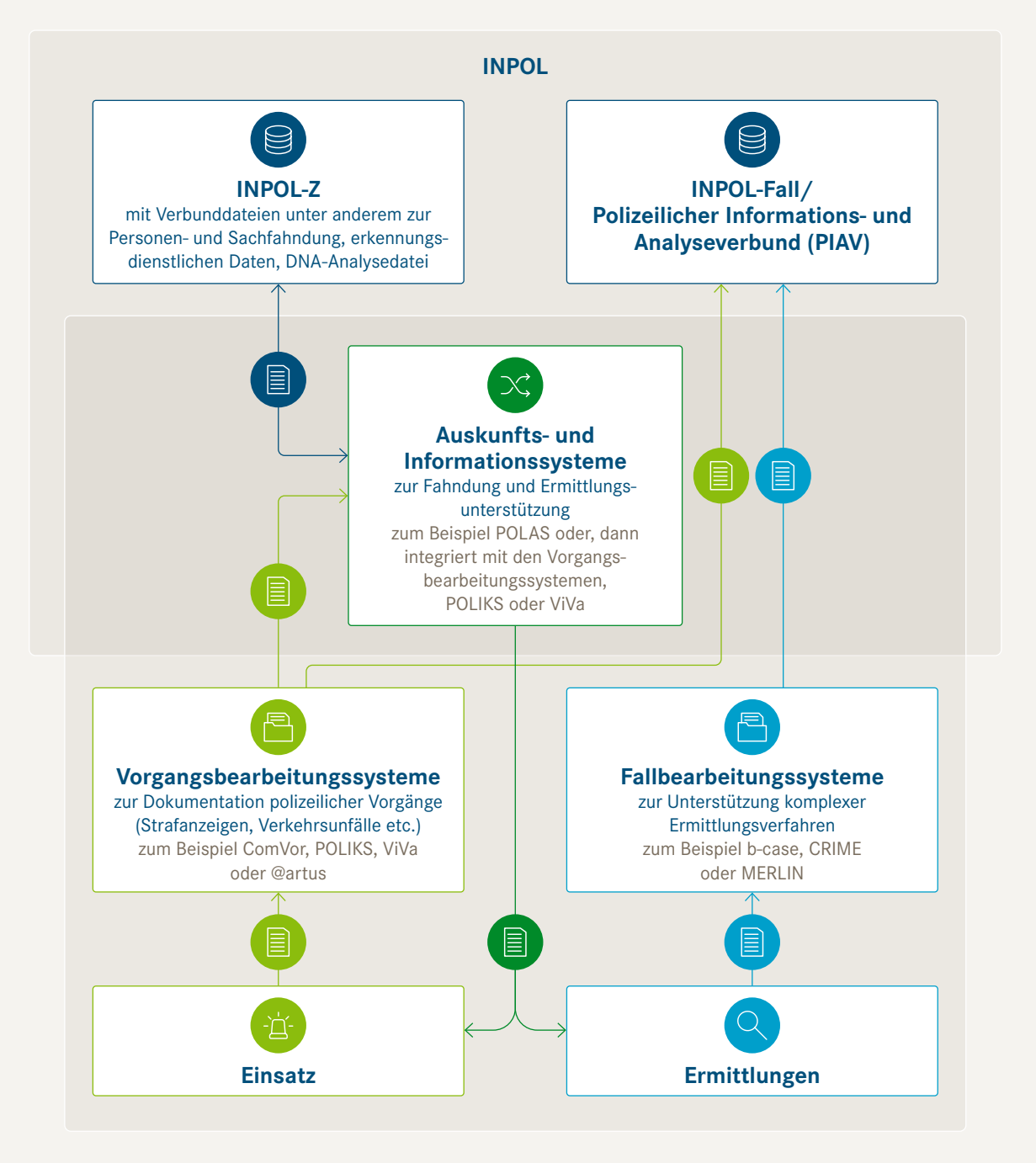
Im Folgenden liegt der Fokus auf der polizeilichen Praxis und der Frage, wie die Polizei sensible Daten zu „rassischer und ethnischer Herkunft“ (vgl. Kasten S. 15) tatsächlich in ihren Informationssystemen verarbeitet. Insbesondere vor dem Hintergrund der unzureichenden gesetzlichen Vorgaben (vgl. 2.3) stellt sich die Frage, welche Kategorien sensibler Daten gespeichert und genutzt werden. Die in diesem Kapitel ausgeführten Beispiele aus der Praxis verdeutlichen auch, welche Risiken rassistischer Diskriminierung bestehen. Zum besseren Verständnis der Darstellung wird zuerst eine kurze Einführung in Stand und Perspektiven der polizeilichen Datenverarbeitung in Deutschland gegeben.

Polizeiarbeit hat, wie der ehemalige BKA-Chef Horst Herold 1970 schrieb, „schon immer im Sammeln, Speichern und Verarbeiten von Daten bestanden“.[87] Diese Wissensarbeit ist zentraler Aspekt des Handelns der polizeilichen Eingriffsverwaltung. Was im 19. Jahrhundert mit dem Aufbau des Erkennungsdienstes, des kriminalpolizeilichen Meldedienstes, seiner zentralen Karteien, Verbrecherlisten und Fahndungsbücher begann, wird seit den späten 1960er-Jahren in wachsendem Maße digitalisiert.[88] Heute sind IT-Systeme das Rückgrat der Dokumentation und Verwaltung polizeilicher Vorgänge, der Speicherung von Informationen zur Gefahrenabwehr, zur Verhütung und Verfolgung von Straftaten sowie anderer polizeilicher Aufgaben.

Aktuell sind die Datenbestände der deutschen Polizeien in einer sehr heterogenen Landschaft von Informationssystemen verteilt. Eine offizielle Bestandsaufnahme im Rahmen des aktuellen Programms zur Modernisierung der polizeilichen IT-Architektur ergab rund 2.000 relevante Anwendungen in Deutschland, darunter zwölf verschiedene Vorgangsbearbeitungssysteme, 15 Fallbearbeitungssysteme und allein beim Bundeskriminalamt mehr als 70 Datenbanken, in denen Informationen von überregionaler Bedeutung gespeichert sind.[89] Die Dimension der Systeme unterscheidet sich entsprechend ihrer Zwecke, der Anzahl beteiligter Dienststellen und Behörden, des Umfangs der gespeicherten Daten und ihrer Funktionalitäten.[90] Abbildung 2 gibt einen knappen und damit notwendigerweise vereinfachten Überblick über die wichtigsten Systeme. Das Glossar (S. 26 f.) enthält Hintergrundinformationen zu den wichtigsten polizeilichen IT-Systemen und Datenbanken.

87 Herold (1970), S. 33.
88 Heinrich (2007), S. 121 ff.
89 Schäberle (2023), S. 1432.
90 Arzt (2021), Rn. 1110.

Abbildung 2: Polizeiliche Informationssysteme (vereinfachte Darstellung)



Glossar: Polizeiliche IT-Systeme

Vorgangsbearbeitungssysteme sind traditionell das Rückgrat der polizeilichen Informationsverarbeitung. Sie hören auf Namen wie @rtus, ComVor, EVA, IVO, POLIKS oder ViVa, dienen der Dokumentation aller polizeilich relevanten Vorgänge und enthalten neben dem Sachverhalt etwa zu angezeigten Ordnungswidrigkeiten, Straftaten oder Verkehrsunfällen in großem Umfang Daten über Verdächtige, Geschädigte oder Zeug*innen.[91] So waren 2023 allein im Vorgangssystem @rtus-Bund der Bundespolizei 3,5 Millionen Vorgänge mit 4,3 Millionen Personendatensätzen gespeichert.[92] Beim Anlegen eines Vorgangs werden die zuständige Polizeidienststelle und das Aktenzeichen eingetragen und der Sachverhalt erfasst. Dabei wird die Erfassung durch standardisierte Formulare und Kataloge etwa zu Delikten strukturiert, lässt aber auch Raum für Erläuterungen im Freitext.[93]

Fallbearbeitungssysteme wie CASE, EASy, MERLIN, SAFIR oder KRISTAL werden zur Unterstützung komplexer kriminalpolizeilicher Ermittlungsverfahren auf Ebene einzelner Dienststellen oder von den Kriminalämtern betrieben. Sie haben die analogen kriminalpolizeilichen Karteikartensammlungen, Spurenakten etc. ersetzt. In den Systemen werden die zahlreichen Einzelinformationen zu Straftaten, Personen, Orten, Waffen, Telefonnummern etc. erfasst, aber auch Fotos, Videos und gescannte Dokumente. Über Schnittstellen können andere polizeiliche Datenbanken und weitere staatliche Register wie das Ausländerzentralregister oder die Daten der Meldebehörden abgefragt und im Trefferfall die Quelldaten als neue Objekte gespeichert werden. All diese Informationen können miteinander in Beziehung gesetzt und anschließend ausgewertet werden, um etwa Beziehungsnetzwerke zwischen Personen oder Tatorte auf einer digitalen Karte abzubilden. Zugriff auf die Fallbearbeitungssysteme hat in der Regel nur ein kleiner Kreis zuständiger Sachbearbeiter*innen.[94]

Auskunfts- und Fahndungssysteme und der polizeiliche Informationsverbund INPOL: Aus den Vorgangsbearbeitungs- und Fallbearbeitungssystemen werden (ausgewählte) Informationen übermittelt an und zusammengeführt in INPOL, dem seit 1972 existierenden elektronischen Informationsverbund der deutschen Polizeien. INPOL dient sowohl der Fahndung nach Personen und Sachen als auch für Auskünfte etwa zu Identifizierungszwecken. Beteiligt sind alle 19 Polizeien des Bundes und der Länder sowie der Zoll. INPOL besteht aus zwei Säulen:

Die erste INPOL-Säule ist das **zentrale System INPOL-Z**, das vom Bundeskriminalamt (BKA) betrieben wird. Es umfasst verschiedene sogenannte Verbunddateien etwa zur Personen- oder Sachfahndung, mit Fingerabdrücken, DNA-Profilen, Kriminalaktennachweisen oder Haftdaten. Zum anderen besteht INPOL aus den **Teilnehmersystemen** der Verbundpartner (häufig, aber unzutreffend INPOL-Land genannt). Dort stellen die lokalen Dienststellen Informationen ein und übermitteln die Daten bei bundesweiter Relevanz außerdem an INPOL-Z. In manchen Bundesländern sind die Vorgangsbearbeitungssysteme mit dem INPOL-Teilnehmersystem integriert und übernehmen damit gleichzeitig die Funktion eines Fahndungs- und Auskunftssystems. In anderen Bundesländern sind die Systeme getrennt, sodass das INPOL-Teilnehmersystem, häufig unter dem Namen POLAS, als polizeiliches Fahndungs- und Auskunftssystem parallel zum Vorgangsbearbeitungssystem existiert. Aus den INPOL-Teilnehmersystemen können üblicherweise auch andere staatliche Register wie etwa das Ausländerzentralregister oder die Daten der Meldeämter abgefragt werden. Zugriff haben alle Polizeibeamt*innen, Staatsanwaltschaften und Gerichte.

91 Arzt (2021), Rn. 1179 ff.
92 Deutscher Bundestag (28.04.2023), S. 16 f.
93 Konferenz der Leiterinnen und Leiter der Archivverwaltung des Bundes und der Länder (2020), S. 11 f.
94 Arzt (2021), Rn. 1289 ff.; Konferenz der Leiterinnen und Leiter der Archivverwaltung des Bundes und der Länder (2020), S. 15 f.; Eder (2005).

Die zweite **INPOL-Säule** ist INPOL-Fall, ein Auswerte- und Analysetool, das aus verschiedenen Dateien besteht und vom BKA geführt wird. Technisch handelt es sich bei diesen Dateien um Fallbearbeitungssysteme, nur dass sie nicht Informationen zu einzelnen Ermittlungskomplexen erfassen, sondern zu verschiedenen Phänomenbereichen von bundesweiter Bedeutung, etwa zu Rauschgiftkriminalität oder Staatsschutzdelikten. Seit 2016 werden die einzelnen Verbunddateien von INPOL-Fall sukzessive durch den **Polizeilichen Informations- und Analyseverbund (PIAV)** abgelöst, der alle gemeldeten Personen-, Fall-, und Sachdaten unabhängig vom Phänomenbereich in einer gemeinsamen Anwendung erfasst und für die operative und strategische Kriminalitätsanalyse nutzbar machen soll.

Neben den beschriebenen Systemen existieren im Bereich des polizeilichen Staatsschutzes außerdem **Projektdateien** zur Unterstützung zeitlich befristeter Analyseprojekte oder auch auf Dauer angelegte Informationssysteme wie die **Antiterror- und die Rechtsextremismusdatei**, die gemeinsam mit den Nachrichtendiensten und anderen Behörden genutzt werden. Für Zwecke der grenzüberschreitenden Polizeikooperation werden zudem über das Schengen-Informationssystem, die Computersysteme des europäischen Polizeiamtes Europol, die Datenbanken Interpols sowie über diverse andere bi- und multilaterale Foren, Plattformen und Netzwerke Daten mit Partnerbehörden im Ausland geteilt.

Programm P20: Vor dem Hintergrund der äußerst zersplitterten polizeilichen IT-Landschaft, die von Eigenentwicklungen, inkompatiblen Insellösungen, Mehrfacherfassung von Daten, unterschiedlichen Standards, Dateiformaten und Erhebungsregeln geprägt ist, hat die Innenministerkonferenz (IMK) am 30. November 2016 die **Saarbrücker Agenda** verabschiedet. Als Ziele werden die bessere Verfügbarkeit polizeilicher Informationen, eine höhere Wirtschaftlichkeit und ein stärkerer Datenschutz genannt.[95] Zur Umsetzung der Saarbrücker Agenda haben die Innenminister*innen von Bund und Ländern das Programm „P20“ (früher „Polizei 2020“) angestoßen, das bis etwa 2030 umgesetzt werden soll. Herzstück des Programms ist die Vision eines polizeilichen „Datenhauses“, in dem alle polizeilichen Daten nach einheitlichen Standards zentral und redundanzfrei vorgehalten werden. Im Rahmen von „P20“ wird aktuell an 35 Projekten gearbeitet, bei denen es insbesondere um die Bereitstellung einheitlicher Systeme für die Vorgangsbearbeitung, Fallbearbeitung und das Asservatenmanagement geht, die perspektivisch alle an das Datenhaus angebunden sein sollen.[96] Die polizeiliche Sachbearbeitung soll dann unabhängig von den Endgeräten durch intuitive „Apps“ unterstützt werden und das zentrale Datenhaus die Basis sein für den Einsatz neuer Technologien etwa zur „intelligenten“ Suche oder zur automatischen Erkennung von Personen oder Objekten in Bildern und Videos.[97]

Abbildung 2 (S. 25) und das Glossar (S. 26 f.) verdeutlichen, dass die Polizei in zahlreichen Systemen und in erheblichem Umfang personenbezogene Daten verarbeitet. Dabei geht es sowohl um Daten von Verurteilten, Beschuldigten, Tatverdächtigen und Personen, von denen angenommen wird, dass sie in Zukunft Straftaten begehen werden („Anlasspersonen“), aber auch um Daten von deren Kontakt- und Begleitpersonen, von Geschädigten und Opfern, Zeug*innen, Hinweisgeber*innen oder sonstigen Auskunftspersonen sowie von Vermissten und unbekannten hilflosen oder toten Personen.

So waren im April 2023 in INPOL knapp zehn Millionen Datensätze mit Nachweisen zu Fingerabdrücken, Lichtbildern und Personenbeschreibungen in der Datei „Erkennungsdienst“ erfasst und etwa 860.000 Personen zur Fahndung ausgeschrieben.[98] Zusätzlich waren Daten zu Millionen von Menschen in den Vorgangsbearbeitungssystemen

95 Innenministerkonferenz (30.11.2016).
96 Gadorosi / Matthey (2023).
97 Brück (2019).
98 Deutscher Bundestag (28.04.2023).

der Polizeien in Bund und Ländern gespeichert. Genaue Angaben zur Zahl der Betroffenen sind nicht möglich, da Personen in diesen Systemen häufig mehrfach erfasst werden; aber allein in Berlin und Schleswig-Holstein waren im Frühjahr 2023 jeweils rund zwei Millionen Einzelpersonen in den polizeilichen Vorgangsbearbeitungssystemen POLIKS beziehungsweise @rtus registriert.[99]

3.1 Kategorien sensibler Daten zu „rassischer oder ethnischer Herkunft“

Seit jeher steht das polizeiliche Informationswesen vor der Herausforderung, den wachsenden Datenbestand recherchierbar zu halten. Bereits Ende des 19. Jahrhunderts wurden daher Klassifizierungssysteme entwickelt, um die Wiedererkennung von Verdächtigen zu ermöglichen und die gesammelten Informationen besser nutzbar zu machen.[100] In den 1920er-Jahren führte dies in Deutschland zur reichsweiten Vereinheitlichung, Normierung und Standardisierung des Fahndungswesens. Mit dem Wiederaufbau der (west-)deutschen Polizei nach dem Zweiten Weltkrieg wurde bald an diese Tradition angeknüpft.[101] Als in den 1960er-Jahren die Überlegungen zur Computerisierung des Informationswesens in der Polizei begannen, verschärfte sich die Herausforderung der Standardisierung mit der Frage, wie „weiche“ in „harte“, computerlesbare Daten umgewandelt werden könnten. Karl Reuter, ehemaliger Ministerialrat im Bundesinnenministerium, brachte das Problem auf den Punkt, als er 1965 schrieb: „Ein denkender Sachbearbeiter kann – um es an einem simplen Beispiel zu abstrahieren – bei einem gesuchten ‚schlanken‘ Täter vielleicht auf den Gedanken kommen, daß er mit einem bekannten ‚schmächtigen‘ Täter identisch ist. Eine solche Übereinstimmung kann und darf eine Datenverarbeitungsmaschine nicht feststellen. Die deutsche Sprache ist – gottlob – so reich, daß es möglich ist, die gleiche Person oder den gleichen Vorgang zutreffend mit ganz unterschiedlichen Worten und Begriffen zu umschreiben. Dieser Sprachreichtum kann in der elektronischen Datenverarbeitung zu einer Sprachverwirrung führen, wenn man nicht vorher eine Sprachbereinigung vornimmt: die Einführung einer maschinengerechten Sprache mit möglichst ‚fixen‘ Begriffen.“[102]

Seitdem wird an einer bundesweit einheitlichen Struktur gearbeitet, um den elektronischen Austausch und die Vergleichbarkeit von Datensätzen zwischen den deutschen Polizeien zu gewährleisten. Diese betrifft sowohl die Arten beziehungsweise Kategorien der zu erfassenden Daten als auch die Frage, ob die Datenfelder mit Zahlen, Lichtbildern, gescannten Dokumenten, mit Freitext oder aus Listen mit standardisierten Werten („Katalogen“) gefüllt werden. Gesetzlich vorgegeben sind dabei lediglich grobe Rahmenbedingungen. Grundsätze über die Art der Daten, die in Verbunddateien des polizeilichen Informationssystem INPOL gespeichert werden, regelt aktuell (noch) die BKA-Datenverordnung (BKADV) vom 4. Juni 2010[103] sowie Kataloge, die in polizeilichen Bund-Länder-Gremien abgestimmt werden. Nachdem lange nur interne Anordnungen zur Errichtung der Dateien maßgeblich waren, sollte die BKADV Rechtssicherheit für das Führen polizeilicher Dateien beim BKA einschließlich der zu INPOL gehörenden Verbunddateien schaffen.[104] Aufgrund der Anbindung der Länderpolizeien an die Verbunddateien ergeben sich aus der BKADV auch verbindliche Vorgaben für die dortige Datenverarbeitung.

Die BKADV definiert 21 Arten von Personen- beziehungsweise Grunddaten, acht weitere zur Identifizierung geeignete Merkmale sowie 26 weitere Arten von personenbezogenen Daten, die in BKA- oder INPOL-Dateien zu Beschuldigten, Tatverdächtigen und teilweise auch anderen Personen gespeichert und weiterverarbeitet werden können.

99 Antworten des Innenministeriums Schleswig-Holstein und der Berliner Innensenatorin auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).
100 Heinrich (2007), S. 126 ff.
101 Ebd., S. 145 ff.
102 Reuter (1965), S. 266.
103 Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen. Obwohl die BKADV sich noch auf das alte BKA-Gesetz bezieht, gilt sie übergangsweise fort. Siehe: Graulich (2019), Rn. 4.
104 Bundesrat (28.05.2010), S. 1.

Die Verordnung legt nahe, dass Daten, die eine unmittelbare oder mittelbare Zuschreibung „rassischer oder ethnischer Herkunft“ (vgl. Kasten S. 15) erlauben, in erheblichem Ausmaß durch die deutsche Polizei verarbeitet werden. So kann das BKA als Zentralstelle in Dateien des Polizeilichen Informationssystems INPOL neben Grundpersonalien wie Namen, Staatsangehörigkeit oder Geburtsort unter anderem die „Volkszugehörigkeit“ (§ 1 Abs. 1 Nr. 17 BKADV), die „äußere Erscheinung“ (§ 1 Abs. 2 Nr. 2e BKADV), „verwendete Sprachen“ (§ 1 Abs. 2 Nr. 4 BKADV) oder eine „Mundart“ (§ 1 Abs. 2 Nr. 5 BKADV) von Beschuldigten, Tatverdächtigen und Anlasspersonen speichern.[105] Soweit im Einzelfall zur Terrorismusbekämpfung erforderlich, kann auch die „Religionszugehörigkeit“ erfasst werden (§ 2 Abs. 1 Nr. 17 BKADV). Dokumentiert ist die Existenz entsprechender Datenfelder in diversen Datei-Errichtungsanordnungen des BKA. Dies gilt sowohl für Dateien, die etwa im Bereich des polizeilichen Staatsschutzes nur einem sehr begrenzten Nutzer*innenkreis zugänglich sind und wenige tausend Einträge haben,[106] als auch für große, bundesweit genutzte Datenbanken wie die INPOL-Verbunddatei „Erkennungsdienst“ mit rund zehn Millionen Einträgen.[107] Für die Antiterrordatei sind Datenfelder für die Erfassung von „Volkszugehörigkeit“, „Sprachen“ und „Dialekten“ sogar gesetzlich normiert.[108]

Am Beispiel der Datenkategorien „Volkszugehörigkeit“ und „äußere Erscheinung“ beziehungsweise „Phänotyp“ soll im Folgenden detaillierter gezeigt werden, wie und aus welchen Anlässen sensible Daten durch die Polizei gespeichert werden können.

3.1.1 Volkszugehörigkeit

Laut Begründung der BKA-Datenverordnung dient die Datenkategorie „Volkszugehörigkeit“ der Eingrenzung der möglichen Herkunft oder Nationalität einer Person: Da „die willkürliche Ziehung von Staatsgrenzen mancher Länder […] Völker in ihrer gewachsenen Struktur auseinandergerissen oder aber zum Miteinander mit anderen Völkern gezwungen“ habe, sei die Zugehörigkeit „zu einem bestimmten Volk oder Stamm“ aussagekräftiger als die Kenntnis über den Geburtsstaat, etwa bei „Kosovo-Albanern“. In Zweifelsfällen würde die Kenntnis der „Volkszugehörigkeit“ insbesondere bei fehlenden Informationen über einen Geburtsort eine bessere geografische Eingrenzung von polizeilichen Ermittlungen und die Beschaffung weiterführender Informationen über eine Person erlauben.[109]

In Berlin erläuterte die Innensenatsverwaltung, nach der polizeilichen Nutzung der Kategorie „Volkszugehörigkeit“ befragt, im Herbst 2014, dass die Angabe der Ergänzung der Staatsangehörigkeit diene und, so wie die Merkmale Alter oder Geschlecht, eine „ermittlungs- und fahndungsunterstützende Information“ darstelle. Sie könne aber auch bedeutsam werden, um Zugang zu Personen zu bekommen und interkulturell kompetent mit ihnen umzugehen, etwa damit vermieden wird, dass in Vernehmungssituationen ein Dolmetscher in der Amtssprache des Herkunftslandes hinzugezogen wird, obwohl ein Betroffener sich als Angehöriger einer sprachlich unterdrückten Minderheit versteht.[110] Ebenfalls 2014 erklärte das Bundesinnenministerium, dass die Erfassung der Volkszugehörigkeit nicht obligatorisch sei, sondern es im Ermessen der polizeilichen Sachbearbeiter*innen liege, ob die „Zugehörigkeit zu einer bestimmten Ethnie ein tatauslösendes oder zumindest in der Kontexterfassung relevantes Moment darstellt (zum Beispiel bei türkisch-kurdischen Auseinandersetzungen)“.[111]

Der durch die AG Kripo[112] abgestimmte Katalog für die Erfassung im Datenfeld „Volkszugehörigkeit“

105 Bei Zeug*innen, Opfern, Hinweisgeber*innen oder sonstigen Auskunftspersonen können nach § 3 BKADV nur Grundpersonalien gespeichert werden.

106 Bundeskriminalamt (2007): Errichtungsanordnung der Amtsdatei „IntTE-S (Internationaler Terrorismus – Strafverfahren)“. Wiesbaden.

107 Bundeskriminalamt (2006): Errichtungsanordnung der Verbunddatei „Erkennungsdienst“. Wiesbaden.

108 Vgl. § 3 Abs. 1 ATDG. Anders die Rechtsextremismusdatei, in der nach § 3 RED-G zwar „Sprachkenntnisse“ in den erweiterten Grunddaten erfasst werden können, nicht jedoch Muttersprachen, Dialekte oder eine „Volkszugehörigkeit“.

109 Bundesrat (28.05.2010), S. 19.

110 Abgeordnetenhaus Berlin (13.10.2014), S. 1.

111 Bundesministerium des Innern (2014), S. 33.

112 Die AG Kripo ist die Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (BKA), deren Leitung beim Präsidenten des BKA liegt. Das Gremium ist dem Arbeitskreis II der Innenministerkonferenz nachgeordnet.

umfasste im Jahr 2020 mehr als 100 Katalogwerte: von A wie Abchase bis W wie Weißrusse. Enthalten war aber auch der Wert „deutsch“ sowie Werte für alle 16 deutschen Bundesländer, offensichtlich um regionale Differenzierungen vornehmen zu können. In Berlin räumte der Senat ein, dass der Katalog zum Teil „historisch überholte und unpräzise Begrifflichkeiten [enthält], welche auf historisch überholte Bestände zurückgehen, die durch nicht verjährende und somit keiner Löschfrist unterliegende Delikte entstanden sind“.[113] Demnach hat sich das zuständige Gremium der AG Kripo inzwischen darauf verständigt, sowohl Katalogwerte zu mehr oder weniger großen geografischen Regionen wie „Afrika“ oder „Baltikum“ als auch die deutschen Bundesländer oder historische Begriffe wie „Pommern (polnisch verwaltet)“ zu bereinigen und als dauerhafte Katalogwerte ausschließlich Zuschreibungen für ethnische beziehungsweise nationale Minderheiten zu verwenden.[114] Deutlich wird in jedem Fall, dass die Katalogwerte zu „Volkszugehörigkeit“ – trotz einiger erratischer Katalogwerte – unmittelbar der Erfassung ethnischer Zuschreibungen dienen.

Die Erfassung der „Volkszugehörigkeit“ war und ist eines der zentralen Konfliktfelder, wenn es um die polizeiliche Erfassung sensibler Daten geht. Vor dem Hintergrund der systematischen Registrierung und Stigmatisierung durch „~~Zigeuner~~“[115]- beziehungsweise „Landfahrer“-Karteien, Fahndungsblätter und INPOL-Hinweise, die Ende des 19. Jahrhunderts ihren Anfang nahm und mindestens bis in die 1980er-Jahre andauerte, kämpft die Bürgerrechtsbewegung der Sinti und Roma bis heute gegen Praktiken der ethnischen Sondererfassung.[116]

Dabei gab es im Laufe der Jahre immer wieder semantische Verschiebungen, die es erlaubten, tradierte Erfassungsmethoden mit neuen Begriffen fortzuführen: aus „~~Zigeuner~~“ wurde „Landfahrer“, aus „Landfahrer“ wurden „mobile ethnische Minderheit“ oder „häufig wechselnder Aufenthaltsort“.[117] Der personengebundene Hinweis „häufig wechselnder Aufenthaltsort“ (PHW HWAO) wurde erst 1989 aus dem bundesweiten INPOL-Katalog gestrichen.[118] Es ist unklar, ob oder in welchem Ausmaß durch die Nutzung von Stellvertreterbegriffen – aktuell etwa Hinweisen wie „Reisende Täter“ oder „Clan“ – die informationelle Stigmatisierung unter neuem Namen fortgeführt wird.

Vor dem Hintergrund der Proteste gegen die stigmatisierenden Benennungspraktiken forderte der Deutsche Bundestag 1986 die Bundesregierung einstimmig dazu auf, „sicherzustellen, daß Sondererfassungen der Sinti und Roma bei polizeilichen Informationssystemen und anderen Dateien ausgeschlossen werden“.[119] Initiativen folgten auch auf Länderebene. So veröffentlichte zum Beispiel das brandenburgische Innenministerium 1993 einen Erlass, der die Polizeibediensteten darauf hinwies, dass „Angaben über die Volkszugehörigkeit von Personen, die einer Straftat verdächtig sind, Diskriminierungen darstellen können, die Vorurteile verstärken und wecken“ und darum bat (sic!), zum Beispiel die „Bezeichnung von tatverdächtigen Sinti oder Roma als Zigeuner beziehungsweise den Hinweis bei solchen Tatverdächtigen auf ihre Zugehörigkeit zu den Sinti oder Roma zu unterlassen“; dies betraf – mit Ausnahme der „Pflicht, Anzeigen und Vernehmungen authentisch zu protokollieren“ – sowohl den internen Gebrauch als auch die Kommunikation nach außen.[120]

2007 führte eine Initiative des Zentralrats Deutscher Sinti und Roma dazu, dass die Innenministerkonferenz (IMK) auf ihrer Frühjahrstagung ihren Arbeitskreis II (AK II) damit beauftragte, die Erlasse zum Thema zu überprüfen und gegebenenfalls ergänzen zu lassen. Die Sichtung durch die Projektgruppe

113 Abgeordnetenhaus Berlin (13.10.2014), S. 1.

114 Abgeordnetenhaus Berlin (28.01.2020), S. 4–7. Aus der Antwort geht nicht eindeutig hervor, ob die Bereinigung bundesweit erfolgte oder nur für Berlin vollzogen wurde.

115 Nach dem Vorbild der Unabhängigen Kommission Antiziganismus wird der diskriminierende Begriff hier durchgestrichen, damit die historischen und semantischen Zuschreibungen sichtbar bleiben, ihre Geltung jedoch verneint wird. Siehe: Unabhängige Kommission Antiziganismus (2021), S. 10.

116 Rose (2000); Reuss (2023).

117 Details zur Erfassungspraxis bei Feuerhelm (1987); Stephan (2011); End (2019).

118 Stephan (2011), S. 273. In einigen Bundesländern führten die Polizeien den PHW HWAO allerdings weiter. Vgl. Töpfer (2020), S. 36 f.

119 Deutscher Bundestag (25.06.1986), S. 3.

120 Ministerium des Innern des Landes Brandenburg (19.08.1993).

des AK II ergab ein breites Spektrum, das vom völligen Fehlen einer individuellen Vorschrift zum Minderheitenschutz in damals fünf Ländern (Bremen, Hamburg, Nordrhein-Westfalen, Sachsen-Anhalt und Thüringen) sowie beim BKA bis zu Erlassregelungen mit ausformulierten Vorgaben reichte. In Brandenburg, Baden-Württemberg, Bayern und Rheinland-Pfalz existierten demnach Vorschriften, welche die Polizeibeamt*innen dazu aufforderten, weder polizeiintern noch extern die ethnische Zugehörigkeit oder vergleichbare Bezeichnungen zu verwenden.[121] Andere Bundesländer (Berlin, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Sachsen und Schleswig-Holstein, Sachsen) regelten die Verwendung entsprechender Bezeichnungen lediglich für die externe Kommunikation, damit in öffentlichen Fahndungsaufrufen oder Pressemitteilungen nicht auf die Zugehörigkeit zu einer ethnischen oder religiösen Minderheit oder die Hautfarbe eines Beschuldigten oder Tatverdächtigten hingewiesen wird. Als Mindeststandard für den „Schutz nationaler Minderheiten vor Verwendung diskriminierender Minderheitenkennzeichnungen durch Polizeibehörden“ erarbeitete die Projektgruppe des AK II folgende Musterregelung:

„Die Polizei bedient sich keiner Stigmatisierungen, Kategorisierungen oder pauschalen Bezeichnungen von Menschen. Gleiches gilt für Ersatzbezeichnungen oder Begriffe, unabhängig davon, ob sie tatsächlich oder subjektiv geeignet sind, einen Menschen, eine Ethnie, eine Volkszugehörigkeit oder eine Minderheit zu diskriminieren, zu stigmatisieren oder abzuqualifizieren. Auf die Zugehörigkeit zu einer Minderheit darf in der internen und externen Berichterstattung nur hingewiesen werden, wenn sie für das Verständnis eines Sachverhaltes oder für die Herstellung eines sachlichen Bezuges zwingend erforderlich ist. Die Polizei verwendet im internen wie im externen Gebrauch anstelle von Kategorien differenzierte und detaillierte Darstellungen, insbesondere im Zusammenhang mit der Fahndung, der Personenbeschreibung oder der Schilderung eines Tatherganges. Form und Inhalt des polizeilichen Sprachgebrauchs im Innen- und Außenverhältnis sind so zu halten, dass sie nicht diskriminieren oder Vorurteile schüren. Die Polizei berücksichtigt, dass sie im internen wie im externen Gebrauch jede Begrifflichkeit vermeiden muss, die von Dritten zur Abwertung von Menschen missbraucht beziehungsweise umfunktioniert oder in deren Sinne interpretiert werden kann. Dem muss auch im internen Bereich Rechnung getragen werden, da interne Dokumentationen nach außen dringen und dort Wirkung entfalten können. Die Verpflichtung zu einer authentischen oder wortgetreuen Dokumentation von Angaben bei Anzeigen, Vernehmungen oder Berichten bleibt hiervon unberührt.“[122] Auf ihrer Herbstsitzung 2007 nahm die IMK den Abschlussbericht der Projektgruppe samt Musterregelung zur Kenntnis,[123] und in der Folge wurden etwa in Nordrhein-Westfalen (2008) und Brandenburg (2014) Erlasse nach dem Vorbild der Musterregelung verabschiedet oder neugefasst.[124] Somit hat sich in den letzten zwanzig Jahren zwar die Sensibilität für den Umgang mit der Kategorie „Volkszugehörigkeit“ insbesondere mit Blick auf anerkannte nationale Minderheiten wie Sinti*zze und Rom*nja erhöht,[125] gleichwohl bleibt die Kategorie als solche in der polizeilichen Datenverarbeitung präsent (siehe Kapitel 3.2).

121 Für Baden-Württemberg wurde allerdings notiert, dass zur Vermeidung von Nachteilen bei der polizeilichen Aufgabenerfüllung und Gewährleistung der fachlich notwendigen Bezeichnung spezifischer Tätergruppen erforderlichenfalls Begriffe wie „mobile Straftäter“ (bedarfsweise auch mit Verweis auf die regionale Herkunft oder Nationalität) verwendet werden dürften, wenn diese Beschreibungen in neutraler Form bestimmte Tat- oder Tätermerkmale oder Charakteristika weitergeben oder den Modus Operandi beschreiben würden. Dabei müsse dann beachtet werden, dass diese Bezeichnungen nicht synonym für bestimmte Gruppierungen genutzt würden, also eine neue Ersatzbezeichnung generierten, sondern tatsächlich individuelle Tat- und Tätermerkmale wiedergäben.

122 Projektgruppe des AK II (10.10.2007), S. 6.

123 Innenministerkonferenz (10.12.2007), Beschluss zu TOP 11, S. 15.

124 Ministerium des Innern des Landes Nordrhein-Westfalen (15.12.2008); Ministerium des Innern des Landes Brandenburg (10.09.2014).

125 Unter den mehr als 100 Katalogwerten des besagten INPOL-Katalogs „Volkszugehörigkeit“ findet sich keine der vier in Deutschland anerkannten nationalen Minderheiten, sodass zumindest eine standardisierte Erfassung nicht möglich ist. Siehe: Abgeordnetenhaus Berlin (28.01.2020), S. 4–7. Die Nennung von „Sinti und Roma“ in Freitextfeldern oder auch der Polizeilichen Kriminalstatistik eines Landes wurden aber auch nach 2007 verschiedentlich bekannt und von Datenschutzaufsichtsbehörden beanstandet. Siehe etwa: Berliner Beauftragte für Datenschutz und Informationsfreiheit (2021), S. 76 ff.

3.1.2 Äußere Erscheinung/„Phänotyp“

Das Datenfeld „äußere Erscheinung“ dient zusammen mit anderen Merkmalen wie Gewicht oder Schuhgröße der Personenbeschreibung. Angaben über die „äußere Erscheinung“ werden üblicherweise ihm Rahmen von erkennungsdienstlichen Maßnahmen oder für unbekannte gesuchte Personen, zum Beispiel aufgrund von Zeug*innenaussagen, erfasst. Das Datenfeld wird synonym für den Begriff „Phänotyp“ genutzt. Laut Begründung der BKA-Datenverordnung können entsprechende Angaben als Ausschlusskriterium oder Indiz für die Täterschaft bestimmter Personen dienen.[126] Genutzt wird es beispielsweise bei Fahndungen oder für das gezielte Filtern von erkennungsdienstlichen Dateien, etwa wenn Zeug*innen anhand umfangreicher Lichtbildsammlungen Tatverdächtige identifizieren sollen.

Für die „äußere Erscheinung“ beziehungsweise den „Phänotyp“ existiert ein standardisierter Katalog, der zuletzt im Jahr 2003 geändert wurde. Demnach können polizeiliche Sachbearbeiter*innen aus einer Liste mit 19 Katalogwerten auswählen.[127]

Bereits Mitte der 1990er-Jahre hatte es Kritik an „rassistischen Typisierungen“ gegeben, die polizeilichen Sachbearbeiter*innen für die computergerechte, standardisierte Personenbeschreibung im sogenannten Erfassungsbeleg KP8 zur Verfügung standen. Die Bundesregierung verteidigte die Typisierung damals als unverzichtbar und verwies auf langjährige polizeiliche „Erfahrungspraxis“. Weiter argumentierte sie, dass ein geeigneter Schutz der Daten dadurch gewährleistet sei, dass die Daten nur dem internen Polizeigebrauch dienten, es sich lediglich um Zusatzangaben handle und es keine Dateien über die genannten Merkmale gebe.[128] Letztlich aber bewirkten die Diskussionen eine Überarbeitung des Erfassungsbelegs KP8, bei der etwa Begriffe wie „südländisch“ oder „slawisch“ gestrichen wurden.

Tabelle 1: INPOL-Katalogwerte für die Kategorie „Phänotyp“

afrikanisch
nordafrikanisch
nordostafrikanisch
zentral-/südafrikanisch
afro-amerikanisch
indianisch
mittel-/südamerikanisch
nordamerikanisch
asiatisch
ostasiatisch
südasiatisch
südostasiatisch
westasiatisch
zentralasiatisch
europäisch
osteuropäisch
südeuropäisch
südosteuropäisch
westeuropäisch

Gleichwohl zeigen die aktuellen INPOL-Katalogwerte für die Kategorie „Phänotyp“, dass bis heute an einer Form der standardisierten Erfassung festgehalten wird, die sich zumeist an der unterstellten (geografischen) Herkunft von Personen orientiert. Dabei wird deutlich, dass dem Katalog die rassifizierende Annahme zugrunde liegt, dass es in geografischen Regionen angestammte autochthone Gruppen mit spezifischen Physiognomien gibt. So hieß es auf eine Anfrage zur

126 Bundesrat (28.05.2010), S. 21 f.
127 Abgeordnetenhaus Berlin (28.01.2020), S. 8.
128 Siehe etwa: Deutscher Bundestag (19.12.1996).

Erfassungsmethodik der Erfassung in Berlin, dass die Zuordnung zum Katalogwert „Phänotyp“ grundsätzlich auf Grundlage der Staatsangehörigkeit erfolge, bei offensichtlichen Diskrepanzen zwischen der Staatsangehörigkeit und dem Erscheinungsbild jedoch die Möglichkeit bestehe, einen anderen Katalogwert auszuwählen.[129] Damit ist die Datenerfassung auf die Reproduktion von Stereotypen angelegt: Wer nicht der polizeilichen Vorstellung eines „Westeuropäers“ entspricht, wird auch nicht als solcher erfasst, selbst wenn seine Staatsangehörigkeit ihn als solchen ausweist.

Der Katalog ist auch in der Polizei nicht unumstritten. So hat etwa die Polizei in Berlin nach Angaben des Senats inzwischen entschieden, die Kategorie „indianisch“ nicht länger zu nutzen.[130] Eine grundlegende Änderung ist jedoch nicht in Sicht, sodass die rassifizierende Typisierung weiterhin alltäglich sichtbar in der Polizeiarbeit tradiert werden wird. Und dies, obwohl die Polizei auch zahlreiche andere körperliche Merkmale wie Haut- und Haarfarbe oder die Form von Ohren und Mund erfasst und die Erforderlichkeit einer Datenkategorie „Phänotyp“ somit fragwürdig ist.[131]

3.2 Datenspeicherung

In welchem Umfang die besonderen Kategorien personenbezogener Daten durch die Polizei verarbeitet werden und welche Relevanz sie für die Praxis haben, lässt sich angesichts der Komplexität und Intransparenz der polizeilichen Datenverarbeitung nur punktuell bestimmen. Für diesen Zwecke hat das Deutsche Institut für Menschenrechte die Innenministerien der Bundesländer um Auskunft zum Bestand ausgewählter Datenkategorien[132] in den polizeilichen Vorgangsbearbeitungssystemen gebeten. Dabei wurde lediglich auf die Vorgangsbearbeitungssysteme als das Rückgrat der polizeilichen Datenverarbeitung (siehe Glossar, S. 26 f.) fokussiert, um den Bearbeitungsaufwand für die Innenministerien in Grenzen zu halten.

Rückmeldung mit Statistiken zur Datenhaltung in den Vorgangsbearbeitungssystemen gab es aus den neun Ländern Berlin, Bremen, Niedersachsen, Nordrhein-Westfalen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen und Sachsen-Anhalt.[133] Aus den anderen Ländern hieß es, dass wegen Mehrfacherfassungen von Personen keine aussagekräftigen Aussagen möglich wären oder der Aufwand der Auswertung zu hoch sei.

Der berichtete Bestand in den Vorgangsbearbeitungssystemen liegt zwischen zwei Millionen in Bremen und knapp 30 Millionen Personendatensätzen in Nordrhein-Westfalen. Oft handelt es sich dabei um Mehrfacherfassungen, weil ein und dieselbe Person im Zusammenhang mit unterschiedlichen Vorgängen registriert wurde, sodass nicht für jedes Land klar ist, wie hoch die tatsächliche Anzahl Betroffener ist, und ein Vergleich absoluter Zahlen irreführend sein kann.

Deutlich wird aber, dass es zwischen den Ländern deutliche Unterschiede in der Datenerfassung gibt: Wenig überraschend rangieren Grunddaten zu Personen wie Namen und Geburtsort in den Statistiken aller Vorgangsbearbeitungssysteme weit oben. Sie sind für die große Mehrheit der erfassten Personen hinterlegt. Meist gilt dies auch für die Staatsangehörigkeit, die allerdings in Rheinland-Pfalz nur für jede zweite und im Saarland nur für jede dritte Person registriert ist.

Da in den Vorgangsbearbeitungssystemen zahlreiche Menschen nur als Geschädigte oder Zeug*innen geführt werden, ohne erkennungsdienstlich erfasst worden zu sein, spielen dort Informationen zur Personenbeschreibung eine nachgeordnete Rolle. In Niedersachsen, Rheinland-Pfalz und Sachsen-

129 Abgeordnetenhaus Berlin (09.06.2023), S. 3.

130 Abgeordnetenhaus Berlin (20.12.2023), S. 10.

131 Einen Eindruck vom Detailreichtum polizeilicher Personenbeschreibungen gibt der Auszug aus der 14-seitigen Personenabfrage zu dem in der Justizvollzugsanstalt Kleve verbrannten Amad A., der im Rahmen der Untersuchung des Falls durch den nordrhein-westfälischen Landtag öffentlich wurde. Landtag Nordrhein-Westfalen (05.04.2022), S. 241 ff.

132 Gefragt wurde nach den Kategorien Vor- und Nachname, Staatsangehörigkeit, Geburtsort und -land, Volks- und Religionszugehörigkeit, „Phänotypus“, Sprache, Stimm-/Sprachmerkmale, Mundart und Personengebundene/Ermittlungsunterstützende Hinweise.

133 Antwort der Innenministerien und -senator*innen der Länder auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).

Anhalt ist eine Speicherung der Kategorien „Volkszugehörigkeit“ in den Vorgangsbearbeitungssystemen nicht vorgesehen. Das Gleiche gilt in diesen Ländern sowie im Saarland für „Religionszugehörigkeit“. Dort, wo diese Kategorien gespeichert werden können, sind sie nur bei weniger als einem Prozent der registrierten Personen hinterlegt.[134] Aus dem Saarland wurde berichtet, dass es sich bei den Angaben zur „Volkszugehörigkeit“ hauptsächlich um Angaben zu den Bundesländern handelt, aus denen die Personen kommen, und die Nennung „Saarland“ mit Abstand überwiegt. Informationen dazu liegen für andere Länder nicht vor. Die Kategorie „Phänotyp“ kann in allen Vorgangsbearbeitungssystemen erfasst werden, was auch etwas häufiger passiert als für die Kategorie „Volkszugehörigkeit“ und in Niedersachsen und Nordrhein-Westfalen mehr als zwei Prozent der Personendatensätze betrifft – am häufigsten finden sich dort die Zuschreibungen „europäisch“ und „westeuropäisch“. In den anderen Ländern liegt die Quote nur im Promillebereich. Ähnlich stellt sich die Situation für die Kategorien „Sprache“ und „Mundart“ dar.

In der polizeilichen Vorgangsbearbeitung dominieren unter den abgefragten Kategorien Grunddaten wie Namen, Geburtsort und – wenngleich mit deutlichen Unterschieden – Staatsangehörigkeit. Im Vergleich dazu spielen Kategorien wie „Phänotyp“ und „Sprache“ und – manchmal – auch „Volkszugehörigkeit“ nur eine nachgeordnete Rolle. In absoluten Zahlen geht es dabei allerdings in großen Bundesländern zahlenmäßig um Größenordnungen im fünf- bis sechsstelligen Bereich. So wurde aus Nordrhein-Westfalen berichtet, dass dort etwa 72.000 Personendatensätzen eine „Volkszugehörigkeit“ zugeschrieben ist und 600.000 Personendatensätzen ein „Phänotyp“.

Mit ihrem Fokus auf die Vorgangsbearbeitungssysteme blendet die Bestandsaufnahme notgedrungen andere Datenbestände aus. Einen kleinen Einblick eröffnen die Informationen zur Nutzung der Antiterrordatei (ATD), einer Datei, die als Verbunddatei bundesweit vom polizeilichen Staatsschutz (und den Nachrichtendiensten) genutzt wird. Im Folgenden wird auf Grundlage der ATD-Evaluation von 2011 und regelmäßiger Berichte, die das BKA seit 2013 veröffentlicht, die Befüllung der Datenfelder zu „Volkszugehörigkeit“ und „Religionszugehörigkeit“ dargestellt.

Tabelle 2: Befüllung ausgewählter Datenfelder in der Antiterrordatei[135]

Belegung in %	2007	2008	2009	2010	2011	2014	2015	2016	2017	2018	2019	2020
Volkszugehörigkeit	1	4	4	4	4	8,7	8,7	12,4	12,6	10,4	14,3	30,2
Religionszugehörigkeit	5	7	7	7	7	21,7	25,9	22,2	21,1	35,2	43,3	29,5

2020 waren in der Antiterrordatei rund 10.000 Personen erfasst. Die Tabelle 2 zeigt, dass dabei inzwischen in erheblichem Umfang sensible Daten verarbeitet werden. Die Befüllung des Datenfeldes „Volkszugehörigkeit“ ist von 2007 bis 2020 deutlich angestiegen. Nach der Inbetriebnahme der Datei im Jahr 2007 waren entsprechende Angaben nur in jedem hundertsten Personendatensatz hinterlegt. Der niedrige Stand korrespondierte mit der Aussage von ATD-Nutzer*innen, die bei der

134 Für Sachsen lassen sich die für die Kategorie „Volkszugehörigkeit“ berichteten Zahlen nicht vergleichen, weil sie sich auf ein Datenfeld „Ergänzung zu Staatsangehörigkeit/Geburtsland/Volkszugehörigkeit“ beziehen.

135 Deutscher Bundestag (07.03.2013), S. 38; Bundeskriminalamt (2017), S. 14 ff.; Bundeskriminalamt (2020), S. 9 ff.

Evaluierung von 2011 zu Protokoll gegeben hatten, dass das Datum „Volkszugehörigkeit“ nur eine marginale Bedeutung für die Ermittlungsarbeit habe.[136] 2020 war das Datenfeld „Volkszugehörigkeit“ in jedem dritten Personendatensatz befüllt. Die Zahlen für „Religionszugehörigkeit“ sind seit 2007 von fünf Prozent auf 43 Prozent im Jahr 2019 gestiegen, bevor sie 2020 auf knapp 30 Prozent sanken. Aufgrund der begrenzten Verfügbarkeit von Informationen konnte dieses Kapitel nur Schlaglichter werfen auf die polizeiliche Speicherung sensibler Daten zu vermeintlicher „rassischer oder ethnischer Herkunft“. Es ließ sich zeigen, dass Datenkategorien wie „Volkszugehörigkeit“ oder „Phänotyp“ gemessen am Gesamtvolumen der polizeilichen Datenspeicherung nur eine nachgeordnete Rolle spielen. In absoluten Zahlen ist das Ausmaß jedoch auch in der Vorgangsbearbeitung in der Summe erheblich, wobei es deutliche Unterschiede in der Praxis der Länderpolizeien gibt, über deren Gründe sich nur spekulieren lässt.

3.3 Nutzung gespeicherter Daten

Was passiert nun mit den sensiblen Daten, wenn sie einmal von der Polizei gespeichert wurden? Wie können sie weiter genutzt werden? Welche Diskriminierungsrisiken bestehen dabei? Und wie steht es um ihren besonderen Schutz? Diesen Fragen geht das folgende Kapitel nach, indem es kurz den allgemeinen rechtlichen Rahmen für die Nutzung von polizeilich gespeicherten Daten erläutert und diskutiert, welche Maßnahmen existieren, um den besonderen Schutz dieser Daten zu gewährleisten, und warum sie zu kurz greifen. Abschließend soll anhand einiger Beispiele gezeigt werden, welche Diskriminierungsrisiken sich daraus ergeben.

3.3.1 Einfachgesetzliche Voraussetzungen

Grundsätzlich kann die Polizei (sensible) Daten, die sie einmal rechtmäßig erhoben hat, speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben (unbedingt) erforderlich ist. Dies regeln die Generalklauseln zur Weiterverarbeitung von Daten, die sich in allen Polizeigesetzen in Bund und Ländern finden.[137] Dabei gilt der Grundsatz der Zweckbindung. Das heißt, die weitere Nutzung von Daten darf nur zu dem Zweck erfolgen, zu dem sie erhoben wurden. Möglich ist indes auch eine Nutzung der Daten zu einem anderen Zweck. Verfassungsrechtlich zulässig ist dies, wenn die Polizei die Daten auch zu diesem anderen Zweck erheben dürfte und mit der neuen Verarbeitung den Schutz ähnlich bedeutender Rechtsgüter oder die Aufdeckung ähnlich schwerwiegender Straftaten bezweckt wie mit der ursprünglichen Datenerhebung.[138] Entsprechend lassen Polizeigesetze und Strafprozessordnung ausdrücklich zu, dass Daten, die zur Strafverfolgung erhoben werden, auch für präventivpolizeiliche Zwecke weiterverarbeitet werden können und umgekehrt.[139] Während einige Länder eine neue Nutzung bereits erhobener Daten zu anderen Zwecken jedoch nur unter bestimmten Voraussetzungen erlauben, fehlt in den meisten Fällen eine solche Präzisierung der Zweckbindung.[140] Im Ergebnis wird die polizeiliche Weiterverarbeitung einmal erhobener Daten durch das Fachrecht im Detail wenig reguliert. Dies gilt auch für sensible Daten und insbesondere dann, wenn es sich dabei um Daten handelt, die massenhaft bei offenen Standardmaßnahmen wie erkennungsdienstlichen Maßnahmen oder der Protokollierung von Zeugenaussagen erhoben werden.

Präzisere Vorgaben zur Nutzung von polizeilichen Dateien, etwa zum Nutzungszweck oder dem Kreis der zugriffsberechtigten Personen, werden durch polizeiinterne Errichtungsanordnungen oder Verarbeitungsverzeichnisse festgelegt. Sie sind Voraussetzung für den rechtmäßigen Betrieb solcher Dateien. Während vor der Umsetzung der JI-Richtlinie ins nationale Recht die Datenschutzaufsichtsbehörden zu den Anordnungen und

136 Deutscher Bundestag (07.03.2013), S. 38.

137 Siehe etwa Art. 53 Bayerisches Polizeiaufgabengesetz, § 42 Allgemeines Sicherheit- und Ordnungsgesetz Berlin, § 23 Polizeigesetz Nordrhein-Westfalen oder § 29 Bundespolizeigesetz. Zulässig ist die Weiterverarbeitung regelmäßig auch zur Dokumentation und Verwaltung von polizeilichen Vorgängen, (kriminal)statistischen und einigen anderen Zwecken wie Aus- und Fortbildung oder Forschung.

138 Bundesverfassungsgericht (2016): Bundeskriminalamtsgesetz. Urteil vom 20.04.2016, 1 BvR 966/09, Rn. 284 ff. Bei Daten, die aus besonders eingriffsintensiven Überwachungsmaßnahmen, wie einer Online-Durchsuchung oder Wohnraumüberwachung stammen, verlangt das Bundesverfassungsgericht zudem, dass auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sind.

139 Kingreen / Poscher (2022): § 14, Rn. 14.

140 Ebd., Rn. 15.

Verzeichnissen vorab beratend konsultiert werden mussten, ist diese Pflicht seitdem entfallen.[141] Inzwischen müssen die Polizeibehörden den Aufsichtsbehörden die Errichtungsanordnungen oder Verarbeitungsverzeichnisse lediglich nachträglich zur Verfügung stellen.[142]

Neben den Generalklauseln zur Weiterverarbeitung von Daten existieren nur für wenige Formen der Nutzung und Auswertung ihrer eigenen Datenbestände durch die Polizei spezifische gesetzliche Eingriffsbefugnisse. Gesetzliche Vorgaben existieren für den Datenabgleich und die verfassungsrechtlich umstrittenen automatisierten Datenanalysen. Daneben erlaubt das Polizeirecht die Rasterfahndung, deren Besonderheit aber ist, dass die Polizei dabei auch Datenbestände Dritter nutzt, weshalb dies hier nicht weiter vertieft wird.

Bei einem Datenabgleich werden Daten von Personen, die etwa im Rahmen einer Personenkontrolle oder anderer polizeilicher Maßnahmen in den Fokus der Polizei geraten, mit bestehenden Datensammlungen abgeglichen.[143] Dabei geht es darum zu prüfen, ob und welche Informationen bereits über die Betroffenen vorliegen, ob sie etwa zur Fahndung ausgeschrieben sind oder ob bereits an anderer Stelle ein Ermittlungsverfahren geführt wurde. Die Hürden für den Datenabgleich sind jedoch kaum höher als für eine Datennutzung auf Grundlage der Generalklausel; zulässig ist regelmäßig ein Abgleich mit dem Fahndungsbestand oder wenn Tatsachen die Annahme rechtfertigen, dass der Datenabgleich für die polizeiliche Aufgabenerfüllung erforderlich ist.[144] Als besondere Form des Abgleichs mit polizeilichen Datenbeständen regeln einige wenige Polizeigesetze außerdem ausdrücklich die Erstellung von Lagebildern für Zwecke der Kriminalitätsbekämpfung.[145]

Der Einsatz automatisierter Analysemethoden wurde inzwischen in Hessen, Hamburg und Nordrhein-Westfalen gesetzlich zugelassen.[146] Bei solchen Datamining-Methoden soll eine Software im umfangreichen polizeilichen Datenbestand automatisiert Netzwerke und andere Zusammenhänge zwischen Personen, Organisationen, Sachen und anderen Objekten erkennen, irrelevante Informationen ausfiltern, Daten für digitale Karten aufbereiten oder sie statistisch auswerten. Das Bundesverfassungsgericht hat solchen Methoden aufgrund der hohen Streubreite und Intensität der damit verbundenen Grundrechtseingriffe in mittlerweile zwei Entscheidungen enge Grenzen gesetzt und die konkreten Regelungen in Hessen und Hamburg für verfassungswidrig erklärt.[147]

Zu beachten sind bei automatisierten Verfahren zudem Vorgaben, die sich aus der Umsetzung von Artikel 11 JI-Richtlinie ergeben. Demnach dürfen ausschließlich auf einer automatisierten Verarbeitung basierende Entscheidungen nicht auf sensiblen Daten beruhen, wenn keine geeigneten Maßnahmen zum Schutz der Betroffenen getroffen wurden. Ein automatisiertes Profiling[148], das zur Folge hat, dass eine Person aufgrund des Anknüpfens an sensible Daten diskriminiert wird, ist ausdrücklich verboten.

Die Masse der polizeilichen Nutzung sensibler Daten, bei denen noch Menschen in den Verarbeitungsprozess eingebunden sind, wird jedoch kaum anders gewertet als eine Weiterverarbeitung anderer Datenkategorien und unterliegt somit nur wenigen Beschränkungen durch das Polizeirecht.

141 Art. 24 JI-Richtlinie.

142 Siehe etwa Art. 64 Abs. 1 S. 2 Bayerisches Polizeiaufgabengesetz, § 80 Abs. 4 Bremisches Polizeigesetz oder § 80 Abs. 6 Bundeskriminalamtgesetz.

143 Mit Nachweisen der einschlägigen Normen siehe Kingreen / Poscher (2022), § 14, Rn. 42.

144 Siehe etwa: Art. 61 Bayerisches Polizeiaufgabengesetz, § 48 Bremisches Polizeigesetz, § 25 Polizeigesetz Nordrhein-Westfalen oder § 34 Bundespolizeigesetz. Für Zwecke der Strafverfolgung sind Datenabgleiche zudem nach § 98c Strafprozessordnung erlaubt.

145 Zum Beispiel: § 188 Abs. 6 Landesverwaltungsgesetz Schleswig-Holstein.

146 § 25a Hessisches Sicherheits- und Ordnungsgesetz, § 49 Hamburgisches Gesetz über die Datenverarbeitung der Polizei und § 23 Absatz 6 Polizeigesetz Nordrhein-Westfalen.

147 Bundesverfassungsgericht (2020): Antiterrordateigesetz II. Beschluss vom 10.11.2020, 1 BvR 3214/15; Bundesverfassungsgericht (2023): Automatisierte Datenanalyse. Urteil vom 16.02.2023, 1 BvR 1547/19 und 1 BvR 2634/20.

148 Als „Profiling“ definiert Art. 3 der JI-Richtlinie jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte zu bewerten und damit zum Beispiel die Interessen oder das Handeln einer Person zu analysieren oder vorherzusagen.

3.3.2 Schutzmaßnahmen

Nachdem gezeigt wurde, dass die Nutzung sensibler Daten durch die Polizei rechtlich wenig beschränkt ist und die gesetzlichen Vorgaben für Garantien zum Schutz Betroffener unverbindlich und unbestimmt sind, stellt sich die Frage, ob Maßnahmen vorgesehen sind, die dem erhöhten Schutzbedarf sensibler Daten Rechnung tragen.

Eine Antwort auf diese Frage ist nicht leicht, da die polizeiliche Datenverarbeitung aufgrund von Geheimschutz wenig transparent ist und viele interne Vorgaben nicht öffentlich zugänglich sind. Die Ergebnisse der Umfrage des Deutschen Instituts für Menschenrechte unter den Innenministerien der Länder legen jedoch nahe, dass sich das Schutzniveau für die polizeiliche Verarbeitung sensibler Daten kaum von jenem unterscheidet, das für die Verarbeitung nicht-sensibler Daten gilt: Zwar sollen technische Maßnahmen, Schulungen des Personals und Verfahrensregeln zur Übermittlung vor unbefugten Zugriffen schützen und etwa Prüffristen zur Aussonderung der Daten eine verhältnismäßige Datenverarbeitung sicherstellen. Mit Ausnahme der wenigen positiven Ansätze, die gesetzlich in Bayern, Bremen und Mecklenburg-Vorpommern vorgesehen sind (siehe S. 22 f.), sind jedoch kaum Unterschiede beim Schutzniveau ersichtlich. Das Innenministerium Sachsen-Anhalt[149] und die Berliner Senatsverwaltung für Inneres schreiben explizit, dass sensible Datenkategorien nicht gesondert behandelt werden, sondern die allgemeinen Regeln zur Datenverarbeitung gelten. Aus Berlin wird allerdings berichtet, dass es Pläne zur Überarbeitung einer Geschäftsanweisung gibt, die besonderen Bezug auf sensible Daten nehmen soll.[150] In Bremen soll es zukünftig eine Rechtsverordnung zur Konkretisierung der gesetzlich vorgesehenen verkürzten Aussonderungsprüfpflicht geben.[151]

Besondere Berücksichtigung finden sensible Daten demnach in der Regel nur im Kontext von Datenschutzfolgeabschätzungen. Nach Artikel 27 der JI-Richtlinie haben die EU-Mitgliedstaaten gesetzlich dafür zu sorgen, dass datenverarbeitende Stellen immer dann eine Datenschutzfolgenabschätzung durchführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. Entsprechende Regelungen finden sich in § 67 BDSG und dem Landesrecht. Die Folgenabschätzung soll eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge beinhalten sowie eine Bewertung der Risiken, der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren zum Datenschutz. Damit soll der Nachweis erbracht werden, dass die Vorgaben der Richtlinie eingehalten werden. Zur Klärung der Frage, ob überhaupt ein Risiko bei der Datenverarbeitung gesehen wird und die Notwendigkeit besteht, eine Datenschutzfolgeabschätzung zu erstellen, werden vorab sogenannte Schwellwertanalysen durchgeführt. Dabei findet, so zeigen etwa Dokumente der Polizei Hamburg, die geplante Verarbeitung sensibler Daten besondere Berücksichtigung, was eine anschließende Datenschutzfolgenabschätzung wahrscheinlich macht.

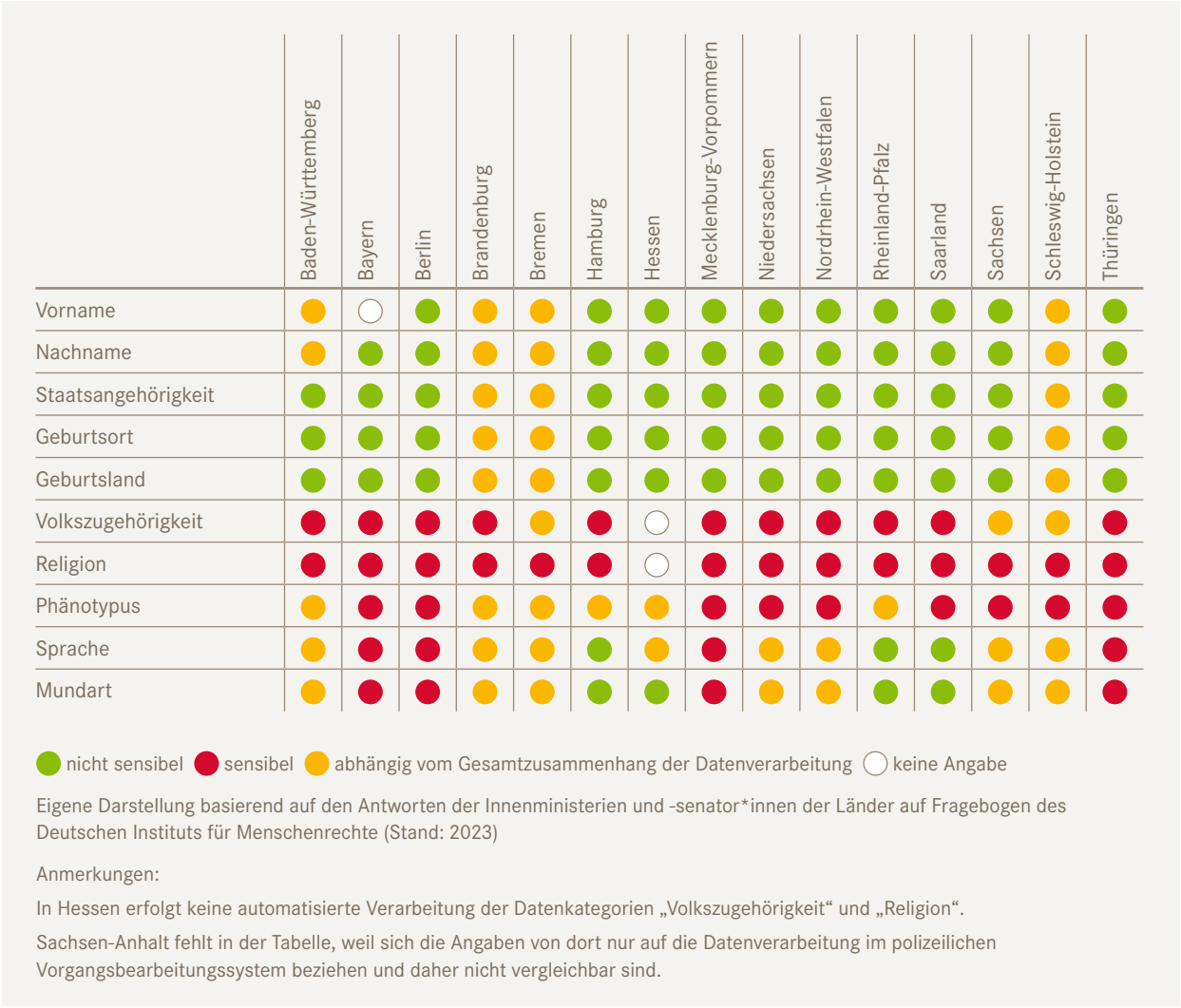
Allerdings bleibt das ganze Verfahren – von der Erstellung der Schwellwertanalyse bis zur Fertigstellung der Datenschutzfolgenabschätzung – ein rein interner Vorgang, bei dem höchstens behördliche Datenschutzbeauftragte zu beteiligen sind. Unabhängige Datenschutzaufsichtsbehörden sind, anders als im ersten Entwurf für die JI-Richtlinie ursprünglich vorgeschlagen, nur dann vorab zu konsultieren, wenn die Errichtung neuer Dateisysteme geplant ist, die als hochriskant gelten. Potenziell Betroffene bleiben, anders als bei Folgenabschätzungen nach der Datenschutzgrundverordnung, grundsätzlich außen vor. Die Entscheidung darüber, welche Formen der Datennutzung eigentlich als prüfungsbedürftige Verarbeitungsprozesse

149 Antwort des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).

150 Antwort der Berliner Senatsverwaltung für Inneres und Sport auf Antworten des Innenministeriums Schleswig-Holstein und der Berliner Innensenatorin auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).

151 Antwort des Senators für Inneres und Sport der Freien Hansestadt Bremen Antworten des Innenministeriums Schleswig-Holstein und der Berliner Innensenatorin auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).

Abbildung 3: Welche Datenkategorien behandeln Polizeien der Länder als sensible Daten?



Eigene Darstellung basierend auf den Antworten der Innenministerien und -senator*innen der Länder auf Fragebogen des Deutschen Instituts für Menschenrechte (Stand: 2023)

Anmerkungen:

In Hessen erfolgt keine automatisierte Verarbeitung der Datenkategorien „Volkszugehörigkeit“ und „Religion“.

Sachsen-Anhalt fehlt in der Tabelle, weil sich die Angaben von dort nur auf die Datenverarbeitung im polizeilichen Vorgangsbearbeitungssystem beziehen und daher nicht vergleichbar sind.

und welche Datenkategorien als sensibel gewertet werden, obliegt damit ausschließlich der Polizei.[152]

Dabei ist es keineswegs eindeutig, welche Datenkategorien aus polizeilicher Perspektive als sensible Daten im Sinne von Artikel 10 JI-Richtlinie gewertet werden. Die Antworten aus den Bundesländern auf den Fragenkatalog des Deutschen Instituts für Menschenrechte zu dieser Frage variieren erheblich, wie Abbildung 3 zeigt. Einigkeit herrscht nur hinsichtlich der Kategorie „Religionszugehörigkeit“, die in allen Bundesländern, die auf die Umfrage des Institutes geantwortet haben, als besonders schutzwürdiges sensibles Datum gilt.[153] Ganz überwiegend werten die Innenministerien auch die Kategorie „Volkszugehörigkeit“ als sensibles Datum; allerdings stufen Schleswig-Holstein und Sachsen „Volkszugehörigkeit“ nur in bestimmten Verarbeitungskontexten entsprechend ein, was eventuell damit zu tun hat, dass die verfügbaren Katalogwerte nicht in jedem Fall ethnischen Zuschreibungen entsprechen (siehe Kapitel 3.1.1). In der Mehrzahl wird auch äußere Erscheinung/„Phänotyp“ als sensible Datenkategorie gewertet. Allerdings nehmen vier Länder diese Wertung nur in bestimmten Verarbeitungskontexten vor. So wertet etwa die Polizei in Hamburg das Merkmal nur dann als sensibles Datum, wenn zum Beispiel aus der Kombination eines erfassten „Phänotypus“ mit weiteren Informationen eine „Ethnie“

152 Eine Ausnahme wurde vom Bundesdatenschutzbeauftragten für die Kontrolle von Bundeskriminalamt und Bundespolizei berichtet, wo weiterhin eine Beteiligung bei (wichtigen) Vorhaben stattfindet. Allerdings basiert diese Praxis auf informellen Absprachen beziehungsweise dem überholten Bundespolizeigesetz. E-Mail vom Bundesbeauftragten für Datenschutz und Informationsfreiheit vom 30.06.2023.

153 Ausnahme: Sachsen-Anhalt, wo eine differenzierte Bewertung mit Hinweis auf die einheitliche Behandlung der Datenkategorien nach den allgemeinen Datenverarbeitungsregeln im Vorgangsbearbeitungssystem nicht erfolgte.

bestimmbar sei. In Berlin und Bayern gelten auch „Sprache“, „Stimm- und Sprachmerkmale“ und „Mundarten“ grundsätzlich als besondere Datenkategorien; in der Mehrzahl der Länder wird dies nur in bestimmten Verarbeitungskontexten so gesehen; die Innenministerien aus Hamburg, Rheinland-Pfalz und dem Saarland verneinten eine solche Wertung grundsätzlich. Vor- oder Nachnamen, Angaben zur Staatsangehörigkeit, zu Geburtsorten oder -ländern wurden zwar überwiegend nicht als besondere Datenkategorien gewertet; in einigen wenigen Ländern wie Schleswig-Holstein gilt jedoch auch in diesen Fällen der Verarbeitungskontext als entscheidend.[154]

Somit ist es in hohem Maße kontextabhängig, welche Datenkategorien überhaupt als sensible Daten gelten und entsprechend im Zusammenhang mit polizeiinternen Risikoabschätzungen zum Tragen kommen.

3.3.3 Diskriminierungsrisiken – Fallbeispiele

Somit ist die Nutzung sensibler Daten in der polizeilichen Praxis bis auf wenige Ausnahmen kaum eingehegt. Vor diesem Hintergrund wird im Folgenden exemplarisch gezeigt, wie in der Polizeiarbeit an sensible Daten angeknüpft wird und welche Diskriminierungsrisiken sich daraus ergeben können.

Einsatzunterstützung durch Leitstellen

Welche Risiken sich aus der niedrigschwelligen Verfügbarkeit sensibler Daten auch im alltäglichen Streifendienst ergeben können, zeigt das Beispiel der Einsatzunterstützung durch die Leitstellen. Die Einsatzleitstellen spielen eine zentrale Rolle für die Arbeit der Schutzpolizei. Sie nehmen Notrufe an, bearbeiten stille Alarme, lenken über Funk polizeiliche Einsätze und erstellen tägliche Lagemeldungen. Bei den Leitstellen handelt es sich um hochtechnisierte Arbeitsplätze. Zur Registrierung, Vorbereitung und Unterstützung der Einsätze haben die Mitarbeiter*innen der Leitstellen Zugriff auf zahlreiche polizeiliche und nichtpolizeiliche Informationssysteme wie die Vorgangsbearbeitungs- und Fahndungssysteme, die Melderegister oder öffentlich zugängliche Internetquellen.[155]

Zur Arbeit der Beamt*innen in den Leitstellen gehört es, Notrufe zu „übersetzen“ und mit Informationen aus dem verfügbaren Datenbestand über das Einsatzziel anzureichern und an die zuständigen Streifenbeamt*innen weiterzugeben, damit diese sich möglichst gut auf den Einsatz vorbereiten können. Zentral sind dafür Informationen über die Personen vor Ort. Um wie viele handelt es sich, wie sehen sie aus, sind sie hilflos oder aggressiv, bewaffnet oder verletzt? Dabei wird in diesen Einsatzmeldungen zur Beschreibung von Personen häufig auch die mutmaßliche oder tatsächliche Nationalität oder eine zugeschriebene ethnisch-kulturelle Herkunft genannt.[156] Damit sollen relevante Personen am Einsatzort schnell identifizierbar gemacht oder auf mögliche Sprachbarrieren hingewiesen werden. Mitunter sind sie aber als Warnung vor drohenden Widerstandshandlungen gemeint oder werden als solche verstanden, sodass besondere Maßnahmen zur Eigensicherung veranlasst oder weiteres Personal angefordert werden.[157]

Somit kann eine Angabe über die Nationalität oder „Volkszugehörigkeit“, deren Speicherung ursprünglich reinen Identifizierungszwecken diente, in der Vorbereitung von Einsätzen zum Signum für angeblich drohende Gefahren werden. Die Deutung der aus der Leitstelle übermittelten Informationen und die Entscheidung, wie robust der Einsatz durchgeführt wird, obliegt den Beamt*innen vor Ort. Wenn sie aufgrund generalisierender Zuschreibungen Angaben über Nationalität oder vermeintliche „ethnische Herkunft“ mit individuellem Verhalten gleichsetzen, kann die Verfügbarkeit des sensiblen Datums somit den entscheidenden Unterschied dabei machen, ob ein Einsatz ohne Not eskaliert.

Auswerteprojekt zur Suche nach „Gefährdern“ in Rheinland-Pfalz

Wie Auswerte- oder Analyseprojekte der Polizei zur vorbeugenden Bekämpfung von Straftaten und zur Terrorismusbekämpfung Menschen in den

154 Antwort der Innenministerien und -senator*innen der Länder auf Fragebogen des Deutschen Instituts für Menschenrechte (siehe Fußnote 11).
155 Hierzu: Grutzpalk (2016), S. 33 ff.
156 Für Berlin beschrieben bei: Howe u.a. (2022), S. 72 ff.
157 Ebd.

Fokus der Polizei rücken können, nur weil sie eine bestimmte „nationale Herkunft“ haben, zeigt ein Beispiel aus Rheinland-Pfalz. Dort führte das Landeskriminalamt im Dezember 2017 das „Auswerteprojekt Erkennen von Risikopersonen aus der Zuwanderungsbewegung im Bereich des islamistischen Terrorismus“ (AERBiT). Ziel war es, Zugewanderte zu identifizieren, die mögliche Bezüge zum Phänomenbereich „religiöse Ideologie“ der politisch motivierten Kriminalität aufweisen könnten und bislang überwiegend im Bereich der Allgemeinkriminalität polizeibekannt geworden waren.

Auf Grundlage von Erkenntnissen über die Täter von dschihadistischen Anschlägen in jüngerer Zeit in Europa und weiteren Merkmalen entwickelte das Landeskriminalamt ein Personenprofil, mit dem im polizeilichen Vorgangsbearbeitungssystem recherchiert wurde: Gesucht wurde nach männlichen Personen im Alter zwischen 14 und 35 Jahren aus 18 Herkunftsstaaten. Um welche Staaten es sich dabei handelte, ist unbekannt. Auswahlkriterium war, dass dort islamistische Terrororganisationen aktiv sind oder die Staaten in Krisenregionen liegen. Methodisch entspricht die Recherche einer Rasterfahndung, die das Bundesverfassungsgericht nur unter der Voraussetzung einer konkreten Gefahr für zulässig erklärt hat.[158] Der Unterschied gegenüber der Rasterfahndung war, dass keine Daten aus nichtpolizeilichen Quellen herangezogen wurden. Gleichwohl bedeutet die Suche im polizeilichen Vorgangsbearbeitungssystem, dass das Auswerteprojekt eine große Streubreite hatte.

Die ausgerasterten Personen wurden anschließend vom Staatsschutz des Landeskriminalamtes mit Unterstützung der lokalen Polizeipräsidien und gegebenenfalls in „Fallkonferenzen“ mit anderen Behörden auf Anzeichen einer islamistischen Radikalisierung überprüft. Bis Juni 2018 wurden jedoch keine der mutmaßlichen „Risikopersonen“ als „Gefährder“ oder „relevante Personen“ eingestuft. Erkenntnisse zu strafrechtlichen Verurteilungen von insgesamt 146 Personen wurden jedoch an die für das Ausländer- und Flüchtlingswesen zuständige Verwaltungsbehörde des Landes übermittelt. Zusätzlich wurden die Namen aller „Risikopersonen“ an das Integrationsministerium des Landes weitergegeben. Gegen mindestens 33 der 146 Personen wurden anschließend ausländer- oder asylrechtliche Maßnahmen zur Ausweisung eingeleitet.[159]

Im Gegensatz zu Menschen anderer Nationalität, deren Verurteilungen unentdeckt blieben, wurde den Betroffenen zum Verhängnis, dass sie ins polizeiliche Risikoprofil passten, weil sie die „falsche“ Staatsbürgerschaft hatten. Ohne dass von ihnen eine terroristische Gefahr ausging, erfolgte durch das Analyseprojekt somit eine Benachteiligung aufgrund der nationalen Herkunft.

Lagebilder zu „Clankriminalität“ in Nordrhein-Westfalen

Wie auch Namen zu einem sensiblen Datum werden können und welche stigmatisierenden Wirkungen sich daraus ergeben, lässt sich an der Erstellung der Lagebilder zur sogenannten Clankriminalität in Nordrhein-Westfalen illustrieren. Als dort 2019 erstmals ein solches Lagebild erstellt wurde, bediente sich das zuständige Landeskriminalamt einer an Familiennamen orientierten Recherchemethode.[160] Zuvor war in Zusammenarbeit mit anderen Landeskriminalämtern und Verwaltungsbehörden sowie den Kreispolizeibehörden eine Liste mit Familiennamen erstellt worden, die als relevant erachtet wurden. Eine genauere Analyse des Landeskriminalamtes zeigte, dass die dabei verwendeten Familiennamen auch Nachnamen beinhalteten, die überdurchschnittlich häufig in muslimisch geprägten Ländern vorkommen, sodass schließlich 211 Familiennamen extrahiert wurden, die aufgrund der unterschiedlichen Schreibweisen abschließend zu 104 „Clannamen“ geclustert wurden. Auf dieser Grundlage wurden zu einem

158 Bundesverfassungsgericht (2006): Rasterfahndung II. Beschluss vom 04.04.2006, 1 BvR 518/02.

159 Landtag Rheinland-Pfalz (06.06.2018); Landtag Rheinland-Pfalz (27.06.2018).

160 Landeskriminalamt Nordrhein-Westfalen (2019). Dabei wird „Clankriminalität“ als „die vom Gewinn- oder Machtstreben bestimmte Begehung von Straftaten unter Beteiligung Mehrerer, wobei in die Tatbegehung bewusst die gemeinsame familiäre oder ethnische Herkunft als verbindende, die Tatbegehung fördernde oder die Aufklärung der Tat hindernde Komponente einbezogen wird, die Tatbegehung von einer fehlenden Akzeptanz der deutschen Rechts- oder Werteordnung geprägt ist und die Straftaten einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind“ (S. 7).

bestimmten Stichtag im polizeilichen Vorgangsbearbeitungssystem sämtliche Daten zu Straftaten auf Basis der besagten Familiennamen für den Zeitraum 2016 bis 2018 erhoben.

Die Auswertung beschränkte sich zudem auf Tatverdächtige mit libanesischer, türkischer, syrischer oder deutscher Staatsangehörigkeit sowie auf Tatverdächtige mit ungeklärter Nationalität und Staatenlose. Die entsprechende Suche im Vorgangsbearbeitungssystem führte zu einem Datenbestand von 6.449 Tatverdächtigen und 14.225 mutmaßlichen Straftaten. Zusätzlich erfolgte unter der Prämisse, dass sich daraus Rückschlüsse auf die Anerkennung der Rechtsordnung ziehen ließen, für den gleichen Zeitraum eine Auswertung von registrierten Verkehrsordnungswidrigkeiten auf der Basis von zwei „Clannamen". Das Lagebild bereitet die entsprechend extrahierten Daten auf, um deliktspezifische und regionale Schwerpunkte, Staatsangehörigkeiten und Geschlecht von Tatverdächtigen darzustellen und behördliche Maßnahmen zu diskutieren.

Am Ende des Lagebildes schreibt das Landeskriminalamt selbst, dass „dieser methodische Ansatz eine an ethnischen Kriterien orientierte Profilbildung darstellt".[161] Gleichwohl wird an der Lagebilderstellung zu „Clankriminalität" auf Grundlage des namensbasierten Ansatzes weiterhin festgehalten[162], sodass Menschen nur aufgrund ihres Nachnamens Gefahr laufen, Ziel polizeilicher Maßnahmen und öffentlich stigmatisiert zu werden.

161 Ebd., S. 24.

162 Landeskriminalamt Nordrhein-Westfalen (2021).

4 Fazit

Die deutschen Polizeien verarbeiten in erheblichem Ausmaß sensible Daten zu vermeintlicher „rassischer und ethnischer Herkunft“ (vgl. Kasten S. 15). Dabei geht es nicht nur um Angaben zu „Volkszugehörigkeit“ oder „Phänotyp“. Je nach Verarbeitungskontext kann es sich auch um Standarddaten wie Name oder Staatsangehörigkeit handeln, die unter Umständen stellvertretend für rassifizierende Zuschreibung genutzt werden. Erhoben werden die Daten zum Beispiel bei erkennungsdienstlichen Maßnahmen, der Protokollierung von Zeugenaussagen oder im Rahmen von Überwachungsoperationen.

Die Polizei ist bei der Erhebung, Speicherung, Nutzung, Übermittlung und Löschung von personenbezogenen Daten sowohl an das Recht auf Privatsphäre und Datenschutz als auch an das Verbot der rassistischen Diskriminierung gebunden. Da die Verarbeitung sensibler Daten zu „rassischer oder ethnischer Herkunft“ immer das Risiko rassistischer Diskriminierung birgt, gelten für sie besonders hohe Anforderungen:

Nach Artikel 10 der JI-Richtlinie ist eine Verarbeitung nur zulässig, wenn sie „unbedingt erforderlich“ ist und entsprechende Garantien zum Schutz der Rechte und Freiheiten der Betroffenen bestehen. Zudem muss in der Regel eine gesetzliche Grundlage für die Verarbeitung existieren. Die bisherige Umsetzung der JI-Richtlinie in deutsches Recht garantiert jedoch kein ausreichend hohes Schutzniveau für die Verarbeitung sensibler Daten. § 48 des Bundesdatenschutzgesetzes sowie die einschlägigen landesrechtlichen Regelungen zur polizeilichen Datenverarbeitung übernehmen regelmäßig mehr oder weniger nur den Wortlaut der JI-Richtlinie.

Das Ziel, einen adäquaten Schutz vor Diskriminierungsrisiken zu gewährleisten, wurde bei der Umsetzung der JI-Richtlinie weitgehend verfehlt: Es mangelt sowohl an hinreichend präzisen Vorgaben, die deutlich machen, welche Tatbestände eine unbedingte Erforderlichkeit der Datenverarbeitung begründen würden, als auch an verbindlichen Vorgaben für Maßnahmen zum Schutz der Betroffenenrechte bei der Verarbeitung sensibler Daten.

Mit der aktuell laufenden Modernisierung der polizeilichen IT-Architektur, die auf eine bessere Verfügbarkeit der Daten und ihre „intelligente“ Auswertung zielt, wachsen die Diskriminierungsrisiken: Durch intransparente algorithmengestützte Datenverarbeitung droht die Gefahr, dass Gruppen, die bereits jetzt in überproportionalem Maße durch die Polizei registriert sind, künftig verstärkt ins Visier der Polizei geraten.

Das Deutsche Institut für Menschenrechte empfiehlt den Gesetzgebern in Bund und Ländern daher dringend nachzusteuern, um den Schutz vor rassistischer Diskriminierung auch bei der polizeilichen Datenverarbeitung zu gewährleisten. Hierzu sollten Vorschriften erlassen werden, welche die tatbestandlichen Voraussetzungen für die Erhebung, Speicherung und weitere Nutzung sensibler Daten eng gefasst präzisieren und verbindliche Regeln für Schutzmaßnahmen normieren.

Damit die Gesetzgeber dieser Aufgabe informiert nachkommen können, ist eine offene Diskussion über die polizeiliche Verarbeitung solcher Daten notwendig. Hierzu zählen insbesondere die Fragen:

- In welchem Ausmaß und in welchen Systemen werden Daten zu „rassischer und ethnischer Herkunft“ derzeit verarbeitet?
- Wie werden Standarddaten für rassifizierende Zuschreibungen genutzt?
- Wann und warum wird die Verarbeitung sensibler Daten von der Polizei für erforderlich gehalten?
- Sind die entsprechenden Grundannahmen zur Erforderlichkeit zutreffend oder handelt es sich um die Reproduktion rassistischer Stereotype?

– Welche gesetzlichen (und praktischen) Maßnahmen sind erforderlich, um den gebotenen Diskriminierungsschutz zu gewährleisten?

Eine solche Debatte braucht nicht nur eine kritische Selbstreflexion der Polizei, sondern auch die Beteiligung von Datenschutzexpert*innen, Wissenschaft und zivilgesellschaftlichen Akteuren, insbesondere den Selbstorganisationen von Menschen mit Rassismuserfahrungen.

Bislang steht die Intransparenz der polizeilichen Datenverarbeitung einer solch offenen Debatte im Weg. Laufende und künftige Forschungsvorhaben und ein stärkeres Bewusstsein für die Risiken der Verarbeitung sensibler Daten zu vermeintlich „rassischer oder ethnischer Herkunft“ bei Polizei, Datenschutzaufsichtsbehörden, aber auch bei den Betroffenen selbst könnte helfen, Licht ins Dunkel zu bringen.

Das Deutsche Institut für Menschenrechte empfiehlt daher den Innen- und Forschungsministerien, Zugänge und Mittel für Forschung bereitzustellen. Die mit Diskriminierung und Rassismus befassten Beauftragten der Bundesregierung könnten in Zusammenarbeit mit dem Bundesdatenschutzbeauftragten oder der Konferenz der Datenschutzbeauftragten von Bund und Ländern entsprechende Dialogformate ausrichten und Bericht erstatten.

Auf dieser Grundlage sollten die Gesetzgeber die laufenden Diskussionen über eine differenzierte Normierung der polizeilichen Weiterverarbeitung von Daten nutzen, um auch die Risiken rassistischer Diskriminierung zu minimieren. Bis dahin braucht es die Wachsamkeit der Betroffenen und der unabhängigen Datenschutzaufsichtsbehörden.

5 Literatur

Abgeordnetenhaus Berlin (13.10.2014): Polizeiliche Erfassung der „Volkszugehörigkeit“ und des „Phänotypus“ in Datenbanken. Schriftliche Anfrage der Abgeordneten Christopher Lauer und Fabio Reinhardt (PIRATEN) vom 18. September 2014 und Antwort, Drucksache 17/14582. https://pardok.parlament-berlin.de/starweb/adis/citat/VT/17/SchrAnfr/s17-14582.pdf (abgerufen am 16.10.2023)

Abgeordnetenhaus Berlin (28.01.2020): Schriftliche Anfrage der Abgeordneten Niklas Schrader und Anne Helm (LINKE) vom 09. Januar 2020 zum Thema: „Racial Profiling“ und Erfassung von „Volkszugehörigkeit“ und Phänotyp von Verdächtigen durch die Polizei Berlin und Antwort vom 28. Januar 2020, Drucksache 18/22057. http://pardok.parlament-berlin.de/starweb/adis/citat/VT/18/SchrAnfr/s18-22057.pdf (abgerufen am 16.10.2023)

Abgeordnetenhaus Berlin (09.06.2023): Diskriminierende Datenerfassung POLIKS. Schriftliche Anfrage der Abgeordneten Elif Eralp (LINKE) vom 22. Mai 2023 und Antwort vom 5. Juni 2023, Drucksache 19/15612. https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-15612.pdf (abgerufen am 16.10.2023).

Abgeordnetenhaus Berlin (20.12.2023): Diskriminierende Datenerfassung POLIKS Teil II. Schriftliche Anfrage der Abgeordneten Elif Eralp (LINKE) vom 5. Dezember 2023 und Antwort vom 20. Dezember 2023, Drucksache 19/17533. https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-17533.pdf (abgerufen am 21.02.2024).

Albers, Marion (2005): Informationelle Selbstbestimmung. Baden-Baden: Nomos

Albers, Marion / Schimke, Anna (2023): BDSG § 48. In: Wolff, Heinrich Amadeus / Brink, Stefan / Ungern-Sternberg, Antje von (Hg.): Beck’scher Online-Kommentar Datenschutzrecht, 44. Auflage. München: C.H.Beck

Arzt, Clemens (2021): Praxis der polizeilichen Datenverarbeitung. In: Bäcker, Matthias / Denninger, Erhard / Graulich, Kurt / Lisken, Hans (Hg.): Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz, 7. Auflage. München: C.H. Beck, S. 1161–1218

Arzt, Clemens (2023): Polizeiliche Verarbeitung „besonderer Kategorien personenbezogener Daten“. Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland. In: Die Öffentliche Verwaltung 76 (23), S. 991–1002

Atali-Timmer, Fatoş / Fereidooni, Karim / Schroth, Kathrin (2022): Rassismuskritische Polizeiforschung. Eine Spurensuche. In: Hunold, Daniela / Tobias Singelnstein (Hg.): Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme. Heidelberg: Springer, S. 33–52

Baer, Susanne / Markard, Nora (2018): Artikel 3, Absatz 2 und 3. In: Huber, Peter M. / Voßkuhle, Andreas (Hg.): Grundgesetz. Kommentar. Band 1 (Präambel, Artikel 1–19), 7. Auflage. München: C.H.Beck, S. 409–457

Barskanmaz, Cengiz (2019): Recht und Rassismus. Das menschenrechtliche Verbot der Diskriminierung aufgrund der Rasse. Berlin: Springer

Barskanmaz, Cengiz (2020): Verfassungsdogmatik und Interdisziplinarität ernstnehmen. In: Aus Politik und Zeitgeschichte 70 (42–44), S. 19–22

Barskanmaz, Cengiz (2022): Menschenrechtliche Grundlagen polizeilicher Praxis. In: Hunold, Daniela / Singelnstein, Tobias (Hg.): Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme. Heidelberg: Springer, S. 55–81

Bergmann, Jens / Jacobsen, Astrid (2021): Diskriminierung und Rassismus in der Polizei als Forschungsfeld – eine problemorientierte Bestandsaufnahme. In: SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 18 (4), S. 45–57

Berliner Beauftragte für Datenschutz und Informationsfreiheit (2021): Datenschutz und Informationsfreiheit. Jahresbericht 2020. Berlin. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/jahresbericht/BlnBDI-Jahresbericht-2020-Web.pdf (abgerufen am 16.10.2023)

Bielefeldt, Heiner (2011): Datenschutz als Solidaritätsgebot. In: Bielefeldt, Heiner / Deile, Volkmar / Hamm, Brigitte / Hutter, Franz-Josef / Kurtenbach, Sabine / Tretter, Hannes (Hg.): Nothing to hide – nothing to fear? Datenschutz – Transparenz – Solidarität (Jahrbuch Menschenrechte 2011). Wien / Köln / Weimar: Böhlau, S. 25–33

Bosch, Alexander (2020): Die aktuelle Debatte um Rassismus und Rechtsextremismus in der Polizei. In: Vorgänge 59 (231/232), S. 167–177

Braun, Frank (2022): BDSG § 48. In: Gola, Peter / Heckmann, Dieter (Hg.): Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage. München: C.H. Beck

Brück, Vanessa (2019): Polizei 2020 – Das Zukunftsprogramm der Polizei in Deutschland. In: Polizeispiegel 53 (7–8), S. 10–11

Bundeskonferenz der Migrantenorganisationen (27.02.2020): Offener Brief an die Bundeskanzlerin Dr. Angela Merkel. Berlin. http://s890498910.online.de/wp-content/uploads/2020/02/260220_Offener-Brief-der-MO-an-Bundeskanzlerin-Merkel-2.pdf (abgerufen am 16.10.2023)

Bundeskriminalamt (2015): Verwaltungsvorschrift nach § 3 Absatz 4 des Antiterrordateigesetzes (ATDG-Verwaltungsvorschrift – ATD-VwV) vom 3. Juli 2015. In: Bundesanzeiger vom 24.07.2015

Bundeskriminalamt (2017): Datenbestand und Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) in den Jahren 2014–2017. Bericht an den Deutschen Bundestag. Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/AntiterrordateiRechtsextremismusdatei/bericht_atd_red.pdf?__blob=publicationFile&v=2 (abgerufen am 16.10.2023)

Bundeskriminalamt (2020): Datenbestand und Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) in den Jahren 2018–2020. Bericht an den Deutschen Bundestag. Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/AntiterrordateiRechtsextremismusdatei/bericht_atd_red_2018-2020.pdf (abgerufen am 16.10.2023)

Bundesministerium des Innern (2014): Vierter Bericht der Bundesrepublik Deutschland gemäß Artikel 25 Absatz 2 des Rahmenübereinkommens des Europarats zum Schutz nationaler Minderheiten. Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/heimat-integration/minderheiten/4-vierter-staatenbereicht-rahmenuebereinkommen.pdf?__blob=publicationFile&v=3 (abgerufen am 16.10.2023)

Bundesministerium des Innern, für Bau und Heimat (2021): Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. Berlin. https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf (abgerufen am 15.03.2024)

Bundesministerium der Justiz und für Verbraucherschutz (2017): Das Internationale Übereinkommen der Vereinten Nationen zur Beseitigung jeder Form von Rassendiskriminierung (ICERD) vom 21. Dezember 1965. Berlin. https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/2017_ICERD.pdf?__blob=publicationFile&v=4 (abgerufen am 16.10.2023)

Bundesrat (28.05.2010): Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen. Verordnung des Bundesministeriums des Innern, Drucksache 329/10

Chan, Janet (2001): The technological game. How information technology is transforming police practice. In: Criminal Justice 1 (2), S. 139–159

Creemers, Niklas / Guagnin, Daniel (2014): Datenbanken in der Polizeipraxis. Zur computergestützten Konstruktion von Verdacht. In: Kriminologisches Journal 46 (3), S. 138–152

Cremer, Hendrik (2013): „Racial Profiling" – Menschenrechtswidrige Personenkontrollen nach § 22 Abs. 1 a Bundespolizeigesetz. Empfehlungen an den Gesetzgeber, Gerichte und Polizei. Berlin: Deutsches Institut für Menschenrechte. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Racial_Profiling_Menschenrechtswidrige_Personenkontrollen_nach_Bundespolizeigesetz.pdf (abgerufen am 16.10.2023)

Cremer, Hendrik (2020): Das Verbot rassistischer Diskriminierung. Vorschlag für eine Änderung von Artikel 3 Absatz 3 Satz 1 Grundgesetz. Berlin: Deutsches Institut für Menschenrechte. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Analyse_Studie/Analyse_Verbot_rassistischer_Diskriminierung.pdf (abgerufen am 16.10.2023)

Danielzik, Chandra-Milena (2018): Was ist Rassismus? Eine Begriffsklärung. In: Cobbinah, Beatrice / Danielzik, Chandra-Milena (Hg.): Rassistische Straftaten erkennen und verhandeln. Ein Reader für die Strafjustiz. Berlin: Deutsches Institut für Menschenrechte, S. 33–47. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/user_upload/Publikationen/Praxis_Rassistische_Straftaten_erkennen_und_verhandeln_barrierefrei.pdf (abgerufen am 16.10.2023)

Datenschutzkonferenz (2021): Stellungnahme der DSK zur Evaluierung des BDSG. https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf (abgerufen am 15.03.2024)

Dengler, Pascal / Foroutan, Naika (2017): Die Aufarbeitung des NSU als deutscher Stephen-Lawrence-Moment? Thematisierung von institutionellem Rassismus in Deutschland und Großbritannien. In: Fereidooni, Karim / EL, Meral (Hg.): Rassismuskritik und Widerstandsformen. Wiesbaden: Springer, S. 429

Deutscher Bundestag (25.06.1986): Entschließungsantrag zum Antrag betr. Verbesserung der Situation der Sinti und Roma; Antrag betr. Lage der Sinti, Roma und verwandte Gruppen; Entschließungsantrag zur Großen Anfrage betr. Lage und Forderungen der Sinti, Roma und verwandte Gruppen; Antrag betr. Gesetzentwurf zur Regelung einer angemessenen Versorgung für alle Opfer nationalsozialistischer Verfolgung in der Zeit von 1933 bis 1945; Antrag betr. Bestandsaufnahme, Bericht und Prüfung von verbesserten Leistungen an Opfer nationalsozialistischer Verfolgung von 1933 bis 1945; Antrag betr. Entschädigung für Zwangsarbeit während der Nazi-Zeit sowie zur Entschließung zu Entschädigungsleistungen für ehemalige Sklavenarbeiter der deutschen Industrie, Drucksache 10/5765

Deutscher Bundestag (19.12.1996): „Kritik an rassistischen Typisierungen“ in polizeilichen Erfassungsbögen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Volker Beck (Köln), Cem Özdemir, Kerstin Müller (Köln), Manfred Such und der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drucksache 13/6623

Deutscher Bundestag (07.03.2013): Bericht zur Evaluierung des Antiterrordateigesetzes. Unterrichtung durch die Bundesregierung, Drucksache 17/12665

Deutscher Bundestag (09.02.2021): Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei. Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Drucksache 19/26541

Deutscher Bundestag (07.05.2021): Schriftliche Fragen mit den in der Woche vom 3. Mai 2021 eingegangenen Antworten der Bundesregierung, Drucksache 19/26541

Deutscher Bundestag (21.05.2021): Bericht der Unabhängigen Kommission Antiziganismus: Perspektivwechsel – Nachholende Gerechtigkeit – Partizipation. Unterrichtung durch die Bundesregierung, Drucksache 19/30310

Deutscher Bundestag (28.04.2023): Aktueller Stand der polizeilichen Datenhaltung in Deutschland. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 20/6633

Die Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration / Die Beauftragte der Bundesregierung für Antirassismus (2023): Rassismus in Deutschland. Lagebericht. Ausgangslage, Handlungsfelder, Maßnahmen. Berlin. https://www.integrationsbeauftragte.de/resource/blob/1864320/2157012/77c8d1dddeea760bc13dbd87ee9a415f/lagebericht-rassismus-komplett-data.pdf (abgerufen am 16.10.2023)

Eder, Gerald (2005): EASy – die zukunftsweisende Ermittlungssoftware. In: Die Kriminalpolizei 23 (4), S. 133–135

End, Markus (2019): Antiziganismus und Polizei. Heidelberg: Zentralrat Deutscher Sinti und Roma

Ericson, Richard (2007): Rules in policing. Five perspectives. In: Theoretical Criminology 11 (3), S. 367-401

Ericson, Richard / Haggerty, Kevin (1997): Policing the risk society. Oxford: Clarendon Press

Europäische Kommission (25.07.2022): Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/68. Richtlinie zum Datenschutz bei der Strafverfolgung, COM (2022) 364 final

Europäische Kommission gegen Rassismus und Intoleranz (2020): ECRI-Bericht über Deutschland (Sechste Prüfungsrunde). Verabschiedet am 10. Dezember 2019. Straßburg. https://rm.coe.int/ecri-report-on-germany-sixth-monitoring-cycle-german-translation-/16809ce4c0 (abgerufen am 16.10.2023)

Farkas, Lilla (2017): The meaning of racial or ethnic origin in EU law: between stereotypes and identities. Luxembourg: Publications Office of the European Union

Feltes, Thomas / Weingärtner, Rahel / Weigert, Marvin (2016): „Ausländerkriminalität“. In: Zeitschrift für Ausländerrecht 36 (5), S. 157–165

Feuerhelm, Wolfgang (1987): Polizei und „Zigeuner“. Strategien, Handlungsmuster und Alltagstheorien im polizeilichen Umgang mit Sinti und Roma. Stuttgart: Enke

Fink, Felix / Kretschmann, Andrea (2022): Polizei und Rassismus. Konsolidierung eines neuen Forschungsbereiches? In: Forschungsjournal Soziale Bewegungen 35 (4), S. 703-719

Fischer, Tin (20.04.2023): Auch „Nichtdeutsche“ unter den Tätern. In: DIE ZEIT 2023 (17), S. 19

Foroutan, Naika (2020): Rassismus in der postmigrantischen Gesellschaft. In: Aus Politik und Zeitgeschichte 70 (42–44), S. 12–26

Frenzel, Eike M. (2021): BDSG § 48. In: Paal, Boris P. / Pauly, Daniel A. (Hg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. DS-GVO BDSG, 3. Auflage. München: C.H. Beck

Gadorosi, Holger / Matthey, Susanne (2023): Auf dem Weg zu einer digitalen und vernetzten Polizei – P20. In: Wehe, Dieter / Siller, Helmut (Hg.): Handbuch Polizeimanagement, 2. Auflage. Wiesbaden: Springer, S. 1411–1429

Graulich, Kurt (2019): Bundeskriminalamtgesetz. In: Schenke, Wolf-Rüdiger / Graulich, Kurt / Ruthig, Josef (Hg.): Sicherheitsrecht des Bundes. BPolG, BKAG, ATDG, BVerfSchG, BNDG, VereinsG, 2. Auflage. München: C.H. Beck, S. 397–808

Grutzpalk, Jonas (2016): Die Erforschung des Wissensmanagements in Sicherheitsbehörden mit Hilfe der Akteurs-Netzwerk-Theorie. In: Grutzpalk, Jonas (Hg.): Polizeiliches Wissen. Formen, Austausch, Hierarchien. Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 15–48

Haggerty, Kevin (2004): Technology and crime policy. Reply to Michael Jacobsen. In: Theoretical Criminology 8 (4), S. 491-497

Heinrich, Stephan (2007): Innere Sicherheit und neue Informations- und Kommunikationstechnologien. Veränderungen des Politikfeldes zwischen institutionellen Faktoren, Akteursorientierungen und technologischen Entwicklungen. Münster: LIT Verlag

Herold, Horst (1970): Kybernetik und Polizei-Organisation. In: Die Polizei 61 (2), S. 33–37

Herrnkind, Martin (2014): „Filzen Sie die üblichen Verdächtigen!“ oder: Racial Profiling in Deutschland. In: Polizei & Wissenschaft 15 (3), S. 35–58

Howe, Christiane u. a. (2022): Bericht zur Berliner Polizeistudie. Eine diskriminierungskritische, qualitative Untersuchung ausgewählter Dienstbereiche der Polizei Berlin. Berlin: Zentrum Technik und Gesellschaft. https://www.static.tu.berlin/fileadmin/www/10002449/PDF_s/Publikationen/Forschungsberichte/Bericht_Polizeistudie_ZTG_TU_Berlin.pdf (abgerufen am 16.10.2023)

Hunold, Daniela / Wegner, Maren (2020): Rassismus und Polizei. Zum Stand der Forschung. In: Aus Politik und Zeitgeschichte 70 (42–44), S. 27–32

Hunold, Daniela / Singelnstein, Tobias (2022): Einleitung. In: Hunold, Daniela / Singelnstein, Tobias (Hg.): Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme. Heidelberg: Springer, S. 1–12

Innenministerkonferenz (10.12.2007): Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 185. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder am 7. Dezember 2007 in Berlin. https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/07-12-07/07-12-07-Beschl%C3%BCsse.pdf?__blob=publicationFile&v=2 (abgerufen am 16.10.2023)

Innenministerkonferenz (30.11.2016): Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2016/saarbruecker-agenda.pdf?__blob=publicationFile&v=2 (abgerufen am 16.10.2023)

Jacobsen, Astrid / Bergmann, Jens (2022): Vor der Erhebung. Ein Essay über Forschungszugänge in die Polizei. In: Die Polizei 113 (2), S. 52–53

Johannes, Paul C. / Weinhold, Robert (2018): Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Baden-Baden: Nomos

Kampert, David (2022): § 48 BDSG. In: Sydow, Gernot / Marsch, Nikolaus (Hg.): DS-GVO – BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Handkommentar, 3. Auflage. Baden-Baden: Nomos

Kaneza, Elisabeth (2020): Black Lives Matter. Warum Rasse nicht aus dem Grundgesetz gestrichen werden darf. In: Recht und Politik 56 (4), S. 536–541

Kingreen, Thorsten / Poscher, Ralf (2022): Polizei- und Ordnungsrecht mit Versammlungsrecht, 12. Auflage. München: C.H.Beck

Kischel, Uwe (2022): Die Streichung des Begriffs „Rasse". Ersetzt der sozialwissenschaftliche Rassismusbegriff den normativen Rassebegriff? In: Froese, Judith / Thym, Daniel (Hg.): Grundgesetz und Rassismus. Tübingen: Mohr Siebeck, S. 71–97

Konferenz der Leiterinnen und Leiter der Archivverwaltung des Bundes und der Länder (2020): Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern. Abschlussbericht. https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-polizeiliche-fachverfahren.pdf?__blob=publicationFile (abgerufen am 16.10.2023)

Landeskriminalamt Nordrhein-Westfalen (2019): Clankriminalität. Lagebild NRW 2018. Düsseldorf. https://polizei.nrw/sites/default/files/2019-05/190515_Lagebild%20Clan%202018.pdf (abgerufen am 16.10.2023)

Landeskriminalamt Nordrhein-Westfalen (2021): Clankriminalität. Lagebild NRW 2020. Düsseldorf. https://polizei.nrw/sites/default/files/2021-09/210902_LaBi%20Clan%202020.pdf (abgerufen am 16.10.2023)

Landtag Nordrhein-Westfalen (05.04.2022): Schlussbericht des Parlamentarischen Untersuchungsausschusses III („Kleve") zu dem Auftrag des Landtags Nordrhein-Westfalen vom 20. November 2018 Drucksache 17/4293 betreffend die Untersuchung der Umstände der Verwechslung, Inhaftierung, des Todes von Amad A. und des Umgangs mit dessen Familie. Drucksache 17/16940. https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-16940.pdf (abgerufen am 21.02.2024).

Landtag Rheinland-Pfalz (06.06.2018): Projekt AERBiT. Antwort des Ministeriums des Innern und für Sport auf die Kleine Anfrage des Abgeordneten Matthias Lammert (CDU), Drucksache 17/6416. https://dokumente.landtag.rlp.de/landtag/drucksachen/6416-17.pdf (abgerufen am 16.10.2023)

Landtag Rheinland-Pfalz (27.06.2018): Ausländische Intensivstraftäter in Rheinland-Pfalz – Teil II. Antwort des Ministeriums des Innern und für Sport auf die Kleine Anfrage des Abgeordneten Matthias Lammert (CDU), Drucksache 17/6647. https://dokumente.landtag.rlp.de/landtag/drucksachen/6647-17.pdf (abgerufen am 16.10.2023)

Liebscher, Doris (10.01.2023): Mit „Rasse" gegen Rassismus? Zur Debatte um den Rassebegriff (nicht nur) im Grundgesetz. Bonn: Bundeszentrale für politische Bildung. https://www.bpb.de/themen/rassismus-diskriminierung/rassismus/516707/mit-rasse-gegen-rassismus/ (abgerufen am 16.10.2023)

Ministerium des Innern des Landes Brandenburg (19.08.1993): Bezeichnung von Minderheiten durch die Polizei. In: Amtsblatt für Brandenburg 1993 (84), S. 1606

Ministerium des Innern des Landes Brandenburg (10.09.2014): Gewährleistung der Diskriminierungsfreiheit in der Polizei des Landes Brandenburg. In: Amtsblatt für Brandenburg 2014 (42), S. 1287

Ministerium des Innern des Landes Nordrhein-Westfalen (15.12.2008): Leitlinien für die Polizei des Landes Nordrhein-Westfalen zum Schutz nationaler Minderheiten vor Diskriminierungen (Runderlass). https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&gld_nr=2&ugl_nr=2051&bes_id=12564&menu=0&sg=0&aufgehoben=N&keyword= (abgerufen am 16.10.2023) Nabulsi, Selma (2024): Alles sensibel? Die aktuelle Rechtsprechung des EuGH zu Art. 9 Abs. 1 DSGVO. In: Privacy in Germany – PinG 12 (1), S. 12-16.

Nabulsi, Selma (2024): Alles sensibel? Die aktuelle Rechtsprechung des EuGH zu Art. 9 Abs. 1 DSGVO. In: Privacy in Germany – PinG 12 (1), S. 12–16.

Nogala, Detlef (2019): Polizei, avancierte Technik und soziale Kontrolle – wie geht's dem Frosch heute? In: Vorgänge 58 (227), S. 21–30

Payandeh, Mehrdad (2022): Das Verbot rassistischer Diskriminierung im Völkerrecht und seine Bedeutung für das verfassungsrechtliche Diskriminierungsverbot. In: Froese, Judith / Thym, Daniel (Hg.): Grundgesetz und Rassismus. Tübingen: Mohr Siebeck, S. 217–242

Petri, Thomas (2019): Artikel 9 DSGVO. In: Simitis, Spiros / Hornung, Gerrit / Spiecker Döhmann, Indra (Hg.): Datenschutzrecht. DSGVO mit BDSG. Großkommentar. Baden-Baden: Nomos, S. 579–600

Projektgruppe des AK II (10.10.2007): Abschlussbericht der Projektgruppe „Schutz nationaler Minderheiten vor Verwendung diskriminierender Minderheitenkennzeichnungen durch die Polizeibehörden". Wiesbaden. https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/07-12-07/07-12-07-Bericht%20zu%20TOP%2011.pdf?__blob=publicationFile&v=2 (abgerufen am 16.10.2023)

Reichertz, Jo / Wilz, Sylvia M. (2022): Wie verändert die Einführung der Informations- und Kommunikationsmedien die polizeiliche Ermittlungsarbeit? In: Thüne, Martin / Klaas, Kathrin / Feltes, Thomas (Hg.): Digitale Polizei. Einsatzfelder, Potenziale, Grenzen und Missstände. Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 75–90

Reuss, Anja (2023): Antiziganismus und polizeiliche Datensammlung. In: Cobbinah, Beatrice / Danielzik, Chandra-Milena (Hg.): Rassismus in der Strafverfolgung. Von der Notwendigkeit struktureller Veränderungen. Berlin: Deutsches Institut für Menschenrechte, 2. Auflage, S. 51–56. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Praxis_Rassismus_in_der_Strafverfolgung.pdf (abgerufen am 16.10.2023)

Reuter, Karl (1965): Fahnden und Finden. In: Die Polizei 56 (9), S. 265–266

Rommelspacher, Birgit (2009): Was ist eigentlich Rassismus? In: Melter, Claus / Mecheril, Paul (Hg.): Rassismuskritik, Rassismustheorie und -forschung. Schwalbach am Taunus: Wochenschau Verlag, S. 25–38

Rose, Romani (2000): Bürokratischer Rassismus. Sinti- und Roma-Dateien in Bayern. In: Müller-Heidelberg, Till u. a. (Hg.): Grundrechte-Report 2000. Zur Lage der Bürger- und Menschenrechte in Deutschland. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag, S. 50–54

Ruch, Andreas (2022): Rechtlicher Schutz vor polizeilicher Diskriminierung aus rassistischen Gründen. In: Hunold, Daniela / Singelnstein, Tobias (Hg.): Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme. Heidelberg: Springer, S. 83–103

Schäberle, Jürgen (2023): Programm Polizei 2020 – Chancen und Risiken für die Teilnehmer. In: Wehe, Dieter / Siller; Helmut (Hg.): Handbuch Polizeimanagement, 2. Auflage. Wiesbaden: Springer, S. 1431–1443

Schwichtenberg, Simon (2020): § 48 BDSG. In: Kühling, Jürgen / Buchner, Benedikt (Hg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Kommentar, 3. Auflage. München: C.H. Beck, S. 1760–1761

Stephan, Andrej (2011): „Kein Mensch sagt HWAO-Schnitzel". BKA-Kriminalpolitik zwischen beständigen Konzepten, politischer Reform und „Sprachregelungen". In: Baumann, Imanuel u. a. (Hg.): Schatten der Vergangenheit. Das BKA und seine Gründungsgeneration in der frühen Bundesrepublik. Köln: Luchterhand, S. 247–285

Tabbara, Tarik (2021): Von der Gleichbehandlung der „Rassen" zum Verbot rassistischer Diskriminierung. In: Der Staat 60 (3–4), S. 577

Töpfer, Eric (2020): (Dis-)Kontinuitäten antiziganistischen Profilings im Zusammenhang mit der Bekämpfung „reisender Täter" zur Vorlage bei der Unabhängigen Kommission Antiziganismus. Berlin: Deutsches Institut für Menschenrechte. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/PDF/UKA/Forschungsbericht_Dis_Kontinuitaeten_antiziganistischen_Profilings_im_Zusammenhang_mit_der_Bekaempfung_reisender_Taeter.pdf (abgerufen am 16.10.2023)

Tsianos, Vassilis / Karakayali, Juliane (2014): Rassismus und Repräsentationspolitik in der postmigrantischen Gesellschaft. In: Aus Politik und Zeitgeschichte 64 (13–14), S. 33–39

Unabhängige Kommission Antiziganismus (2021): Perspektivwechsel. Nachholende Gerechtigkeit. Partizipation. Berlin: Bundesministerium des Innern, für Bau und Heimat

Wegner, Kilian (2023): Über die sogenannte Clankriminalität. Kurze Kritik eines (Kampf-)Begriffs. In: Verfassungsblog vom 11.08.2023. https://verfassungsblog.de/uber-die-sogenannte-clankriminalitat (abgerufen am 16.10.2023)

Weichert, Thilo (2017): „Sensible Daten" revisited. In: Datenschutz und Datensicherheit 41 (9), S. 538–543

Weichert, Thilo (2022): Kennzeichnungspflicht von polizeilichen Datensätzen. Anspruch und Wirklichkeit. In: Neue Zeitschrift für Verwaltungsrecht 41 (12), S. 844–851.

Weichert, Thilo (2024): Art. 9 DSGVO In: Kühling, Jürgen / Buchner, Benedikt (Hg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Kommentar, 4. Auflage. München: C.H. Beck

Zentralrat Deutscher Sinti und Roma (15.06.2020): Pressemitteilung: Der Zentralrat Deutscher Sinti und Roma fordert die Streichung von „Rasse" aus dem Grundgesetz. https://zentralrat.sintiundroma.de/der-zentralrat-deutscher-sinti-und-roma-fordert-die-streichung-von-rasse-aus-dem-grundgesetz/ (abgerufen am 16.10.2023)

Anhang

Abbildungen

Tabellen

Abkürzungen

Abs.	Absatz
AGG	Allgemeines Gleichbehandlungsgesetz
Art.	Artikel
ATD	Antiterrordatei
BayPAG	Bayerisches Polizeiaufgabengesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BKADV	BKA-Daten-Verordnung (Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen)
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern und für Heimat

CERD	Committee on the Elimination of Racial Discrimination (UN-Ausschuss gegen rassistische Diskriminierung)
DIMR	Deutsches Institut für Menschenrechte
DSGVO	Datenschutz-Grundverordnung
Ebd.	Ebenda
ECRI	Europäische Kommission gegen Rassismus und Intoleranz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
EU	Europäische Union
ff.	folgende (Seiten)
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination (Internationales Übereinkommen zur Beseitigung jeder Form von rassistischer Diskriminierung, auch: Antirassismus-Konvention)
IMK	Innenministerkonferenz
INPOL	Polizeiliches Informationssystem
JI-Richtlinie	EU-Datenschutz-Richtlinie im Bereich Justiz und Inneres
Rn.	Randnummer
S.	Seite
UN	United Nations (Vereinte Nationen)
Ziff.	Ziffer

Impressum

HERAUSGEBER
Deutsches Institut für Menschenrechte
Zimmerstraße 26/27 | 10969 Berlin
Tel.: 030 259 359–0 | Fax: 030 259 359–59
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

ANALYSE | Mai 2024
ISBN 978-3-949459-44-3 (PDF)
ISBN 978-3-949459-49-8 (Print)

ZITIERVORSCHLAG
Töpfer, Eric (2024): Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung. Berlin: Deutsches Institut für Menschenrechte

Der Text ist eine aktualisierte Fassung des Kapitels „Risiken rassistischer Diskriminierung durch polizeiliche Datenverarbeitung“ in der Publikation „Entwicklung der Menschenrechtssituation in Deutschland Juli 2022 – Juni 2023. Bericht an den Deutschen Bundestag gemäß § 2 Absatz 5 DIMRG“. Berlin: Deutsches Institut für Menschenrechte, 2023

LIZENZ
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

TITELFOTO
© picture alliance/Harald Tittel/dpa

SATZ
www.avitamin.de

ABBILDUNGEN
WEBERSUPIRAN.berlin

DRUCK
Druck- und Verlagshaus Zarbock GmbH & Co. KG

Gedruckt auf 100 % Altpapier

eco zoom natureOffice.com/DE-077-367729 · CO2e-bilanzierte Aktivitäten · CO2e-Emissionen ausgeglichen

FSC www.fsc.org RECYCLED Papier aus Recyclingmaterial Paper made from recycled material FSC® C003425

BLAUER ENGEL DAS UMWELTZEICHEN www.blauer-engel.de/uz195
- ressourcenschonend und umweltfreundlich hergestellt
- emissionsarm gedruckt
- überwiegend aus Altpapier AR1

Dieses Druckerzeugnis ist mit dem Blauen Engel ausgezeichnet.

Deutsches Institut für Menschenrechte

Zimmerstraße 26/27
10969 Berlin

www.institut-fuer-menschenrechte.de